U.S. DRUG ENFORCEMENT ADMINISTRATION
AND
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

ELECTRONIC PRESCRIPTIONS

FOR CONTROLLED SUBSTANCES (EPCS)

July 12, 2006

Crystal City Marriott
1999 Jefferson Davis Highway
Arlington, Virginia

Proceedings By:

CASET Associates, Ltd.
10201 Lee Highway, Suite 180
Fairfax, Virginia 22030
(703)352-0091

TABLE OF CONTENTS

P R O C E E D I N G S (8:35 a.m.)

MR. CAVERLY: If we have any additional panelists, if they could take the stage, please, and any questioners, we will get started this morning.

Welcome back. For those of you who were not here yesterday, let me just welcome you to this DEA and HHS sponsored two-day public meeting on electronic prescribing for controlled substances.

If you were not here yesterday, you missed a lot of conversation. We had three different panels representing the physicians, practitioners and technology, and we received a lot of good information. We appreciate particularly public comments at the end of yesterday's session, and we will have an opportunity to provide additional public comments at the end of today's sessions. So once again, welcome.

I was struck, if I can editorialize a moment, yesterday from DEA's standpoint, the Controlled Substances Act is at the heart of what we do. That is what we have been asked to enforce. This is such an important public health and welfare issue. It was emphasized to me yesterday how important this is.

So that is the end of my editorializing. Once again, welcome to this second day.

We are going to begin pretty immediately with the

vendor perspective this morning. We have on our panel scheduled Michael Burger, who is the product manager, e-prescribing, for Emdeon Practice Services, James Chen, who is the chief executive officer for DrFirst, Nigel Johnson, who is the vice president for product management for Zix Corporation, and Russ Thomas, who is the chief executive officer for Gold Standard. We have allowed approximately 15 minutes for each one of our presenters, and then following the format of yesterday, we will also permit questions, both from the HHS side of the house, as well as from DEA.

So once again, welcome. Michael Burger, I think you are first up.

Agenda Item: Vendor Perspectives Panel

MR. BURGER: Good morning, everyone. Thank you very much for the opportunity to participate today. My name is Mike Burger, and I am the product manager for clinical products at Emdeon Practice Services. As well I am the director of strategic clinical initiatives, which is a fancy name for catchall for these kinds of things. So I get to go out and represent our company's perspective.

Emdeon Corporation is composed of a couple of different parts, some of which are household names. Part of our company is WebMD.com, which is our consumer facing web portal. The other part of it is Medscape.com, which is

the physician facing web portal. You have read the statistics and the press releases, I'm sure. WebMD particularly is very, very widely used on the consumer side. Medscape is the largest CME provider, online CME provider in the country today.

Emdeon Business Services is another division of our company. It was formerly known among other things as Envoy. It is the largest health care EDI network in the country. This year we are going to process nearly three billion health care transactions. Every single one of those contains PHI, claims, eligibility, prescriptions, pharmacy to PBM transactions, those kinds of things. So we have got lots and lots and lots of experience, lots and lots of transactions, in the health care EDI business.

Last but certainly not least is Emdeon Practice Services, which is the division of the company that I represent. There are a couple of different products that we have in the marketplace, among them the medical manager, PCN and Versus and Entergy, which is our growth product.

We are the largest of the practice management software vendors. There are about 180,000 physicians that are using one of our products in their offices. All of those physicians are using our billing and scheduling product. The new frontier is the electronic health record, and there are a growing number of those physicians that are

adopting electronic health records. Hopefully if we do our job right, they will be adopting ours, but they have the opportunity to adopt other companies' EHRs if they do desire.

In the e-prescribing world, we have offered e-prescribing since 1995 before it was called e-prescribing. It was just called a prescription writeup. From the very first customer, who was a physician in Klamath Falls, Oregon, of all places, is still using our e-prescribing software today. So we have been at this for quite awhile.

We have PC-based software. We have got a PDA, a personal digital assistant or a Palm Pilot version. We have got a web-based application as well. E-prescribing initially was only embedded in our EMR, but now we have a stand-alone application just in case physicians are not ready to adopt the full EMR, to get them started with e-prescribing.

We are active in 40 states, which means that we have physicians that are actively e-prescribing in 40 states. We are a long-time participant and supporter of NCPDP. All the prescription transactions, as you will hear from all of the vendors, are strictly script compliant.

A couple of things that we have learned in your years in the e-prescribing business is that doctors will adopt technology if there are requirements to use that

technology which exceed those for paper. So if the most common denominator is a piece of paper, we are not really arguing or fighting or discussing over which kind of technology to use. If the technology is more difficult than a piece of paper, we are challenged. So more challenge, there will be less adoption.

Doctors don't want to adopt technology if they have to use multiple systems for multiple purposes. That has been demonstrated again and again and again. One of the reasons why the e-prescribing never really took off in the early days was because the only thing we could use e-prescribing for was to get prescriptions to certain pharmacies. Physicians said, if I have to do some one way and some the other way, and I have to try to remember which is which, it is not practical.

We feel that price pressure, surprise, surprise, is pushing the price down, not up. So I am not confident that the opinion that it would be okay for a few more dollars to provide PKI encryption for example is valid in the marketplace. We have physicians frankly who could get e-prescribing for free, or they could be paid to use it through subsidy from payor or PBM. Yet e-prescribing adoption is still a pretty low percentage of the total. So we have to be careful about that little more statement.

The last point that I would make is something

that we have learned which is interesting. To us in the room, it is obvious what the benefits to electronic prescribing are. If you take the time to think about it, there are some definite benefits. However, on the surface, the kneejerk reaction is, the doctor says, I could use this to write a prescription, hand it to the patient, and I am done with it. That is pretty quick. On the other hand, I can pick up the computer, I can log in, I can do my thing, check all the warnings, send it electronically to the pharmacy, the pharmacy gets it, maybe they call me, maybe they don't. Tell me where the cost benefit is.

Now, we can explain the cost benefit, and all the vendors that are in this room are going to talk to you about the cost benefit, but it is not something that is obvious. That is the challenge that we face in the e-prescribing world. So layer on more complication, the business case becomes even less obvious.

I thought I would address a couple of the questions that were raised in the document that we received. In terms of the current risks and identifying them and how to address those risks, there are risks in everything that they do around prescribing. However, there is no security here. There is no audit trail here. So just by basis of having a computer and moving the data from point A to point B gives you an audit trail that

doesn't exist in the paper world.

A couple of the presenters yesterday made the point that we ought to just get started with existing technology and see what happens. If it turns out that there is a tremendous problem with diversion, and we don't think there will be, then we can implement additional security processes and procedures.

The risk for controlled substances and non-controlled substances, we believe that audit trail is going to be the same. We don't perceive that there are going to be any additional risks, and we certainly are prepared to address those.

It should be noted as it was noted yesterday, in those billions of health care transactions that we handle every year, there has never been a breach. We have not ever been investigated, We have not ever been asked for information. So it is not to say that it won't happen, because there is no question that it will. Criminals are smart, and we can only be half a step behind them, but nonetheless I think that as an industry we are in pretty good shape from that perspective.

Modifications. The way our system is designed today, because of the different variations in the state regulations, we take all controlled substances and we design them so they can't be sent electronically.

What that means then is that the physician can still write the prescription using the software to take advantage of all the drug interaction checking and formulary validation and those things, but at the end of the process, instead of being able to send it electronically, they are forced to print it. They sign it with a web signature and the patient takes it to the pharmacy. We have done that because we don't want to have to discuss with each and every pharmacy board each and every prescription in the potential, much less get the Department of Justice involved, and because there is a gray area, we just said, let's take the high road and say you can't do it.

Now, that being said, if we were to decide that we wanted to be able to use EDI for electronic prescribing, it would be very easy, because it would simply be a matter of one field, one character, changing it from N to I, and then positions could be used in electronic prescribing. I could do that in 20 minutes, it is not a big deal. It wouldn't require anything different on our part.

Opportunity cost is our biggest issue. This is not a technology thing. We are a technology company, so if we want to make this really complicated, that is great for us, because we can make a lot of money. We can install all kinds of fancy stuff and then sell it at a premium. That

is a good thing. That is the reason software companies are in business. But adoption, that is the challenge. If you build a lot of technology and nobody buys it, what value does the technology have.

We are concerned also from an opportunity perspective regarding the states. Each state has different regulations regarding transmission of controlled substances. The Schedule 2's are all the same, but with the Schedule 3's, 4's and 5's there are different regulations in each state as to what you can do with an electronic signature and whether they can be faxed or not.

We have been told by a number of state pharmacy boards that everyone is waiting for the DEA's mandate to then model their rules against what DEA says. We are very concerned that that will take the very rapid growth of electronic prescribing and grind it to a screeching halt if we make this regulation for PKI cross all prescriptions. I think that would be a bad thing in terms of adoption.

Again, I only wish this was a prescription tab, but of course I wouldn't be allowed to have one unless I stole it. But this is what we are competing with. The companies that are all up here on the stage today, we all have competing products, and we bump up against each other in the marketplace every once in awhile. But the reality is, we are not competing with anything except this. This

is what most physicians in the marketplace use.

Here is a little snapshot of our business. It has grown by four times since July '03. There are 3200 active prescribers in 40 states like I mentioned. Right now we are at about 350,000 transactions a month. Of those, just about 90 percent are new prescriptions, and 11 percent of those are refills.

What is interesting to note is, even after all of the connectivity that is in the marketplace is said and done, we are still delivering more than half of those via fax. So that just means that the pharmacy which the patient has selected is not yet enabled for EDI. You heard the folks from SureScripts yesterday talking about some of those statistics. There are a whole bunch of pharmacies that are enabled. That entire number is not yet activated. So this is just a little snapshot of the way our business works.

How our system works in terms of electronic prescribing is, we utilize the UEGA or the E-SIGN definition of electronic signature. We talked about that many times before. Our process for validating the prescriber is very, very similar to some of the other presenters. The prescriber contracts with us, they are credentialed and enrolled on our network. The user selects an ID and password which is used to authenticate them into

the system. They have a separate user ID and password that they use for network access. The prescriber is enrolled.

If we are using a value added network or another network throughout the prescriptions, the prescribers are also enrolled there. We also enroll the pharmacies to make sure they are legitimately able to receive prescriptions.

Each transaction in addition to all the information that is required to be a valid prescription, also carries a system generated serial number, a source system ID number, date and time stamp, the sending system ID, the prescriber's name and their identification number and internal sender ID, an agent name if it is not the physician his or herself that is writing the prescription, as well as the pharmacy ID. All of those we consider to be the indicia which validate that this is a true electronic prescribing from an authorized prescriber.

In terms of the integrity of the transactions, we use industry standards, 128-bit encryption, HTTPS, the same kinds of controls that are used in the banking and the credit card industry. Those are the things we are using today.

At the bottom is our policy. If a prescription doesn't meet all of the criteria and have all of the components that we have described, that long list that I just had, we reject the transaction as unsigned. We don't

know who that person is, and we don't consider that a valid prescription, and it never passes into our network for distribution to the pharmacy.

We believe that PKI, electronic signature standard, isn't really necessary, at least not right now. The current technology exceeds the manual process, which is this. The enrollment requirements are based upon independent verification, so we are making sure that the people that are signing up to use this are legitimate. The people that are signing up have HIPAA business partner agreements in place, so there is also a legal document that establishes a relationship between us as an EDI vendor and the prescriber. We have authentication protocols to access all of the applications. We use an encryption to move the data back and forth, and we have -- robust is an interesting word, but we have audit capabilities, and there are no audit capabilities in the manual world.

PKI clearly wants the message contact from the source to the destination, but it really doesn't do much to authenticate that the person that is entering the data is who they say they are. I know that I am as security conscious as the next guy, but in my company we have a requirement that you change your password every 90 days. I can't remember more than two passwords, so after I change it the second time, then I have to write it down, and that

is not really very secure at all. To be sure, that is what the physicians will do, because that is what they do with the EMR today.

What we counsel our customers to do is, treat your password the same as you would the prescription pad. So if you are okay with leaving this prescription pad in the waiting room on a table saying, write your own scripts, not a problem, then you are okay to share your password with everybody. But if you are interested in this, because there is a liability, this is the same as your password, so share it, and then you won't run into a problem.

There certainly is going to be some kind of a cost for PKI electronic signature. Because we are interested in the betterment of society, we are also not in this for a community service. So we would have to charge for whatever technology we implement. If it is complicated technology, it is going to cost more. If it is simple technology it is still going to cost something. As we said, price pressure is down, not up.

Today no state requires PKI. In fact, there have been a couple of states which have adopted PKI regulations, which have since rescinded them, because they were very, very effective. They were so effective, in fact, that nobody did any prescribing in those states because they couldn't comply with the rules, so the rules had to be

rescinded. Now we have e-prescribing, places like Nebraska are an example.

There is some question as whether the current standards that are used for electronic prescribing support what would be necessary for PKI. Things I'm told like the message digest don't exist right now, so those would have to be developed. There is also work flow considerations, some of the things that we talked about yesterday. Pretty straightforward to log in a prescription. If you have an extra process that you need to do just to do controlled substances, that is challenging for the physician because we are competing with this. It is pretty easy to write something down and hand it to the patient. It is more complex if you use the computer.

We are very concerned about slowing the adoption of electronic prescribing. Somebody mentioned yesterday about the hockey stick. We are finally getting to the point where we are on an upward trend, and physicians are really beginning to adopt this, and we don't want to throw a barrier in there.

There was also an opinion that PKI requirements could render VANs or value added networks unusable. PKI is ideal if you are sending an transaction from point A to point B. The reality of the way economic data interchange works is, there is a central function or a clearinghouse

function, so all those prescriptions, whether you are using SureScripts or Metavonts or even our network, most prescriptions go from the prescriber to our network, and our network then sends those transactions out to each of the pharmacies or perhaps to the pharmacy hub and then to the pharmacy. In order for us to do our job, to reformat the data, to accommodate the different pharmacy needs as well as the different versions of NCPDP script that are in use, we have to open that transaction.

If you wanted to use a point to point connection, which is certainly possible, then you would have to build that capability for every practice, every physician, to communicate directly with every pharmacy. One of the folks yesterday mentioned that CVS has 5,000 stores. There is nobody that is going to be interested in supporting or maintaining a direct connection between every prescriber in every one of those stores. It is impractical.

That is the reason that a clearinghouse is in existence. Back when a clearinghouse was a popular word, that was when we were a clearinghouse. Now we are an EDI network but guess what, we're a clearinghouse. So it is a valuable thing, and it is still in existence. With all of the doom that was predicted with the HIPAA regulations, we carry more transactions today than we ever did.

We would recommend that regulations comply with

the definitions of the E-SIGN act for electronic signature. Utilize industry best practices for credentialing and currently deployed authentication processes. We would certainly want the ability to utilize an EDI network. Frankly that is the business we are in, but even if we weren't, the logistics of moving the data require an EDI network. We are comfortable because we already are in compliance with the HIPAA requirements. It would be great to identify a minimum set of indicia to identify the electronic signature so that the pharmacist won't have to think, if this one comes from Emdeon I've got to look for this stuff, it this one comes from DrFirst or one of the other vendors, it has to look like something else.

Also, the most important part of all this is that the pharmacists still review all these things. So the pharmacist's obligation is to make sure that that is an authentic prescription. So even after all this technology, the pharmacist still gets involved as the final human check to make sure that the prescription is safe.

We believe that the standards should facilitate the transition from handwritten to electronic signatures, not hinder that process. To sustain that transition, we want to avoid adopting technology specific standards that would make e-prescribing more burdensome than the paper process. This is a piece of technology that is very cool.

It is timeless, and it is really easy, and it works. A hundred percent of providers prescribe this way today. So this is what we are competing with.

That's it. I am Mike Burger. I am based down in Tampa, Florida. There is all my information. I welcome your questions at the end.

MR. CAVERLY: Has Mr. Chen joined us?

DR. CHEN: About a year and a half ago, I was thinking NCVHS was right -- Michael Burger. In fact, I was saying that after he said it, I don't have to say anything other than ditto.

Last night I pretty much revamped my talk this morning, because essentially the speakers yesterday were really eloquent, they were convincing. I thought what I have to offer is very little other than what they said. However, I think it is useful for me to point out a few important points in my talk.

My name is Jim Chen. I am the CEO of DrFirst. I am the founder and the CEO. DrFirst was founded in the year 2000. We are an e-prescribing company. We have won many prestigious awards. We were also recognized as the health care IT technology vendor of the year 2005. We have also been the -- producer as recorded by SureScripts since they began recording such ranking. Currently we have about 400,000 to 500,000 prescriptions per month.

I am very proud of DrFirst's record in successfully pioneering in e-prescribing. We take those seriously since the inception of our company.

Prior to this role I funded Newman Corporation, a virtual open network environment. It was a pioneer in -- technology. When I took the company to IPO in 1996, I have to tell you that the technology is really an extension of -- we were using PKI and smart card as a basis of our fundamental technologies, so I know one thing or two about PKI and smart card.

One thing industry does not want me to do is to make it so hard that no one else can do a good job, but that is not my intention here. I would like to point out that in the SAFE BioPharma, in the document somewhere is stated that it is best for PKI to be implemented in a closed system environment. As you know that is not what e-prescribing or e-health network today is using. It is a prerequisite to have a very good implementation of PKI and smart card technology in closed network. Open network it could be done, it could be very expensive.

A few points I want to share with you regarding patient safety and adoption of electronic prescribing, and PKI and smart card, I'll talk even more about it, and fraud and abuse.

Electronic prescribing has already proved itself

as an efficient way to increase the patient safety and reduce hassle factors for all participants, improve formulary adherence, reduce costs and allow many functions to be added to enhance health care efficiency -- who has reported significant improvements for their constituents, the three major auto and their employees, has consistently spoken out about their positive experiences. Today nearly 100 percent of the prescriptions are being routed through an e-prescribing system, now going to schedule five, still has prescribed and then printed. I was told last time that they are anticipating the first one million prescriptions going through the system in the very near future.

Here are the points about the advantage of e-prescribing. One of the things that I will discuss further in a later point is enforcement, where enhanced data collection and audit trails are recorded.

Few would argue that electronic prescribing in a system such as we have will improve patient safety, prevent medication errors and save money from patient to payors.

Unfortunately, the practice -- to write prescriptions for controlled substances, especially schedule two to -- two different workforce, one to send prescription and the other to print out prescription for a web signature, along -- that transmission of prescription, not just a subset, where -- for medical practices, which

will then improve the adoption and further improve patient safety.

In addition, security of prescription for controlled substance will increase with electronic transmission using current security measure, further enhancing patient safety. We believe that using electronic prescribing for the controlled substance will improve the ability of law enforcement to track fraud and abuse almost instantaneously.

On the adoption side, I would like to share with you that to date, there are probably no more than five percent of prescriptions are going through the current electronic prescribing system, of which as you know 11 percent or 15 percent are to be done in what I call the paper method.

Just imagine, if you had a physician where you used an e-prescribing tool, you had to deal with those two methods. It is almost like the cell phone technology adoption. If the cell phone technology works 85 percent of the time, you can imagine how difficult it would be for you to pay for a system that does not really work 100 percent. Similarly for the technology adoption.

There are many companies ahead of my company who struggled for the last seven, ten years, and did not make it to this point. Part of the reason is the adoption issue.

At this point I want to share with you a little bit on our security method. All transmissions we have with our clients are encrypted. It is pretty much the same as what you heard from previous presenters. We use the SSL over the web. We use triple dash encryption for the RPDA solution over the air. Every user, whether prescriber or nurse or medical assistant or front office staff has a unique user name and password. The system time out for inactivity and prescribers have a separate PIN code used to digitally sign for the prescription, which is signed with our server sign PKI key.

The system time out for inactivity, and prescribers when they use the PIN code for signing insure the non-repudiation part of the prescriber. Transmission to our connectivity -- such as SureScripts and RxHub occur either over secure lease line or via a VPN. This particular security setup has certainly some issue about non-repudiation, because the server sign-in is not as good as an individual user having their own private key. However, at this point the check and balance in the current system by way of an authenticated user using this unique ID and password and separate PIN for the physicians is rather strong as we heard before, and with proper check and balance we think this can work in converting the schedule two to schedule five drug prescriptions.

Another point I want to make is that it is unlikely the e-commerce system, for example, the 24-hour Internet banking, which is done on the Internet without human intervention. All data can rely on password and user ID, as compared to the case of e-prescribing. At the end of the transmission, you have a pharmacist who will validate the patient and the physician to the best of their knowledge. So it is by far much better than the Internet banking type of system where today many millions of dollars are moving through. Including a human intervention e-prescribing system will be more likely to catch abuses of the system, much better than other systems.

Very quickly, I will talk a little more about PKI and smart card. We heard about the different level of authentication methodology yesterday from NHIT. But one important point is, you cannot go level three right now. I really would like to appeal to you about that part. If I remember correctly, level four is the one with the smart card. In the PKI system, the private key is the essence of the entire system. It is not a public key, it is not a certificate. Always remember, it is the private key.

The protection of the private key is paramount in the entire system structure. Just imagine having your private key sitting in the PC on notebook computer, can you imagine how much exposure that would be, especially in the

diverse environment of physicians' office. Virus or other intrusion software could easily poke into it. So you have got to have a smart card if you ever choose PKI. Just remember that. I want to emphasize that.

I mentioned earlier about PKI system really needs a central authority to manage the system. I think that the examples we heard yesterday, some other countries have advanced a lot more in this area, e-prescribing. It is because they have probably a very central control authority there.

We heard about the NCPDP testimony yesterday, that they had a project in this area. So was ANA. ANA tried with Intel for years, and that project could never really get to where it intended to be.

So remember, a closed system and open network is to major issues to consider. If want to make PKI work, you have got to make sure it is a closed system. Someone has to be truly in charge.

My last point on this slide was quoted from a statement made by NIST network security architect. I don't remember the name, but he said in his testimony last year to NCVHS, he said tread lightly. He was talking about PKI technology. So this is one person, when I read about his testimony, I thought it was very important, very enlightened.

On fraud and abuse, I think it is well known that the system is a real time network as it is right now. So the transaction go from the physicians or the nurses and all that, those prescriptions will have to go through a lot of login process and auditing, log in the data, the records, throughout the steps from us, from the vendors to the SureScripts network or RxHub network and to the pharmacy. There is always a well documented record of who gets what, so on one can dispute that they did not receive the records on that particular time as such and such. So it is a very good record, so it is very easy to do real time monitoring on fraud and abuse.

You could even say that if there is on patient who has been prescribed a particular drug in multiple locations in approximately 24 hours a week, the system can tell you that immediately. So you can imagine how much you can do with even today's system. So I think with careful examination we could have a system that really made that happen.

At this point, I just want to conclude that -- please consider the balance between patient safety and security. Electronic prescribing will improve patient care and reduce medication error, increased capacity will reduce adoption. We would like to highly recommend DEA and HHS to seriously consider to move the current system forward with

some fine tuning and adjustments according to what is needed in order to do a good check and balance. That way we can open the floodgate on e-prescribing and e-health care.

I think this is something the decision makers can be very proud of, because you are the decision maker at this juncture to make this happen. This is going to be a legacy for all of us. Someday you can tell your children, your grandchildren, that you at that point made the right decision to move this forward.

Thank you for holding this important meeting, for inviting me to participate. We at DrFirst are grateful for the work done over the past several years by DEA and HHS, and especially NCVHS and by Office of National Coordinator to promote e-health care and to work on answering these tough issues along the way.

Thank you.

MR. JOHNSON: Thank you very much to everybody for coming to what we all agree is a very important meeting. Thanks to DEA and HHS. I would feel remiss if I didn't copy everybody else in saying that.

Before we start, let me introduce myself. I am Nigel Johnson. I am the V.P. of business development and product management for Zix Corp. Zix Corp you may also know as Pocket Scripts. In July of 2003 we bought the

company Pocket Script and have since taken it what we believe are great heights, and continually growing heights.

I like Jim started out in PKI. When I first started working I worked in military security. Worked on military cryptographic systems, and then I joined a company called Entrust, which built PKI software. Entrust is the largest software provider of PKIs in the world. We built that company up to over $100 million a year in sales. I was the V.P. of product management there, and I like Jim know PKI very, very well. I am very comfortable implementing it, and like Jim, if we were asked to do it, we would probably be the two leaders in the field, because we would be able to do it faster than anybody else.

However, as you will see as we go through this presentation, I believe that it would be a burden that would not be good for e-prescribing. We will go through the details of what we do right now for security and for securing the connections between our prescribers and between us and the pharmacies, and give you a good sense of why I feel PKI wouldn't work and the system works well today.

Just a couple more minutes on Zix Corp. We actually have two businesses. We have the business of encrypted e-mail for regulatory compliance. Our strongest customer base is in the health care industry. We secure

the e-mail between health plans and doctors, lawyers and doctors, between anybody who is running claims.

When we take a look at the size of our market in e-mail alone, I just want to talk about e-mail for a sec, we have insurance companies with 80 million covered lives using our system to communicate with their patients and with their doctors and with the hospitals. We know security very well.

We have moved into e-prescribing because we believe that an electronic prescription is taking a piece of data that is confidential and moving it from one person to another person, and doing that with great competence and integrity.

I want to make sure that it is clear to everybody at this point, and everybody said it before, nobody uses e-mail for e-prescribing. They are completely different systems. But that being said, both our secure e-mail health and our e-prescribing system sit in a data center that we own. It is a $50 million data center with four levels of security to get to it. The only way to get to the heart of that data center is to have biometric access, badge access through a video recorded system, and only a few people can get in, and no single person can get in by themselves. They always have to be escorted by another person, even if that person is up here.

In the e-prescribing world, we did 1.3 million electronic prescriptions last quarter, so over 400,000 electronic prescriptions every month. That continues to grow as the number of doctors that use our system grows.

Our data center itself, for the number of transactions it does, it did 350 million transactions last year. So this is a big data center, a lot like Emdeon. We have a lot of message flow, and we have to have a lot of security around that to make sure that there are no breaches, and we have never had one.

This is just to make sure that everybody is on the same page when we talk about electronic prescribing. This diagram pretty much applies to everybody, and it is also similar to the diagrams we saw yesterday. Doctors, nurses, MAs all have unique IDs on our system, and they connected to us over an SSL connection, secure sockets layer. It is an authenticated connection, every user authenticated every time they get access to the system.

Prescriptions are then sent to our central data center. Secure connection down to either RxHub, SureScripts or any other network vendor that we are using. All the connections are encrypted, all the connections are authenticated.

Let's talk about the risks as we see them. I think we are all saying the same thing. There is a risk of

unauthorized access to private health information, and there is a risk of unauthorized prescribing.

We address these in multiple ways. We follow the second set of recommendations on e-prescribing standards that came from the NCVHS. I believe that those are a very good set of recommendations. On top of that, we have two security audit processes running on our system. One is the SASS 70 type two audit, and the other one is the AICPA CIS Trust audit. These systems are intended for companies who handle sensitive information, PHI or any financial information. You will see any data center that can manage and see that information going through these levels of certification.

We are audited every year by a big four firm. Last year the audit was finished in April of 2006, and it was done by Deloitte and Touche. So they check for the security of our system, can anybody get physical or electronic access to the system. The answer is no. All the policies are in place, all the procedures, all the controls, and they have audited all of our controls and done their tests.

Is the system always available? While we have been talking about security, it is an important point. As Mike kept saying, I wish I had his little pad, a piece of paper is always available, and an electronic system if

somebody is going to use it for e-prescribing, it needs to be available all the time. That is one of the tasks that is done here.

Processing integrity. Michelle asked very rightly, how do we know that the prescription didn't get changed. It is that processing integrity that is tested by both SASS 70 and CIS Trust.

Then of course, confidentiality; let's make sure nobody is looking at the records who shouldn't be looking at the records, so that we can have confidence that people who are using electronic prescribing are not gathering data that can be then used on patients in a way that is not appropriate.

We don't believe that the risks around e-prescribing increase if we are doing electronic prescribing for controlled substances. Specifically here, I mean for schedule two. We do do electronic prescribing for schedules three through five in the states where it is allowed. I think it was Mike who was talking about this. We would certainly prefer that there was harmonized rules across the states, because every time we go into a new state, we have to adopt new rules, and say in this state we can't and this state we can. It is our belief that doctors -- it is not just our belief, we see it because we work with thousands and thousands of doctors -- that they want a

system that allows them to do e-prescribing for everything that they do. They would like to have the control of being able to keep their records in one place, be able to get all of the data that they need to check for patient safety in one place, and they would rather than have all the drugs in one system than have them split.

It is quite something. I have actually not met Mike or Jim before, and we are all three saying the same thing. We believe that having audit logs, being able to actually look at the prescriptions electronically is much better than doing the recurrent written system. We all know, pads can be stolen, prescriptions can be changed on paper.

But the thing that I think nobody else has said, and I will look for their nods to see if they agree with me, that one of the advantages of electronic prescribing is preventing the fraud. If someone has stolen the pad or has copied pads and is scarping prescriptions around the different pharmacies, you can't do much about that. But if it is electronic, you can say here is a practice that is writing something that we don't agree with. You can come to Zix Corp and say, please stop, don't let them do that anymore while we investigate, and you have instant stopping of whatever is happening there, and they would have to be resorting to paper while you are doing that investigation.

So in our minds, there is no need to change our system to be able to prescribe controlled substances.

Authentication is the most important part. It is the foundation of anything you do with security, who is getting access to the system and how do you know who they are.

When we sign up doctors, we go to the doctor's practice. We visit the practice. We walk them through what the benefits of e-prescribing are, and then they sign the contract with us as we are there. We get their DEA certificate. We validate that they have an active DEA certificate, so we have that real connection in person, face to face with the docs when they join our system.

Just like Jim and I'm sure like Mike, doctors, nurses, MAs all have different levels of authority within the system. MAs can change demographic data, that's it. Nurses can write prescriptions, then those prescriptions are electronically sent to the doctor within the system, where the doctor reviews them, and then it is the doctor that is sending the prescription, that is putting their signature on the prescription.

So just like in the real world -- sorry, I am in the real world, just like in the paper world, where the nurse will pull a chart, take a look and see what they recommend the prescription to be, and then put it on the

doctor's desk with the stack of charts, it is the same thing, just done electronically with the doctor in the end taking the responsibility for the sending of the scrip.

Passwords are forced to be complex. Nobody can type in ten or simply do their dog's name or their license plate number. It has got to be ten characters, it has got to have a capital, it has got to have a special character and you have got to have a numeral. Doctors are trained, don't ever leave this out. Like Mike said, pad, password, same thing.

We have a three strikes policy. This is something that I think is a very, very key point when we are talking about authenticate and security. If you have a piece of software that runs by itself and somebody could have unlimited access to that software and they keep trying new passwords, that is not a very good system. But when you are logging into a centralized system that is monitoring how many password tries were there, after three tries, that's it, no more access, you're done, and it is logged that somebody was trying to crack into that particular account. When, as occasionally happens, doctors forget, there is a process for them to be able to reset that password. But that whole process is logged to keep track of who the doctor was, what the process was for resetting it, and who were the people within the company

who did that resetting.

And of course, as with all -- Mike talked about, every connection with our partners is authenticated. We check and make sure that we are going to the right IP address, just as they are making sure they are receiving information from the IP address. Plus, we have authentication controls on top of that.

So our prescription records are protected by policy software and geographic separation. By policy, I mean we have specific rules on who has access to those prescriptions. Only doctors can write prescriptions -- I should say prescribers, not doctors. I have trouble with the word prescribers because it is not in the dictionary yet. Maybe we will change that soon as we keep using it.

All of the prescriptions have a unique code put against them. They are all logged when they were entered. There is a CRC redundancy check. Every day our prescriptions, copies of them, are sent to our remote backup site, so that there is geographic separation between one site and the other. So even if a change was made here, we can see that by checking against the remote site.

The data center, 24/7, on the fourth level, only two people at a time can get in it, never one single person. All of the staff have background checks, biometrics. It is the most secure data center system that

you can get.

This is probably because a good part of the company -- a number of people that work at Zix Corp now come from a security background. We build secure systems. We had in mind eavesdropping, impersonation, hijacking when we built the system and put it together. We don't see any threat from that right now at all. On top of our own personal integrity and what we have put into it because of our experience, we also have all these controls forced on us by CIS Trust and SASS 70.

Lots of talk yesterday about smart cards and PKI. We can do it. It can be done. In fact, the technology is not that hard. Crypto is not super difficult if you spent 15 years doing it. What is really hard is getting it deployed across three people in the chain, actually four: The doctors, the point of care vendors, the networks like RxHub and SureScripts, and then each and every one of the pharmacies. So you have got those three, if you count the doctors four people in the chain. Then you add in each one of those all the different levels of browsers, all the different kinds of operating systems, then all the different software systems. So you have got -- I think there are 40-odd e-prescribing vendors. There are five networks. I can't remember how many -- in fact, I don't know how many unique pharmacy systems there are, but I

believe it is somewhere above 50 unique pharmacy systems spread across all of the different pharmacies. To get all of those running on PKI so that they can all do this form of electronic trust would take a huge, huge effort.

We heard from Jim and also from Safe Biopharma that closed networks work best. I agree with that. I don't know of an open network where the cross certification of multiple CAs has ever worked in private industry. That is what we are talking about. Every doctor's office is a private industry. All the vendors are private, the networks are private, and all of the pharmacy chains and independents are private. So to put together a PKI that works across all of them, it is a glorious dream. It is something that I have believed in for 20 years, but it is not a dream that we can achieve in a short period of time at a low cost.

So in conclusion, allowing for electronic prescription of schedule two drugs will speed the deployment and adoption of e-prescribing, adding complexity with something like PKI versus using audits for controls would certainly slow the adoption of e-prescribing.

Thank you very much for your time.

MR. THOMAS: Good morning. My name is Russell Thomas. I am the Chief Executive Officer of Gold Standard, based in Tampa. Like my fellow presenters before me, let

me thank the DEA, CMS, HHS for bringing us here today to discuss this very important topic.

As with most chief executive officers, with the exception of Dr. Chen, I very quickly get lost in the technology. So what I want to talk about a little bit today is policy, policy would what DEA is trying to accomplish, a policy based upon some real life experiences that we have had in Florida over the last three years, and why from our view it is important to provide for standards that will support the adoption of e-prescribing quickly, and not impede what is I believe a very quickly fast-growing business, fast-growing acceleration of better health care, and the creation of significant opportunities for law enforcement to be proactive instead of reactive in identifying fraud and abuse in health care and prosecuting them. We all know that fraud and abuse cost us as taxpayers a tremendous amount of money.

We know in Florida, for example, in an audit conducted by the Attorney General two years ago, that the state of Florida estimated that in at the time a $12 billion Medicaid program, roughly $1.5 billion annually was lost to fraud and abuse, of which $300 million is in pharmacies. We also know that in the three years since we have implemented our program in Florida, which is both a prescription program -- although prescription was step two

for us in providing clinical point of care systems for high prescriber Medicaid docs, but that in the three years that we have had that in place, the state of Florida has determined that it is saving roughly five to one in return on investment. It has been documented that the state has saved $50 million in the last two years alone with this system, and we believe that a tremendous amount of that is from reduction of fraud and abuse in the prescription system in Florida Medicaid. I'm going to talk a little bit today about how we got there.

So if my slides are ready? A little bit about us, about Gold Standard. We are Tampa based as well. Mike and I were not on the same plane yesterday because I didn't get in until close to midnight last night. He was smarter than me, he came up early. But we are Tampa based. We have been around since 1993.

Our core competencies a company are in clinical information, drug information in particular, databases and clinical applications to support those databases.

Our staff experience, if you look within our employees, we are a company of pharmacists. We have roughly 25 doctors of pharmacy on staff. We develop all of our own clinical content. We develop all of our own systems. We have masters of public health. We are also a technology company. As I said, we develop all of our own

systems in house.

We are now a wholly owned subsidiary of Reed Elsevier. Reed Elsevier with its Elsevier division is the largest provider of health information in the world. We do roughly two and a half billion dollars a year of business in providing health information throughout the world, in over 72 countries. So within our company we have a lot of competence in delivering health information, supporting systems and providing data feeds and data flows across multiple networks.

This is just a snapshot of who our customers are as a company. One of the perspectives I think we bring to this presentation, and perhaps your thoughts as the DEA on how to move forward with this, we really represent a broad base of health care providers. So as we will talk about a little bit today, our systems are in use in Medicaid organizations. We sell to the public sector, the state of Florida and the state of Mississippi both use our medication management e-prescribing solutions throughout the states. We are in over a thousand hospitals in the United States, using our drug content and systems within those hospitals. We sell into managed care environments.

We also sell into retail pharmacy. That is one of the perspectives I want to spend some time talking about today. At the end of the day, the way we feel about this

is, you have to let the pharmacist practice pharmacy. Imposing standards on for example PKI and other things that are going to make it more difficult to adopt e-prescribing we believe is detrimental to that process.

So that is a little bit about who we represent and the customers that we have in health care.

What we will talk about today is our point of care clinical decision support software. We call it Empower. That is our system that we built in 2002 with the state of Florida. One of the unique aspects of our product is that it was built in very close collaboration with a large system, that being Florida Medicaid.

What we do with that system for the state and for other customers is, we deliver an application in a secure environment that provides real time patient histories to the physician. It provides formulary data, and it also provides e-prescribing functionality.

One of the other things we do with that and what has been of real value to our customer is, we provide what we call fraud and abuse and management tools to the state. On the front end, we provide our physicians with the ability to message to the state when they identify a patient in their office that they believe is committing a crime, that has a suspect medication record that they believe requires a view. On the back end, we provide audit

functionality for the state to be able to go in at any time and filter the results, look at the cross results to be able to say, show me for example patients with more than two scheduled narcotics prescriptions written in the last 30 days, show me patients with drugs that interact that if these prescriptions were really being taken by this patient, would cause a severe adverse effect, and therefore we think there may be a reason to look at how the patient is using these medications.

This has been an award-winning program that we have delivered. It has been cited in the Pew Report, which looks across the country at successful programs in Medicaid organizations. It is one of the premier programs in the country for improving the quality of health care as well as providing the state with a product to reduce fraud and abuse in their Medicaid system.

As I mentioned, we are doing that today in both Florida and Mississippi. In Florida we have 3,000 users of the system across the entire state. In Mississippi we have 225 additional users of the system across the entire state.

How do we do this? The devices provision -- again, I heard some of the other folks talk about this, but we do face to face provision with our providers. It is provisioned and delivered by an Empower trainer, one of our own people, who goes to the physician's office, collects

their DEA number, collects a copy of their medical license, records all those documents electronically and provisions them there at the point of care. User name and password is then authorized and made available to the physician. Like the other vendors, we have different levels of authorization within the physician's office, so the physician will have a different level of authorization and a different user name and password from the assistants at the front.

We host our system with Verisign, based out of Atlanta. Again, it is a SASS 70 compliant facility, meets all the requirements for HIPAA regulations.

How do we handle that? As I mentioned, the provider presents a signed, notarized agreement along with a copy of their state identification and medical license. A medical license background check is performed. We do that through the department of health in both Florida and in Mississippi. Then the user name and password is entered and authorized for use.

Again, a little bit about the policy from our perspective. Where we really see the opportunity for DEA here is to accept the standards that are in place today. As I think the other vendors have recommended, to go with what is in place today as far as the systems that are available, and to essentially allow us to open the pipe and

make e-prescribing for controlled substances available just as we do with all other substances.

We believe that this will create great opportunities for savings, for criminal enforcement, for audit functionality, for you and other law enforcement agencies around the country. We absolutely believe that technology is a key to your success, and that the functionality that will be made available in infinitely superior to what you have today with the paper process.

We use as well on the authentication side, true factor authentication, strong password policies. We will talk just a little bit about non-repudiation. We have heard a lot of talk about PKI. We use it on the front end of our system, so coming out of our e-prescribing application to our central data center we use PKI. Candidly, we built it because of you. We didn't know at the time we were building it what standards might be adopted.

We do not believe that it is a necessary standard. I agree with the other comments up here that for us to do it from the device to our central server, back to our home server, is one thing; to then though expand that from us out to SureScripts or RxHub, then to the pharmacy and back, is a very, very complex process. As we have looked at it and evaluated it, we just absolutely do not

see the benefit to doing that. We certainly see that as a detriment to the overall adoption of e-prescribing.

From our perspective, in conclusion, we agree with -- it is probably good that I went last, because I got a chance to see what our competitors think. I do believe we are all singing off the same song sheet here. We believe that e-prescribing presents a tremendous opportunity both to improve the quality of health care, but also to provide a tremendous law enforcement tool for you and for other law enforcement agencies to track down and crack down on pharmacy fraud, medication fraud.

We actually have documented cases in Florida where that has happened. We have cases where doctors have identified narcotics shoppers, for example, have reported those to local law enforcement, and they have been arrested and prosecuted as a result of the data that has been made available to the physician and then to the state on the back end, through our system in real time, not 90 day retrospective data, but real time data made available to investigate and prosecute fraud. It is not infrequent that we get calls from local law enforcement agencies around the state saying, we are investigating this case, can you help us, is this one of your physicians. If so, we put them in touch with the state. They cooperate with the state to do research and background investigation on those physicians.

Thank you. Appreciate the opportunity to be here.

MR. CAVERLY: Once again, I just wanted to thank our panelists for adding their perspective to this discourse. I appreciate the time and opportunity that you have presented us with your presence.

We have entered the time in our meeting where we will have questions asked by both the DEA and HHS personnel who are here. So if I can try to balance off yesterday, we will start off with DEA, if you have some questions for our panelists, please.

MS. GALLAGHER: Good morning. I am Kathy Gallagher with DEA, liaison and policy. Unfortunately, all the panels yesterday pointed the fingers at you all to answer some of our questions, so that is what I am going to do. Some of them will be repeats, but I really appreciate your input.

As you know, DEA is mandated to protect the public safety. That is how we look at every issue. Every issue we have to deal with, we have to look at the public safety. So that is the framework from which we work.

What I hear here today or yesterday and today is that cost is critical, cost is an important issue. I'm not naive to think that that isn't important. But what are the costs? I don't know if you all are willing to go there,

but I would like to know down to the individual practitioner, what would their costs be generally speaking for the current system that is out there now, or a system that has smart card or dual factor security?

I don't know who wants to jump out there. I know it is a tricky question, but I need to get a feel of what is the difference in the cost.

MR. JOHNSON: I'll start, and then let everybody else start to fill in. It is a complicated question, because it is not just a simple matter of putting smart cards down at the doctor's level. The typical cost based on my experience from putting together PKIs, if you were to just do that, it would be in the couple of hundred dollar range. But that is just to say, this is the doctor, and identify the doctor.

A lot of what was talked about yesterday was, we would like a signature on the prescription that then flows through each of the different systems, all of the way down to the pharmacy level. That cost goes from a couple of hundred dollars for each doctor, then you are talking about millions and millions of dollars for the upgrading of all the systems of each of the vendors, the delivery networks, and then the pharmacy chains. So millions of dollars each. That is from my experience in putting together PKIs.

MS. GALLAGHER: That is not for the doctors.

MR. JOHNSON: No, no.

MS. GALLAGHER: For the whole system.

MR. JOHNSON: But remember, in the end somebody has got to pay for that. So out of the e-prescribing system, money comes in, money gets spent, and now more money is being spent, which means more money needs to come in. So those millions of dollars that are spread across all of the vendors' value added networks and SureScripts in the pharmacy chains, that has got to come from somewhere.

So it is not as clearly visible as when we said a couple of hundred dollars for the doc, but out of the system these -- well, look at all the systems. I hesitate to say a really big number, because everybody is going to point at me afterwards in the public record and say, he said this. I don't know how many tens or even hundreds of millions of dollars it would cost to do every system. That money would have to come from somewhere.

MS. GALLAGHER: In comparison to what a doctor is paying now, what does it cost a doctor now to use the technology that you all support?

MR. JOHNSON: Did you want to take that one? Because I've been talking a lot. I can keep going.

MR. THOMAS: Don't disclose any trade secrets. We didn't all sign the form when we came in, I guess.

My perspective on it is much like Nigel's, but I

think you have to look across the network of folks that will incur costs if this happens. Let's talk about retail pharmacy for a second. Retail pharmacy operates on very thin margins as it is, on the pharmacy side, and it generally gets squeezed year in and year out by states in their reimbursement costs and dispensing fees as it is.

I think any cost to retail pharmacy -- because it is going to be an unfunded mandate. If you require PKI across all sectors, you are going to say to retail pharmacy it is going to have to spend millions of dollars to do it. I don't know how many millions, but it is a lot, to do it, and we are not going to provide any additional dollars for you to be able to do that. So what will happen is that they won't.

Retail pharmacy at the end of the day has the discretion to accept an electronic prescription or not, and they simply won't. If they have to install PKI or some other form of higher security at this point, it won't happen because they are not making enough on electronic prescribing at this point.

I love the fact that the industry is growing the way that it is, but it is not growing fast enough to really justify the cost that they have already sunk into making electronic prescribing systems available.

It is going to kill the adoption -- I mean, my

view is that it will be a tremendous detriment to e-prescribing across the network, because our doctors -- to answer your question specifically, the physicians in Florida and Mississippi don't pay anything to use the system. It is funded by the states. It is funded by the states because that is where the return on adjustment is derived, by the states, and saving in fraud and abuse and prescribing errors and medication costs.

We have documented year in and year out that physicians using a system like ours, and I think it is probably true with all of those, but in our particular case, physicians using our system write roughly fewer prescriptions per month than physicians not using it. That is where the state saves their money. That is a combination of eliminating medication errors, so eliminating duplications of therapy and other things like that, and weeding out some of the rampant fraud and abuse that unfortunately you find in health care, particularly in Medicaid systems.

So it is a very large cost, and we have had to look across the entire network, and one that I believe the industry can't accept at this point.

MS. GALLAGHER: And I am not technical at all, I can't even do my VCR. So what you are saying is, the doctors right now aren't incurring a cost. So with PKI

would that change? Would that differ? It seems the costs are at another point. It is not at the practitioner.

MR. THOMAS: Yes, but we are going to pass it on. If we as vendors have to incur the cost of adopting PKI, then we are going to pass that cost on to our customer whether it is the individual physicians from my colleagues that sell to individual docs and to physician systems, or whether you are selling to the payor. That cost is going to get passed along.

Remember, that is one piece of the overall cost puzzle as you are looking at it. I frankly don't know the answer. I know some of the retail pharmacy guys were here yesterday, but my guess is, they don't have the answer, either. If they are required to adopt PKI for the electronic prescribing standard, who is going to pay them to do that?

MS. GALLAGHER: I think DEA's role is to set the standards. We are not trying to drive the technology, that is not our purpose, so I appreciate your honesty.

What I heard yesterday was, the barrier to doctors is cost. That is an important issue. So I wanted to see if that is true.

MR. THOMAS: If I could, I am compelled by your statement though that DEA's job is to protect public safety. I am very pleased to hear that. I would argue

that with the goal of protecting public safety, the proliferation of e-prescribing and e-prescribing in controlled substances is a benefit to public safety, whether you look at that in terms of being able to capture those transactions in real time on the front end, to do DUR against those, so to look for drug interactions and duplications and other things that you lose when the doctor puts down the electronic system and picks up the paper system, or whether you are looking at the overall cost of health care.

Part of protecting public safety, I believe, is insuring that we have a health care system that we can afford. The more we do to expand costs in the health care system, the less likely that everyone is going to be able to afford health care.

MR. BURGER: I'll just add one thing. All of our models are a little bit different in terms of distribution. For the physician or the prescribers that are using our software, every one of them pays. We don't have any subsidies available from PBMS or payors or a variety of other things. They are paying between $20 and $60 per doctor per month for use of this, not including the hardware, but just for the software and the network access and so forth.

As I said, price pressure to us is down, not up.

Frankly, if you can't justify using something like e-prescribing for less a dollar a day, we still have less than ten percent of our customers that are using e-prescribing even at that very nominal cost. So even if it increases by a couple of bucks, that is significant, because price pressure is significant in our market.

DR. CHEN: Obviously that is a very difficult question to answer. Let me try and answer the second one first.

We actually have two models. There is the retail model where the physicians pay. We usually charge them around less than $1,000 a year, so that is similar to what the cell phone cost is.

If a particular program such as payors, Blue Cross Delaware, Blue Cross Maryland, there are all kinds, Blue Cross Massachusetts, they pay physicians for us to run the program, which we then distribute systems. I think Zix is doing a similar thing. So it is sponsored by payors, because the benefit for patient safety and others has been proven real valuable to them.

But the physicians actually pay by participating. It is very painful. You heard me talking passionately about this 15 percent of prescribing process need to be done the old way, and it is painful, because they are a centralized type of operation. They can say all my

physicians must use this. But like one or two physician practices, it is very, very difficult. They already are operating on a very small margin.

I'll just tell you one thing. My son defying my recommendation changed his major from business into medicine to do the primary care. That is the people I am looking at. They really are in need of help. It is very hard for me to quantify the real costs or the pain that they have to bear for this additional burden.

Back to the first question about the costs, in this way. Yesterday we heard two testimonies that link to this. We heard about how impressive that Johnson & Johnson was able to get 70,000 employees use the PKI type of technology. I would be more impressed if we can say if there are 70,000 practices, one or two physician offices have adopted PKI technology from different vendors with different network behind them, that is the most impressive thing to do. Very few people can say that.

My company was the one chosen by NSA in '94 to do the -- it was very famous, everybody knows it, for the electronic e-mail protection. So we know that technology real well. That piece did not go very widely adopted. For what reason? It is very hard to manage, even within a centralized control, management's infrastructure, it is very expensive. So I cannot tell you how expensive it is.

Can it be done? Yes. If today the federal government says we take control of this, I will put my hand up and say, I endorse it, because that will work. But you have to be able to put the equal across all sector of the industry in order to make that happen.

MR. JOHNSON: It is very interesting as I step back and listen to what everybody is saying. We keep saying no PKI, let's not do that. I don't think that once has the DEA come out and said, we are thinking of PKI. Did you ever ask for PKI?

MR. TRENKLE: No.

MR. JOHNSON: So the two people on our left and our right haven't asked for PKI. Somehow it has come up, and everybody is saying that is scary.

Perhaps what we need, and I would look to both sides of the room, is for you to tell us what you think we need, not a technology, don't use any technology terms, but tell us what kind of audit power or evidentiary information that you need, and then let us help you get there, so that we are not fighting about one technology, but trying to meet the needs of both the supporters of this meeting.

I wasn't close enough to the mike, so hopefully that gets into the transcript. We need your help to define what it is you need, so that we can come up with technology propositions for you.

MR. CAVERLY: We have gone on this question quite a bit of time. Let me turn it over to our HHS colleague, please.

MR. TRENKLE: Thank you for that. Actually that was a lead-in to my question. My real question about all of this gets into risk factors and risk mitigation. I think that is really what we need to look at here and not look at specific technologies, and not get into a contest of whether PKI is better than this and better than that, and whether cost scalability -- leaving costs scalability aside, which obviously there are very important issues when you talk about a specific technology.

I think the question that has been raised by DEA in this meeting and in other meetings is, they have very specific risks that are associated with controlled substances. A number of you have made this statement that you feel that today's environment is sufficient to deal with those risks and sufficient to deal with the issues.

Some of you compared it with the paper environment, saying that by going to the electronic environment we will have all the trails and other types of built-in processes that would take care of that.

But beyond that, are there other things that you can see in today's environment that if we did say tomorrow that DEA and HHS were going to work together to come up

with a solution that meets our requirements as well as theirs, or meets the requirements of the greater industry, deals with work flow issues and others, are you saying that there is nothing that needs to be changed in your current environment, or are there questions that you might have? Are there standard practices that maybe need to be adopted? You mentioned the in-person proofing.

I am just curious to hear some of your thoughts on that, looking at the risk factors and mitigation, and then looking at your environment today and any suggestions you might have.

MR. JOHNSON: And you are looking at me.

MR. TRENKLE: You started to answer the question, so I thought you might be a good one to start.

MR. JOHNSON: Just to repeat, I know it is a repetition of what I said earlier --

MR. CAVERLY: Excuse me, Nigel, would you use the microphone so we can capture you?

MR. JOHNSON: I am so used to my voice being so loud by itself, my wife is always saying, shh, don't speak so loudly. I have made myself lose my chain of thought.

The first thing that we really need is to know what you think you need for doing the levels of control that you think you need to have. We have our beliefs, but we haven't had somebody from the chief counsel's office

say, this is what I need to be able to take this administrative action, this is what I need to be able to send this person to jail. We read a lot, but we haven't had a definition statement.

So once we have that, I believe that we then need to take a look at our systems and make sure that we can give you that evidentiary proof. In my experience, I have not seen there be any difference between whether there is a digital signature on something or whether there is just a plain electronic signature on something for somebody to face criminal charges. I haven't seen that difference, so that is why I continue to say, maybe not PKI, even though I believe in the technology. It doesn't seem to be making a difference in the courts yet.

We believe that our systems are there and that we have the controls, but perhaps you might say boy, it would be great if there was a global identifier that tied a prescription to what was adjudicated. Maybe that is something that would be useful. But we don't know until we hear more from you.

Did you guys have any thoughts?

MR. BARBER: I always appreciate an invitation for a lawyer to talk, thank you, Nigel. Most people want lawyers to be quiet.

MR. JOHNSON: Tell me.

MR. BURGER: I'll just add that we currently have a dual system today, because we can do electronic prescribing for the legend medications, but we can't do electronic prescribing for the controlled substances, at least with our software. We just say, we don't do it. So we already have a dual system. It is our opinion that that dual system is hampering the ability for physicians to embrace electronic prescribing globally.

So we could replace that dual system with a different dual system. It will have the same net effect. As far as we are concerned, frankly if it is significantly more expensive for us to do PKI for some other kind of authentication just for controlled substances, we won't do it. We will just say, keep doing it on paper, because if you won't pay a dollar a day for e-prescribing for 90 percent of your drugs, are you going to pay two dollars a day so we can do the other ten percent? Probably not.

So that is our perspective. But it is also a good point. We don't have really -- as an industry we don't have any clear-cut guidelines as to the kind of information that you need. Most likely we will be able to provide it.

I know that there have been some preliminary regulations that have been written that mention PKI specifically ages ago, and they have never really been

formally adopted. So I know that is where we got the idea from, anyhow.

MR. THOMAS: I left out one disclaimer in my introduction. That is, I am a reformed lawyer myself. You're right, people typically don't want us to talk.

But my perspective on it is, I agree with Mike. We have the two-part process today as well, so we fax back and fax into the pharmacy. I do think that is a detriment, because we message the doc when they try to write a controlled substance that they need to check their fax machine. It is easier to pick up the paper.

From a legal perspective, trying to remember back to my criminal law days in law school, which is the closest I ever got to a courtroom, I can't imagine a better chain of custody, or that the chain of custody you have with any electronic process, certainly the ones that we as vendors have in place today for non-controlled substances, isn't significantly better than the paper-based chain of custody that you have to deal with when a prosecutor goes into court to try to make one of these cases. So I think you have everything you need in the processes that we have in place today.

Going back to the public safety argument, the time is right now to open the floodgates, as Dr. Chen pointed out, and allow this to go forward. I think the

risk is very minimal. Some of the more compelling points today were that of all of us sitting at the table, none of us can speak to a breach that we have had in the years of doing this; we have not had one. So the systems have been in place.

DEA by taking their time to adopt these regulations has had an opportunity to see the systems work and to see the industry mature to a point where you have got strong players in place that can make this work. It frankly is a very good time to go forward and let us turn on the switch. For us it is flipping a switch, to be able to go and start prescribing controlled substances electronically, just as to do with all of the drugs.

DR. CHEN: One point I would like to add there is, if we can somehow identify what are the potential risks that are associated with electronic prescribing, regardless of the methodology used for authentication or non-repudiation, we can identify potential risks.

I can tell you that today, even though we don't have good examples of any breaches there, I know there will be, not because there will be; we will just stop doing it. We need to take a look at whether or not those risks are justifiable for the benefit and the greater good that they bring to us.

I truly tell you that. My company, the fact that

we have been here for almost 30 years, the fact that we are here is because we are very faithful in this vision. This helps. This patient safety, it helps with the improvement of the cost as well. Really it does.

If you think about it, payors such as Blue Cross and those organizations, if this doesn't help them, they wouldn't have funded it.

MR. CAVERLY: Question from DEA?

DR. MAPES: For Mr. Burger and the others if you want to also. The authentication that you have in the prescribers, the on-site person to person authentication of the credentialing of their DEA registration, their state and medical license, things like that it is tied to their licensure. If those licenses are taken away, how do you take away their ability to access the electronic system to prescribe, even though we know there is another control on the other end with the pharmacies? What do you have to take it away at the electronic side?

MR. BURGER: We monitor the information about licenses that have been revoked. So we can take proactive measures to deactivate access to the network. Bearing in mind that all of the prescribers that are using our software have the ability to continue to use the software, because they own it. But the part that we can control is their ability to electronically transmit the data if there

is a challenge with their license.

So we proactively monitor the various methods. Also, we have dialogue with pharmacists, so that if the pharmacist hears about something that maybe we don't know about yet, we still can deactivate them at the network level.

So they will still be able to write the prescription, but when it comes to our network, we will take a look and say, wait, this is an unauthorized prescriber and we will reject the transaction. I'm sure that that is the same thing as everybody does.

DR. MAPES: Thank you.

MR. CAVERLY: HHS?

MR. TRENKLE: I just had a little bit of a followup question. One of the issues with the whole issue of the types of technology is not just the technology, but it is the processes that you have in place for revocation and those types of activities along the way to prevent fraud and abuse.

Are there additional processes that you feel need to be built into your system to deal with some of the issues raised by controlled substance? I know earlier you had asked about what are the specific risk factors, but based on what you know, would there be additional processes, or do you feel like there is enough built in

today to deal with revocation and other types of actions that need to be taken?

MR. THOMAS: No. The short answer is no, we wouldn't change anything about our current process if we were prescribing controlled substances electronically. As I said, we are doing it today. We are just using the fax back process. So we built our technology and our authentications and approval processes, assuming that physicians were using these to generate a controlled substance prescription. So we wouldn't change anything.

MR. JOHNSON: I liked your answer, Russ. That was a good answer. It is nice to have validation, isn't it?

I would like to add something though, and I think you might agree with me. The technology processes are all in place. Where I do believe that we would need to add a process, and I believe that everybody at the table might, but I'll let them answer, is if the DEA or the HHS calls us, we will listen. Your call will get escalated to somebody like me or the head of operations or even the CEO as we then go about kicking off some form of investigation that you have requested, and/or shutting off access as you have requested.

But right now, because it has never happened, we haven't worked through the person process of who do we take

calls from, what specific actions do we taken, and pushing it down to the organization where it is at an operational level versus an executive level.

So we can handle all of it through technology and through our executive, but if we were to move into a system where the HHS or the DEA would say, these are the kinds of things we would like to be able to do, we just have to operationalize that with our people operations, but not our technology.

MR. TRENKLE: Installation change.

MR. JOHNSON: Yes, that is the only thing that we would see.

MR. THOMAS: That is interesting, because it has happened to us. We have had the calls, and the call came to me, so I would definitely change the process. But I note that we have Lisa McElhaney later on from Broward, from our own home state. Frankly -- I don't think this is disclosing any confidences -- the calls we have had are from Duvall, so they are from the other part of the state, but that is a very good point. I think we would formalize a process if we started to anticipate an onslaught.

Maybe a little different from us, since the state is our customer to begin with, so we have processes to deal with calls from authorities at this point. But I agree, that is a good suggestion.

DR. CHEN: I agree with the previous speakers. I just want to emphasize one point about the NPI. I think NPI is a very important feature. I think if we can get NPI working for all vendors with DEA endorsing it and everybody pushing behind it, the national provider index, that kind of stuff is very important, because that way we have a clear view of who is actually writing in the network.

I think an additional point may be the more formalized certification process, because right now we talk about what we do and others talk about what they do. There are some slight differences in the way we process it, in terms of enrolling physicians, providers, office workers and password control.

In our case we do a provider signature. It is not the user side PKI, but we do a server side PKI, so that we lock down that particular record. So the physician cannot say, I didn't do it. We know that particular time, that particular date you signed on this, or you gave your password to somebody else. It has a digital signature associated with that record. Things like that.

We do our best to try to protect the system integrity and record integrity, but I think it would be very nice for government to say, here is one more thing you guys can do across the board, and that will help.

MR. CAVERLY: Question from DEA?

MR. BARBER: I'd like to pull a lawyer trick and ask two, if I could. One is to follow up on Ms. Gallagher's question about cost and then I have a question of my own.

You spoke about the great cost of implementing PKI across all of the different pieces in the network. Yet, I am familiar with PKI applications at the personal level, where you can get your own digital certificate for a very small amount of money, and digitally sign and encrypt your e-mails and make your public key available to anyone who wants to read them.

I realize that DEA's perspective on this is very limited, because we are looking at practitioners that prescribe and pharmacies that fill when it comes to prescriptions. Whereas, our HHS colleagues have a much broader purview over a variety of health information issues.

But my question is, is the cost of PKI that you have spoken about related to the value added networks and the other things that are linking to billing and other issues? If we were solely to look -- and I know, Nigel, you said nobody is doing e-prescribing on e-mail, but if we had a secure standard that would prevent a practitioner from sending directly from a doctor's office to a pharmacy.

My question is, are these costs built into PKI if

we cut out all the middle people, which I know isn't your business model, but I think that would be helpful for us as the government to know.

MR. THOMAS: The problem is, it won't work. You can't cut out as much as you might want to. You can't cut out the middle people because the transaction is being processed and screened and approved by those middle people.

So for example, when a transaction leaves our system to go to RxHub or go to SureScripts, they are providing a function within that transaction, in the case of RxHub, checking the transaction with the payor to insure that that patient is in fact authorized to receive that drug and to have that prescription filled.

So for cash pay, that works, because there is not that middle functionality that has to be provided. But for the vast majority of transactions in the prescribing system, that middle layer is providing an important function.

MR. BARBER: Is that where the cost is associated with implementing PKI, in the middle? Is that where the majority of the cost is?

MR. JOHNSON: Let's answer a couple of questions. You asked one, but it was a good complex question that has a lot of opportunity for discussion. So you were a very good lawyer in the U.S. to vote eight questions in just

one.

Let's just talk quickly about the predominant value of e-prescribing that is actually delivered to the payors. That is on the formulary checking at the time that the prescription is written. That requires these middlemen like me and like RxHub and like SureScripts to deliver formulary information from the plant. So you can't cut them out and get the value of e-prescribing, which is getting a lot of the payors to pay for the doctors to get the system. So the economic model falls apart if you don't have that.

But to go to your question, why is it cheap to go and get a certificate on the Internet, and yet Nigel tells me it is very expensive? That comes down to how you handle the certificate itself.

So Lyndon, when you went and got yours, who did you prove your identity to? What happens when your certificate expires? What happens when you say I exposed it to somebody, I left the machine with my password out there, how do you deal with the fact that that needed to be revoked and nobody else can trust that certificate?

So it goes from something that is very simple in its first use, but then over time as you have to check to see is that still valid, if you sign something and then your certificate got revoked later, can I go back and check the signature before it was revoked?

There are complexities in how all of that is managed, which is why the PKI software vendors still charge a lot, because they have to cover all of those different features. So it is more than just you and a coworker who know each other personally, sending back and forth encrypted e-mails so that nobody else can read them. It is about people who have never met each other working through a chain of trust through the lifetime of an identity which could be one year, ten years, 20 years. It is a lot more complicated.

I could spend hours and hours on it, so tell me if I haven't answered the question.

MR. BARBER: I think you have, thank you. Now can I ask my followup? Russ, you mentioned about fraud and abuse detection and how that would be of great benefit to law enforcement. Obviously that is of significant interest. But you also mentioned the state as your client.

I would like your thoughts. Right now DEA's access to prescription records is limited to pharmacies under the statute. Except in rare cases, doctors are not even required to maintain copies of the prescriptions they write.

My question is, from an enforcement perspective, how do you envision DEA having access to the audit trail from the very beginning all the way through from when all

of the middle people are not DEA registrants, we don't have any legal authority? Do we all want to go to Congress and say let's bring you guys under the purview of DEA so that we can come in and do inspections like we do with pharmacies? You like that idea?

But I'm curious as to when the state is not your client, how does law enforcement get these records and audit trails so that we can actually verify record integrity and authentication?

MR. THOMAS: Two things. Certainly you have subpoena power in the course of a criminal prosecution. So when a transaction leaves our system electronically, in our case it goes from us to SureScripts. There is an audit trail maintained there, from SureScripts to a retail pharmacy where an audit trail is also maintained. So you have got those multiple layers of audits being managed.

I would think, again not being a criminal lawyer or looked at this since 1986 when I took that class, your ability to capture that data is much more comprehensive than if you are having to go out and subpoena individual physicians' records, to determine that the scrip written at the point of care is in fact the prescription that was -- written on paper at the point of care is the prescription that was delivered with the same data, the same information.

So I probably can't comment to the legality of the enforcement process, other than to say, if you have that authority, whether it is through some statutorily provided authority to audit our records or the records of the middlemen or the records of individual physicians, versus just using subpoena power which you have in the course of criminal prosecution, you have got much better access to much better data in any event.

Does that make sense?

MR. BURGER: I'll just add, from our perspective in the contract that our customers sign when they sign up for electronic prescribing, there is a clause in there that says that the data that is transferred back and forth is confidential patient information, and it is solely the property of the physician and the pharmacy, not us. So we can't do anything with it other than to reformat it and move it from point A to point B.

But it also says in the doctor signing that contract that if an investigation takes place under federal, state or local law, that we are obligated to cooperate with the investigation.

So as long as it is okay for you to ask us for certain information and we have an army of lawyers that will check that out, then we will give you whatever information we have. It is a key point, there is

information to be had because there is an audit trail, and it exists.

So from that perspective, we certainly don't want to be regulated any more than we already are, but to the extent that it is okay for you to have access to the data, frankly it is pretty straightforward to provide it.

MR. CAVERLY: We have run out of time, but to balance this out, I am going to throw an extra five minutes in and ask if our HHS colleague has any additional questions.

PARTICIPANT: Well, actually Lyndon was touching on the points that I was. I wanted to find out more information about the audit trails.

I guess just one followup question. How long is this audit information kept?

MR. JOHNSON: Six years.

PARTICIPANT: Six years by everyone?

MR. JOHNSON: Six years by Zix Corp. I believe others, I think SureScripts said seven years.

MR. BURGER: And ours is held indefinitely.

PARTICIPANT: Indefinitely, forever. Until the sun goes out.

MR. BURGER: Until I am retired and living on that island.

MR. THOMAS: I just know ours is held one year

longer than our competitors'.

MR. CAVERLY: Well, the sun has gone out on this panel, so thank you again very much, gentlemen, for your time. I have approximately 20 minutes. Let's convene back at five minutes to 11, please.

(Brief recess.)

Agenda Item: State Perspectives Panel

MR. CAVERLY: As we continue this process this morning, once again thank you for your attention. This is a very complex issue, but it is one in which we appreciate the perspectives of the individual panelists.

As we go on, we will be looking now at the state perspective panel. We have four individuals who will be sitting on that panel. Adele, I'm going to mispronounce your last name. Is it Audet or Audet?

MR. AUDET: Audet.

MR. CAVERLY: Audet. Adele Audet, vice president, Alliance of States with Prescription Monitoring Programs. Danna Droz, who is chair of the executive committee of the National Association of State Controlled Substance Authorities. Charisse Johnson, professional affairs manager, National Association of Boards of Pharmacy. And Lisa Robin, Vice President, Leadership and Legislative Services, Federation of State Medical Boards.

So Adele, I guess you are up first then. Thank

you.

MS. AUDET: I will add my thank you to the list of everybody else. Thanks to the DEA and HHS for inviting me to speak today.

Good morning. My name is Adele Audet. I am speaking on behalf of the Alliance of States with Prescription Monitoring Programs. The Alliance is a national organization of representatives from states that have established or are interested in electronic programs to monitor prescribing and dispensing of prescriptions for controlled substances.

It was formed in the late 1980s to provide a forum for exchange of information among state and federal agencies on the issues of monitoring controlled substances, the methods of data collection, and other topics regarding controlled substance prescriptions.

In 1992, Oklahoma became the first state to receive prescription information electronically. Today, all states receive prescription data electronically from the pharmacies. We have estimated the number of prescriptions received by state prescription monitoring programs in 2005 to exceed 70 million.

There are no dues for membership in all states having or interested in establishing prescription monitoring programs are welcome in the Alliance. The

Alliance works with the Drug Enforcement Administration, diversion control programs, SAMHSA and most recently, BJA.

Twenty-four states attended the last annual meeting of the Alliance held in Fort Lauderdale in October of 2005. At present, 28 states have active prescription monitoring programs or are in the process of implementing newly passed legislation. The Alliance is the resource for contact and other information on prescription monitoring programs.

In general, prescription monitoring programs track the prescribing and dispensing of federally controlled substances by pharmacies and other dispensers. Controlled substances are defined in both federal and state laws and regulations. A controlled substance means drug included in schedule one, two, three, four or five, and the assignment in the schedules one through five is based on an assessment of the drug's potential for abuse, whether it has currently accepted medical use and treatment in the United States, and whether and to what extent abuse of the drug or other substance may lead to psychological and physical dependence.

Because of the established and recognized potential for abuse and/or dependence, issuance of prescriptions for controlled substances is regulated by both federal and state regulatory and law enforcement

agencies to protect both public health and public safety. Prescriptions for legend drug products that are not included in schedules one through five are not regulated to the same extent.

In addition, the laws establishing prescription monitoring programs must balance the public health and safety goals of providing controlled substances for the necessary and proper patient care, and the need to impede drug diversion, that is, the channeling of illicit controlled substances for illegal purposes, misuse or abuse. The prescription monitoring programs are tools used by states as part of initiatives to prevent the diversion of controlled substances which are abused by an alarming percentage of the U.S. population.

The prescription information data fields submitted to the prescription monitoring programs vary according to state laws and can include but are not limited to the dispenser identification number, the date the prescription was filled, the prescription number, whether the prescription is new or is a refill, the national drug code for the drug dispensed, the quantity dispensed, estimated number of days supply, patient identification number, patient name, address, date of birth, prescriber identification number, date prescription issued by prescriber, the person who received the prescription from

the dispenser if other than the patient, and the source of payment for the prescription. Also, some states issue serialized prescription forms and the serial number is included in some prescription monitoring programs.

Prescription monitoring data can be used to identify or assist in investigations of prescription drug diversion, for example, forgeries, doctor shopping, fraud, improper or inappropriate prescribing or dispensing. In addition, the prescription monitoring program data can be used to follow prescribing and dispensing trends and for epidemiological analysis of controlled substance use.

To achieve its goals, prescription monitoring programs require accurate data and secure transmission of data. All prescription monitoring programs, and this includes pharmacies and other dispensers that submit information, contracted vendors that receive and clean data, and recipients of program data, are compliant with HIPAA and state regulations regarding protection of health information.

Based on the experience of member states with electronic records for controlled substance prescriptions, the Alliance submits the following comments.

Electronic transmission of information. The Alliance recognize the value of electronic prescribing. The electronic transmission of data to prescription

monitoring programs has allowed programs to take active roles in protecting the public health and public safety from the diversion of controlled substances. In addition, in working with health care professionals, the Alliance knows that electronic prescribing will be an important factor in improving medication safety by eliminating illegible handwritten prescriptions, and law enforcement sees this as a way to decrease forged prescriptions.

However, prescriptions for controlled substances are not simple electronic transactions. Prescriptions for controlled substances contain private health information and are one of the few legal channels for patients to obtain controlled substances. Prescriptions for controlled substances are regulated by state and federal laws and regulations. There are laws and regulations that speak to the manner of issuance that is written, oral or by facsimile. Laws and regulations for prescriptions issued by electronic transmission must be established to parallel the intent of those existing laws and regulations.

Federal and state laws and regulation define the lawful format for prescriptions for controlled substances that are issued in writing or by oral communication. These laws and regulations serve to insure the prescription information, content and validity as well as the identity of the prescriber and lawful dispensing of the controlled

substance. Equivalent legal definitions or criteria for electronic prescribing must be established.

If e-prescribing means the transmission using electronic media of prescription or prescription related information between a prescriber, dispenser, pharmacy benefit manager or health plan, either directly or through an intermediary, including an e-prescribing network, then the possibility of confusion exists, since this definition of electronic prescribing is less stringent than the definition of prescription found at 21 CFR 1300, which is an order for a medication which is dispensed to or for an ultimate user. A prescription is a lawful order and not the mere transmission of health information.

Furthermore, prescribing controlled substances is limited to an individual practitioner who is authorized to prescribe controlled substances by the jurisdiction in which he is licensed to practice his profession, and is registered or exempted from registration pursuant to DEA regulations. Additionally, a prescription issued by an individual practitioner may be communicated to a pharmacist by an employee or agent of the individual practitioner.

At this time, the DEA narrowly defines employee or agent of the individual practitioner. Prescribing is a direct communication between the practitioner and the pharmacist. There is no provision for an intermediary,

whether a person or a network. It would be difficult to envision a lawful order for a medication from a pharmacy benefit manager to the dispenser. Also, state and federal laws and regulations speak to prescriptions, that is, lawful orders for medication, and the manner of issuance. The definition of prescription should remain constant while laws and regulations and address the specific manner of issuance.

State and federal regulations govern the manner of issuance of controlled substances, for example, written, oral or fax. Laws also govern the information on the medication order issued by the prescriber and the pharmacist's requirements for dispensing the controlled substance ordered, including filling the prescription and record retention. These requirements directly affect the patient's health and safety and validate the prescription to the pharmacist. Records must be complete and accurate.

In prescription monitoring states, health care providers, law enforcement and regulatory agencies rely on precise prescription monitoring program records for clinical and investigatory information. While a prescriber is responsible for properly issuing a prescription for a controlled substance, the pharmacist has a corresponding responsibility for dispensing the controlled substance.

The expectations for security, integrity and non-

repudiation for proper prescription issuance and the responsibilities of the prescriber and pharmacist must be consistent for all types of prescriptions. Currently with handwritten prescriptions, authentication, content integrity and validation are accomplished by adherence to the law and good practice standards. The prescriber uses a prescription form that conforms to state and federal laws and regulations.

The pharmacist reviews the prescription, looking not only at appropriateness of therapy, but the handwriting, colors of ink, changes in numerals, erasures, and if the prescriber is not known to the pharmacist, then a verification of the prescription or prescriber is made.

For a prescription that is transmitted electronically, these actions of the prescriber and pharmacist must be converted to functions in the electronic transmission system. These criteria must replace, be as secure as or more secure than the current systems. A prescriber's signature becomes a unique name, number or symbol that is logically attached, executed or adopted by the prescriber to be the legal equivalent of his handwritten signature. Authorization to use the system and attach the electronic signature must be specific and non-transferable, just as a handwritten signature is unique to the individual.

Authorization can be authenticated through passwords, biometrics, physical feature authentication, behavioral actions and token based authentication. Authentication establishes that the validity of the transmission source and/or verifies the individual's claim that he has been authorized to transmit prescription. Digital signatures need not be required if technology allows contemporariness and non-reproducible electronic capture of the signature. There should be an automatic logoff after each prescription is transmitted, lest a batch of prescriptions is transmitted that contains forged prescriptions.

Protected information should be encrypted to make transmissions secure. Mechanisms to insure content integrity of the transmission must be employed to substitute for the pharmacist's inspection of the hard copy handwritten prescription. Mechanisms to detect alternations to content, interruptions in transmission or unauthorized access to the prescription include error correcting memory and digital signatures.

As a pharmacist recognizes a known prescriber's signature, or performs the verification of an unfamiliar signature, electronic authentication should be required. Technical non-repudiation should also be required so that the person applying the signature may not later deny

sending the signed prescription.

A prescription is a direct order for a medication. The electronic transmission of a prescription should be secure and direct from prescriber to pharmacist. Pharmacy benefit managers or health plans should not be allowed to intercept prescriptions, so that medication orders can comply with insurance formularies or other insurance prescribing standards.

Prescriptions are a prescriber's orders for medication therapy, and changes must not be made to the transmission en route. This would be a practice with unacceptable risk to the patient and unacceptable liability for the prescriber and pharmacist.

Certification and authentication of prescriber. Not all prescribers are registered with the Drug Enforcement Administration. For example, some individual prescribers practicing in a hospital or other institution are exempted from registration, and may prescribe controlled substances under the registration number of the hospital or other institution, and the special internal code assigned by the hospital or institution. Secure systems must be established for providing temporary registration numbers within institutional codes.

Temporarily assigned access to secure systems is abused and compromised. Prescriptions for controlled

substances must originate from a system that is adequately managed to address security risks. Safeguards must be in place so that authentication ceases when association with the institution ceases.

Protocols must be considered for reporting changes to prescriptions that have been transmitted electronically. Prescribers and pharmacists communicate frequently on patient drug therapies. Methods must be considered that will allow health care providers to record communications and any changes to prescriptions transmitted electronically that result from such consultations.

The data fields and methods of transmission of prescription monitoring program information have been established by regulation in most states. States will need to continue receiving data in the established manner, usually from registrants. Vendors should be aware that information on controlled substance prescriptions transmitted electronically to pharmacies may not be in a format acceptable to prescription monitoring programs, or may not contain all the elements required to be reported. The wisdom of a PDA to a PMP transmission has not been determined.

In conclusion, the electronic transmission of prescriptions will have many public health and safety benefits. However, the prescription will remain a

medication order, and economic transmission will remain a manner of issuance. The intent of all existing laws and regulations that insure the security of prescriptions for controlled substances must be maintained for this new mode of transmission of prescriptions.

Thank you.

MS. DROZ: My name is Danna Droz. I want to thank DEA and HHS for the opportunity to speak here today.

I am here representing the National Association of State Controlled Substance Authorities, as chairman of the executive committee. NASCSA is an independent nonprofit educational organization. Our membership consists of state agencies from 43 states which are responsible for the scheduling of controlled substances and administering or enforcing the state laws related to controlled substances. Many of these agency representatives are also health care professionals.

NASCSA's primary purpose is to prevent and control drug abuse, yet insure that the controlled substances are reasonably available to persons who have a true medical need for these drugs. NASCSA maintains a working relationship with both the federal Drug Enforcement Administration and the Substance Abuse and Mental Health Services Administration on issues related to federal and state controlled substances acts.

We are here today to discuss electronic prescriptions as the concept relates to controlled substances. Every state has laws that regulate prescriptions in general and additional, more stringent requirements for prescriptions for controlled substances. As state regulators, we support the concept of electronic prescriptions, however, we are not convinced that the standards currently used for electronic prescriptions for non-controlled substances, that is, legend drugs, are adequate, and thus should not be extended to electronic prescriptions for controlled substances. We must either strengthen the requirements for all prescriptions or create additional requirements for prescriptions for controlled substances.

Some documents require greater security than other documents. Businesses often use electronic documents to conduct many aspects of business, including contracts, especially since the passage of the e-sign law. But certain documents still have to be on paper. A birth certificate is the gateway to a driver's license, a social security number or a passport. I have yet to see an electronic birth certificate that is acceptable for getting one of these other documents. That is because the value of the information inherent in the birth certificate is so high that it becomes extremely important that the document

be genuine.

Prescriptions for controlled substances are similarly valuable. A prescription is not simply a health record, but a lawful order for a dangerous drug. The holder of a prescription for Vicodin or Oxycontin can obtain a product that can be resold for many times its original cost. On the other hand, the product can also provide relief from painful medical conditions. As health care professionals, we want patients with legitimate medical needs to be able to get the treatment and relief they deserve. Therefore it is extremely important to distinguish between genuine prescriptions and forged, altered or fraudulent documents. We just insure that the prescriptions are genuine. Notice that I said genuine, not paper.

We need to be able to use electronic prescriptions for controlled substances. However, the requirements for these prescriptions need to be more rigorous than those for other prescription drugs, because the drugs are different, the prescribers are different, the recordkeeping and security are different, the liability is different and therefore the responsibilities are different.

Controlled substances are not like other prescription drugs. Both federal and state laws describe controlled substances in terms of their potential for

abuse, either physical or psychological or their potential to produce addiction. Every drug listed as a controlled substance is reviewed not only by DEA, but also by HHS for an assessment of its abuse or addiction liability. Antibiotics, antihypertensives and antihyperlipidemics are not subject to such a review because they have never been prone to abuse and no person has ever become addicted to them.

Prescribers of controlled substances have requirements that are more stringent. There are dozens of types of health care professionals. Some are authorized to prescribe drugs. But even this may not include the authority to prescribe a controlled substance. Even when the authority to prescribe a controlled substance is granted, sometimes additional restrictions are imposed, such as a nurse practitioner may be allowed to prescribe certain drugs but not others, an optometrist may be limited to prescribing a 24-hour supply of a controlled substance, or a physician's assistant may be able to authorize a refill, but may not initiate therapy.

Even after a state grants the authority under the licensure provisions to prescribe a controlled substance, that practitioner must also obtain a DEA registration. This is just further evidence that prescriptions for controlled substances are not like prescriptions for other

drugs such as antidepressants.

The recordkeeping and security for controlled substances is more stringent. Manufacturers, distributors, practitioners and pharmacists are required to meet security requirements and maintain separate records for every gram of raw material or each dosage unit of a controlled substance that they handle. Even the disposal of leftover raw materials or expired products is highly regulated. Manufacturers and distributors are required to store controlled substances in a secure location. DEA regulations specify the type of safe or cage surrounding the drugs, and they inspect the alarm system every year. The records have to be visually or physically separate from records for other prescription drugs.

The business has to insure that the purchaser is also registered with DEA, and may only deliver those drugs to the address shown on the purchaser's DEA certificate. Finally, the manufacturer or distributor must report many of the sales to DEA through the Arco system. None of this is required for heart drugs or thyroid drugs.

Pharmacists and practitioners who use controlled substances to treat patients have their own set of state and federal regulations about security and recordkeeping. The locations where the drugs may be stored is regulated, and access to the storage area must be limited. In

addition, they must inventory the stock periodically, record every dose and which patient received it. Not only the patient name, but the patient's address, the date it was given, who authorized it, and the quantity used. Then they are still subject to audit by state and federal authorities. There are no such requirements for security for and accountability for allergy medications.

The liability is stricter, and therefore the responsibilities are more rigorous. This responsibility is so important that it is written into federal law and many state laws as well. The Code of Federal Regulations state that both pharmacists and practitioners have a corresponding responsibility to insure that every prescription for a controlled substance is issued and dispensed to a legitimate patient to treat a legitimate medical condition by a practitioner in a legitimate practitioner-patient relationship.

Federal law does not require this for diuretics, cancer chemotherapy or nuclear pharmaceuticals. Why? Because there is little incentive for a person to consume those drugs unless they need them, and even then it is a challenge to get patients to take their prescriptions as prescribed. There are unpleasant side effects, they are expensive, and patients sometimes forget.

But controlled substances are a whole different

story. There are many people who will consume or at least purchase narcotics, sedatives or stimulants, even when they don't have a medical condition. For them, the undesirable side effects are irrelevant. If the cost is high, they can always sell a few to friends or neighbors. For these reasons and more, the law has always held prescriptions for controlled substances to a higher standard.

Electronic prescriptions need to be available as an option to prescribers. Electronic prescriptions can be a secure and cost effective means of delivering a prescription to a pharmacy. More and more physician offices are utilizing computers to maintain records. The easy availability of the Internet facilitates sending the prescription directly to the pharmacy of the patient's choice, rather than relying on the patient himself or herself to deliver it. In theory it could eliminate forgery, alteration and loss.

Electronic prescriptions also nearly eliminate the confusion caused by handwritten prescriptions. The need for accuracy in prescriptions has been the subject of a great deal of research, even though the results are intuitive.

Since 2000, DEA and NASCSA have been discussing electronic prescriptions for controlled substances. When DEA first raised the topic, the NASCSA members had concerns

about these electronic documents. While there are certainly problems with paper prescriptions, the requirements in place created some relative assurances for the pharmacist.

The pharmacist needs to know certain things from every prescription -- who the patient is, who the prescriber is, what drug is prescribed and how the patient should take the drug. But if the prescription is for a controlled substance, the pharmacist must also determine whether the prescriber is authorized by state law, whether he or she has a valid DEA registration, whether the patient has a legitimate medical condition, whether the prescriber is treating within the scope of his or her licensure, and whether the treatment is within the usual course of the prescriber's professional practice.

Electronic prescriptions for controlled substances need to have additional safeguards beyond what is currently allowed for other prescriptions. In the early discussions of electronic prescriptions, the regulators were concerned about electronic prescriptions because of the abuses we have seen with paper and telephone prescriptions for controlled substances. Since DEA regulates telephone, paper and fax prescriptions, we wanted DEA to insure that the electronic prescriptions would be at least as reliable as paper prescriptions. We also felt

that it was important to have a federal standard so that the technology companies knew basically what was required, even though individual states may still have small differences.

Ideally, the federal standard will provide sufficient security that states will not feel the need for additional protection. While the technology can vary, it is clear that there are some basic requirements for any prescription for a controlled substance -- identification of the prescriber, who is sending the prescription, verification of the prescriber's authority, is this a valid DEA number for this prescriber, the integrity of the prescription, has there been any change in the prescription while it has been in cyberspace, non-repudiation of the prescription by the prescriber. What prevents a dishonest doctor from issuing an electronic prescription and then if confronted by law enforcement denying that he or she did so? Non-duplication of the prescription. Once a prescription is plucked from cyberspace, it should only be filled one time. Thus, the prescription as dispensed is unique.

There can be multiple technologies to provide these characteristics to electronic prescriptions. The important thing is that each characteristic accompanies each and every prescription for a controlled substance.

On the surface, one might view standard electronic prescriptions and say that they embody each of the characteristics mentioned. Based on our experience, we expect a larger number and more elaborate scams with electronic prescriptions unless strict protections are in place. Even then, we merely hope to minimize the number of illegal electronic prescriptions.

Identification of the prescriber. One of the biggest diversion problems in recent years involves ancillary personnel in the pharmacy or the prescriber's office. We all know that a person who is technologically sophisticated can do amazing things with a computer. Without strict transmission standards, it will be very easy to transmit a document to multiple pharmacies that has the same appearance as one that actually came from a prescriber. Voila, forged electronic prescriptions.

Verification of the prescriber's authority. State license numbers and DEA registration numbers have specific formats. But this information is very easy for dishonest people to obtain either from other prescriptions, from the Internet or by purchase. Consequently anyone with a computer can create a very realistic prescription blank for a fictitious prescriber.

I once worked a case where a person was creating paper prescription blanks on a home computer. These fakes

were so good that even the physician himself could not distinguish the fakes from the ones he obtained from a local printing company. Why do we think that electronic prescriptions will be any safer unless it is required?

Integrity of the prescription. Once a prescription leaves a practitioner's hand or mouth, it is available for alteration. With paper or oral prescriptions there are red flags that indicate to a pharmacist that further validation is needed. A pharmacist is expected to notice multiple ink colors, multiple handwritings, unusual format of a prescription that is either written or oral. With an electronic prescription there are no similar warning signals. The pharmacist must be assured that the electronic prescription he or she receives has not been modified in any way since the practitioner created it. Electronic can be another word for invisible. Since the electronic alterations will not be visible, the process of transmitting the prescription for a controlled substance must include assurances of integrity.

Non-repudiation is another term for positive identification. I have been involved in investigations of illegal prescriptions where the prescriber simply stated that he or she did not write the prescription, despite other evidence to the contrary. Once a practitioner disavows a prescription, the investigation becomes

extremely difficult and expensive.

We have all had experiences with computer viruses that make e-mail appear as though they originated from a trusted source when in fact their origin may be a foreign country or a prison. A prescription for a controlled substance is so valuable that once a prescriber authorizes it, that practitioner cannot have the ability to later deny the action. Therefore, an electronic prescription for a controlled substance needs more positive identification than typically accompanies an electronic document. The prescription should be positively linked to the prescriber every time.

We need strict federal standards for electronic prescriptions for controlled substances. I have been a regulator in three different states. As regulators we receive phone calls on a regular basis about electronic prescriptions for controlled substances. The industry has answered the needs of medicine and pharmacy for electronic medical records, electronic billing records and electronic business records. It is time to enable the health care professionals to fully utilize the advantages of electronic prescriptions for all drugs, but the current technology for electronic prescriptions is not sufficient for prescriptions for controlled substances. At least, we the regulators have not been convinced that it is.

Practitioners and pharmacists should not have to be cops. We need to protect them by setting standards for electronic prescriptions for controlled substances that are as secure as reasonably possible. Health care professionals also need to be assured that regulators and law enforcement can do the job of catching the bad guys so they can do their job of treating patients.

Federal standards for transmitting prescriptions for controlled substances are overdue, but lax standards are worse than none at all. States have the right to impose criteria that are more stringent than federal law. If the federal standards are less stringent than state law, we the regulators will still have to protect our citizens by continuing to require adherence to stricter state standards.

Thank you.

MS. JOHNSON: Good morning, everyone. My name is Charisse Johnson. I am currently the professional affairs manager with the National Association of Boards of Pharmacy. For those of you who don't know, NABP is the association that represents all of the state boards of pharmacy and their mission to protect the public health. Our membership also includes the District of Columbia, Puerto Rico and the Virgin Islands, and we also have an international membership base.

We applaud the efforts today of the Drug Enforcement Administration along with the Department of Health and Human Services. NABP is privileged to be here today and have the opportunity to provide input during today's forum.

In addition to complying with the federal Controlled Substances Act, pharmacies and pharmacists must also comply with any state-specific controlled substance act which is for the most part enforced by the state boards of pharmacy. Thus, that is our connection with the proceedings here today.

In the brief time that I have, I would first like to discuss NABP's specific initiatives as it relates to electronic prescribing, including model language as included in our model acts. I think it would also be helpful if I give a snapshot view of activity within the states with respect to e-prescribing, and in some cases e-prescribing for controlled substances. I would also like to touch upon some factors external to the boards, namely the Medicare Part D Electronic Prescribing Foundation standards. Lastly, I would like to convey some considerations specific to the state boards that the industry and DEA may consider as we all move forward collectively in these initiatives.

The near future will reveal a federally approved

Drug Enforcement Administration electronic prescribing prescription prescribing system. The board office has been hesitant to establish one mechanism, soon to be superseded by another. Regardless, any electronic signature transmission system needs board of pharmacy approval, and none have been given.

This quote from the Nevada State Board of Pharmacy probably represents the sentiment of most of our state board of pharmacy members who anxiously await DEA's regulations on e-prescribing for controlled substances. However, NABP and the state boards of pharmacy recognize the need and importance of working with DEA to achieve a productive and intertwining of both federal and state laws.

Our pharmacists and pharmacies are probably even more anxious. Currently e-prescribing regulatory adherence with respect to both controlled substances and non-controlled substances is sometimes a murky and confusing issue for our pharmacist practitioners. In addition to the variations between state and federal laws, the potential inconsistency between e-prescribing for Medicare Part D eligible patients and those non-eligible patients makes total compliance even more ambiguous. Ultimately, I think that the prescribing community looks for the attainment of this e-prescribing utopia being in total compliance with all state and federal laws pertaining to e-prescribing.

Although NABP's efforts in e-prescribing started almost 20 years ago, in 1996 the NABP delegation passed a resolution directing that NABP work with DEA to amend the federal Controlled Substances Act to allow the electronic transmission of all controlled substances prescriptions. In 2001 the delegation then appointed a specific task force to further develop model language for the use of devices in the e-prescribing transmission of prescriptions and patient information. Then in 2004 NABP was instructed to work with stakeholders to move e-prescribing initiatives forward, and as a result NABP provided inputs to NCVHS as that agency developed e-prescribing recommendations per the MMA 2003.

The NABP model act and model rules, which is used as a guide as state boards update their regulation, incorporates a definition of electronic transmission. This definition is actually two-pronged, incorporating both facsimile and computer transmission. As a result, the possibilities in transmitting a prescription may result in the more archaic approach of faxing what we hope to envision or what we are envisioning with controlled substances, that is, a computer to computer transmission.

Pursuant to the recommendations of that 2001 task force on electronic transmission, both electronic signature and digital signature have also been added to the NABP model rules, recognizing that the digital signature is the

most secure of the two.

The model act also addresses the conditions under which e-prescribing may occur, including who may actually receive these electronic prescriptions, that being a pharmacist or certified pharmacy technician, who can actually transmit these transmissions, that being a prescriber or their agent. It also details recordkeeping requirements and also most importantly the pharmacist's responsibility to exercise professional judgment when evaluating and authenticating prescriptions.

Fortunately, most states do allow the electronic transmission of prescriptions specifically for non-controlled substances in the context of a computer to computer transaction. However, there are two states that don't allow e-prescriptions received from non-resident prescribers. Additionally, most states also recognize electronic signatures, although we don't have hard data on those states that recognize digital signatures.

If we compare the state and federal laws pertaining specifically to the e-prescribing for controlled substances, most states do mirror current DEA regulations. However, there are some exceptions. For example, California, North Dakota and Washington regulations really anticipate the use of electronic signatures. On the other side of the spectrum, some other states like Utah and New

York strictly prohibit even the faxing of Rx's for controlled substances.

What are some of the concerns of the state boards of pharmacy as efforts continue to advance e-prescribing, and in the specific context of controlled substances? In an attempt to gather this information, NABP conducted a survey targeted to the state boards of pharmacy, and found that these concerns either fall into one or two categories, that being the technology or the security/authenticity concerns.

Boards have reported that they are challenged with keeping regulations consistent with the ever-changing technology. A few states even require that e-prescription software or hardware be approved by the board before implementation by the pharmacy. They have also expressed concerns of security, including assuring authenticity, the integrity of the prescription, and also prohibiting unauthorized access to prescription information.

The MMA 2003 foundation standards for e-prescribing that became effective January 1 have also had a number of potential implications for the state boards in terms of pre-emption of state laws and regulations. In short, the MMA provisions make unenforceable any state law or rule that restricts the ability of prescribers to electronically submit prescriptions from Medicare eligible

patients for a covered drug.

In response to these standards, NABP researched to find specific state laws that could be pre-empted and the potential number of jurisdictions or states that could be affected, and that information is presented here. So for example, any state laws or regulations that expressly prohibit electronic prescribing could be pre-empted. Those laws that prohibit transmission through intermediaries or access to those prescriptions by plans, their agents or authorized third parties could be pre-empted.

Ultimately, the unfortunate result is that in some states, two different sets of electronic prescribing rules may emerge, one for Medicare eligible patients and the other for non-Medicare eligible patients. Therefore we have strongly urged the states to consider reviewing their rules and regulations to avoid this outcome in consideration of the points that I have listed here.

Since the other panelists pretty much covered prescription monitoring programs, I won't go into further detail about those programs, except to highlight that despite the modernization of prescription monitoring programs, forgery and manipulation of prescriptions has still been a concern for some states. Therefore, some states like California have instituted tamper-resistant security prescription requirements that mandate an

incorporation of a number of security features.

In conclusion, in consideration of what I have discussed today, NABP believes that the following principles are necessary in assuring that electronic transmission standards safeguard patient health, safety and welfare.

First, once a prescriber has transmitted an electronic prescription, no intervening entity may alter that prescription information. Any altering by an intermediary of a prescribed drug, strength, quantity, allowed refills or directions would adversely affect patient safety, and is in direct conflict with state laws that were established to insure the integrity of the prescribing process.

Secondly, in order to assure the validity of electronic prescriptions via electronic transmissions, the electronic prescriptions should be signed by use of either an electronic or digital signature. Also, patient privacy and confidentiality must be respected. There must be a clear distinction as to which entities are allowed to have access to certain patient information and what requirements must be satisfied to share such information. Entities that have access to sensitive patient information must also comply with HIPAA regulations. Also, e-prescribing must facilitate prescriber and pharmacist collaboration, which

is a crucial component of quality patient care. Lastly, the patient should have freedom of choice regarding their pharmacy providers and regardless of the technological capabilities of their pharmacy.

With that, I will conclude. Thank you very much.

MS. ROBIN: It is always wonderful to be the last panelist, because it has all been said. I would like to echo the concerns that have been expressed by my fellow panelists.

I am Lisa Robin with the Federation of State Medical Boards. I am very pleased to be here, to have the opportunity to comment on behalf of our medical boards and to express the concerns that they have forwarded to me.

The Federation is a nonprofit organization comprised of 70 medical licensing and disciplinary boards in the United States and territories. We were established in 1912. We are located in Dallas, Texas.

As a collective voice for state medical boards, the Federation advocates for state medical boards as independent state agencies with sufficient statutory authority to regulate the practice of medicine. In addition to providing a variety of services including the United States medical licensing examination, post-licensure assessment, data banking credentials verification, the Federation is a resource for research, policy analysis and

development, education and information.

Our mission is to improve the quality, safety and integrity of health care by promoting high standards for physician licensure and practice. We assist state medical boards in achieving their statutory mandate to protect the public.

We have public policy addressing issues pertinent to medical regulations that our member boards use as a basis for their policy development activities. Such topics include the use of controlled substances for the treatment of pain, office based opioid addiction treatment, physician impairment, boundary issues and scope of practice.

In addition to policy development, we monitor state and federal legislative initiatives, work collaboratively with federal and state regulatory agencies, and provide legislative assistance to and on behalf of our member boards.

The Federation has been actively involved as a national leader on the use of telecommunications and the Internet in the practice of medicine for a number of years. In 1996, we published a model act to regulate the practice of medicine across state lines. In 2002 we published model guidelines for the appropriate use of the Internet in medical practice. This is one of the first national standards established for Internet medical practice.

State medical boards regularly handle cases involving inappropriate prescribing and other prescribing regulations relative to physician practice. In 2005 state medical boards reported over 6,100 disciplinary actions taken against licensees. Of those, 424 were prescription related violations, so this is a priority for medical boards. It is the Federation's hope that as new electronic prescription systems are implemented, there will be a significant reduction in prescription violations. If proper safeguards are implemented, electronic prescribing systems can serve as a deterrent to those who wish to abuse the current paper system. It can reduce medical errors and facilitate access to care and enhance convenience for patients.

Feedback from our state medical boards indicate support for a system whereby information is exchanged directly from registrant to registrant that is implementable, secure and feasible.

Because the proposed system will be applicable to both legend drugs and controlled substances, it is imperative that there will be parity of standards, that the system be sufficient to prevent the diversion of controlled substances. Accordingly, a stricter standard must be applied to accommodate the specific state and federal requirements related to the prescribing of controlled

substances.

We are also concerned that a dual system could be contrary to the public health. It could discourage patients' access to adequate pain care by making the prescribing of controlled substances a more burdensome process.

In accordance with the Federation's policy, electronic communications including prescriptions should be secure within existing technology, and be specific via standards that address authentication, privacy, authorized health care, who can submit and process prescriptions, require patient information to be included on the prescription, and archival and retrieval of information.

Sufficient security measures must be in place and documented to assure confidentiality and integrity of patient identifiable information. Feedback from our medical boards indicate some level of concern regarding patient privacy. Accordingly, boards ask that any system created for electronic prescribing must be designed so as to protect the privacy of patient specific information. Therefore, security is a priority, so that all patient information is securely maintained, and patient information protected from unauthorized access.

States vary as to requirements for the prescribing of controlled substances. If there is

discrepancy between the federal and state privacy requirements, we support the application of the stricter standard in order to best protect the patient.

Any electronic prescribing system must protect the integrity of the prescription and insure the chain of custody is well documented. It is imperative that the system assure the identify of the prescriber, specifically the physician or his designated health professional. The system must be sufficiently secure to prevent non-authorized personnel from issuing the electronic prescription.

Some states have addressed this specifically. There was a recent legislation in New Jersey as far as electronic transmission of prescriptions. It says that a pharmacist must not fill an electronic prescription transmitted by anyone other than a practitioner authorized to prescribe medications, or the prescribing practitioner's authorized agent. If the prescription is transmitted by the practitioner's authorized agent, the transmission shall include the full name and title of the agent.

All electronic prescriptions should contain at least the same patient information required by state law of written prescriptions. State prescription laws should not be superseded by less stringent federal standards. Electronic prescription should contain all the same

elements as their written counterparts.

State medical boards require that physicians maintain adequate recordkeeping of electronic prescriptions. A copy of the electronic prescription should be in the patient's medical record. In the case of an investigation of the practitioner, it is imperative that medical investigators have access to precise records in order to gather sufficient information regarding the diagnosis and appropriate treatment for which the medication is being prescribed. Accordingly, any system for the electronic submission of a prescription must document the chain of custody, preserving a record of the prescription and the medication dispensed. In order to protect against diversion, the system should be interoperable within a state's prescription monitoring system.

Thank you. I appreciate the opportunity to be able to speak to you on behalf of state medical boards. As we move forward into this century, telecommunications and the Internet will continue to become vital and an effective tool in providing resource effective medical care. On behalf of our medical boards, we support these innovations as long as proper safeguards are implemented to make sure that quality of care is not diminished and patient privacy is not compromised.

Thank you.

MR. CAVERLY: Once again, thank you, panelists, for adding your voice to this important process for us. We are now going to take questions from the individual questioners. Tony, I am going to throw the first one to you for HHS.

MR. TRENKLE: Thank you. One theme that I saw coming across all four of you, even though you approached it slightly different, was consistency of approach. I think that that seems to be something that I am hearing from all of you, that a lack of consistency will create more problems than it resolves, and could endanger safety, could be a deterrent to e-prescribing as we all know.

Would any of you care to elaborate on that any more, in terms of what steps you believe HHS and DEA can take to move towards that nirvana, as one person put it? Utopia, maybe.

MS. JOHNSON: I guess I'll speak first, since he used my analogy. I think that HHS and DEA are moving in the right direction currently, first off with the e-prescribing standards per MMA, and then with the discussions that we are having today with DEA. It gives us a good feeling that we are going in the right direction.

However, if we don't have one standard or a minimum standard, what could result is fragmentation, and

maybe leave the states in developing their own standards. That of course is not the direction that we perhaps want to go. So I think that what you are currently doing is a great step in the right direction.

MR. TRENKLE: When you say standard, do you mean a standard or business practice? Some of this may involve similar standards, but some of it is business practices as well. I guess I just want to probe a little bit deeper to you or some of the other panelists.

MS. ROBIN: I believe I can speak for our boards, that there should be consistency among both standards and business practices. There is some concern, if you have different standards or systems applied to different populations of patients, that by doing so you also encourage greater inconsistency among states. As practice of medicine and pharmacy changes, this would become less bound by state boundaries.

I think it is imperative that we apply consistent standards and have similar business practices among jurisdictions.

MS. DROZ: I would agree that one system that meets the highest level of restrictions and standards is definitely preferable to multiple systems. I am glad that we are finally getting to the point of having some hearings and trying to move the regulations forward for e-

prescribing. It has been something that the regulators would like to see because it has a lot of advantages, but in the past there has been too much fragmentation, too many rules, and nothing really that we could all agree on one standard that would apply to all the prescriptions. I think that is what we would like to see.

MR. CAVERLY: DEA, question?

MS. GALLAGHER: I have two, but I will do one. As you know, the registrants are the ultimate legally responsible person for the proper prescribing and proper dispensing. Have you gotten any feedback from those individuals as far as choosing vendors? Is it a world that scares them, or do they understand that they are the ones responsible? The vendors are not at this time registered with DEA.

MS. DROZ: My experience is that while you are correct that the registrants are responsible, they tend to rely on other people to tell them what their responsibilities are. I can't tell you how many times I have gotten a call from a physician's office practice, inquiring about their electronic prescribing capabilities, and my having to tell them that it does not meet the standards of the state. They are saying, oh, but the salesman told me this has been approved by whatever, DEA or the state agency or whatever. It is very frustrating.

So while they are responsible, I don't think they really understand that.

MR. TRENKLE: If you will let me probe on that just a little bit further. The vendor panel that we had here earlier didn't imply, but came out and said they felt that what they had in place today is sufficient to meet the requirements of controlled substances. It sounds like there is some disagreement here among the panel. Can you elaborate on that a little bit more, please?

MS. DROZ: I think that is true. The vendors have a product that they want to sell. It is obviously in their best interest to not make any further changes because that creates additional expense for them.

There may be more security in their systems than we the regulators have been provided. But we are not convinced at this point.

MR. TRENKLE: But can you give specifics as to where you feel that they are not living up to these requirements that you would have, where the shortcomings are?

MS. DROZ: We feel that for one thing, it is too easy for a person who is not authorized to prescribe to create an illegal electronic prescription, just like they can create illegal paper prescriptions and telephone prescriptions. We don't think there is enough security in

the system to differentiate between the doctor and the receptionist.

MS. ROBIN: I believe our concern would be similar. It would relate to the authentication and assuring that the chain of custody is clearly documented, and any attempted changes, that the physician could be notified immediately and there would be nothing that would -- I was also concerned by the time period of maintaining the records. I was concerned by talking about the records being maintained for six years. I'm not sure that that would be adequate for our medical boards.

MR. TRENKLE: I was going to ask that question. What is an adequate period?

MS. ROBIN: I don't know that there is an arbitrary number, but if you are investigating someone's practice, oftentimes they look for a trend, and they would go back for a period of time. So I really believe that the majority of boards would find six years, an arbitrary number, insufficient.

MS. JOHNSON: With respect to prescription record requirements on the state boards of pharmacy behalf, the state boards do now dictate prescription recordkeeping requirements. I think on average for most states, that number is five years. However, and I may be corrected, but I believe that the MMA prescription recordkeeping

requirements are ten years. So I think that would also play into what factors would need to be considered with recordkeeping requirements.

MS. GALLAGHER: This is probably a very clear question and everyone would know the answer, but I am just going to ask it anyway.

The vendors are talking about non-controls. I think Florida is doing controlled substances with e-prescribing, but the majority of them, it appears to be non-controlled. So we don't have the evidence of fraud and methods, probably because they are not necessarily the drugs that people are seeking.

Could you elaborate on why you think controlled substances may be more subject to diversion than non-controls?

MS. DROZ: Because they are more valuable in the marketplace on the legal and illegal markets.

MR. CAVERLY: Additional questions from HHS?

MR. TRENKLE: Yes, I had another question for the panelist on my right here. One of the issues you discussed was the issue of equivalent -- I wouldn't call it functionality, but equivalent ways of being able to detect fraud within the electronic prescribing mode as opposed to the paper world. You mentioned a number of protections that are used by the pharmacists today.

Recognizing the fact that in the electronic prescribing world obviously there are a lot more tools that can't be used in the paper world today to detect fraud as well. So I guess my question to you is, I'm not quite clear from your perspective, were you saying that you have more concerns about dealing with electronic prescribing without additional safeguards or requirements? Or are you saying that we need to have some equivalencies built in here that weren't there today? I'm not clear where you were going with that.

MS. DROZ: I think that there has not been enough work at trying to break an electronic system, electronic prescribing system, to determine what needs to be there. I have a saying that I like to use: Technology is great when it works. But it is when there are problems and errors -- we have not had the opportunity to look at these systems in depth and see where the holes are and where the scammers are going to find a way around anything that we might create.

MR. TRENKLE: So you are recommending more research being done in this area?

MS. DROZ: Yes. I think that all the research has been done and the systems have been created for the 95 percent that are honest patients, honest practitioners, honest pharmacists, but we have not really done any work at

looking at what happens when people are not honest and how they can get around those things. It takes a thief to catch a thief, sort of thing. I don't think that has been done.

MR. CAVERLY: Additional questions from DEA?

MR. BARBER: Have any of your members had cases, either on the pharmacy or medical practitioner side looking at licensing, or in administrative hearings they have needed electronic prescription records? If so, can you talk to us? I know you were here during the vendor sessions about audit trails and how that evidence played out for regulatory purposes, if any of your members have had those types of situations.

MS. JOHNSON: I can't comment on any such cases or circumstances. Perhaps that may be a question for the next panel. I know that Bill Winsley from the Ohio State Board of Pharmacy will be on that panel. He may be able to answer that question.

But I think that the boards would like to have a comfort level with the existing technology, and if that needs to be updated or changed in any way to meet the current requirements with respect to controlled substances, I think that is what they will be looking for.

MS. ROBIN: I can't speak to specific cases, but I had several calls from medical board investigators just

expressing the concern that it is very necessary for them to do their job and have access, at least the same access as they would the current systems, believing that the electronic system is preferable, particularly if it is registrant to registrant, because there is less hands in the pie. It should be an easier system to document.

MR. CAVERLY: Tony, additional questions?

MR. TRENKLE: Not at this moment, no.

MR. CAVERLY: DEA, additional questions?

MR. BARBER: I heard from several of the panelists about registrant to registrant. Obviously the technology panels and the vendor panels indicated there is a lot going on in the middle.

As regulators, how do you view changes to an electronic prescription? Are there permissible changes, perhaps? I know some of our prior panels talked about the types of changes that could be made for formatting, but prior to the dispensing by the pharmacy, what are your views on whether or not changes are permissible, and if so, what are those changes are?

MS. JOHNSON: To clarify, do you mean changes by a third party entity other than the prescriber or the pharmacist?

MR. BARBER: Right, changes by someone other than the registrant or the party that you regulate.

MS. JOHNSON: Sure. I think in my presentation I highlighted some of the state laws and regulations that could be pre-empted per MMA 2003 for e-prescribing standards. One of the state laws and regulations for some of the states that may be pre-empted was access to that prescription information by a PBM or a third party.

Just to give you some background on why those laws came into play, was because NABP had found that some of the PBMs were altering prescription drug information, either be it the drug or the dose, and that could be the practice of pharmacy or the practice of medicine. So that is why those laws were specifically implemented, to deter that type of activity from occurring.

So I guess to answer your question, that type of activity -- certainly the state boards would not want to see that type of activity going on. I don't think that would be in the best interest of patient safety or quality of care.

MS. ROBIN: Yes, I think the problem comes from the third party. The medical board has jurisdiction over the prescriber and the dispenser, but they have no jurisdiction over the third party. There needs to be some mechanism that if there is any alteration, the physician should be notified, because he or she is liable for that as a part of the practice of medicine or maintaining a

standard of care. So I do think there is a concern with any alterations that could be made by a third party.

MS. DROZ: I would just echo I think. We look with any opportunity for change with suspicion. Even though the system says you can only change generics for a brand or something like that, if there is any opportunity, then there is an opportunity to make other changes as well. The liability for what is actually prescribed and dispensed to a patient falls on the prescriber and on the pharmacist, not on any intermediary.

MR. CAVERLY: Tony, did you have any followup to that?

MR. TRENKLE: No.

MR. CAVERLY: I'm sorry, go ahead.

MS. JOHNSON: Just as a followup, even though right now the state law that I was alluding to about prohibiting intervention by a PBM or another third party entity, we have now urged the state boards to change those laws, because we have gotten feedback from the industry that this practice is no longer occurring.

So with that respect, NABP would agree, and actually has urged the states to change those laws.

MR. CAVERLY: Any followup from DEA?

MR. BARBER: Along the same lines about audit trails and potential for changes, under existing state

laws, would your state regulatory boards have difficulty obtaining records from the intermediaries that we have heard from currently, vendors? How would you go about getting records? What legal authorities do you have?

MS. ROBIN: I would say, depending on where the third party is located, they would have no authority. They would have no subpoena authority.

MS. DROZ: The regulatory boards regulate and have leverage to control the prescribers and the dispensers. We have no leverage over that, unless the agency has law enforcement authority. Then perhaps they have subpoena powers. But again, if they are located in another jurisdiction, it may be very difficult or impossible.

MR. CAVERLY: Additional comments or questions from either side? My stomach tells me it is lunch. Although we are ahead of our agenda, I agree with my stomach. I have got approximately 12:15. Even though it says 1:40, can we be back at 1:30, possibly add a little additional time for questionings? Be back after lunch at 1:30.

(The meeting recessed for lunch at 12:15 p.m., to reconvene at 1:35 p.m.)

A T E R N O O N S E S S I O N 1:35 p.m.)

Agenda Item: Law Enforcement Perspectives Panel

MR. CAVERLY: Welcome back from lunch, as we begin our sixth and final panel. We have representing the law enforcement perspective with us here on the stage Lisa McElhaney, who is a sergeant with the Broward County Sheriff's Office. Robert Nicholson is an Assistant United States Attorney working for the executive office for United States Attorneys, and William Winsley, Executive Director of the Ohio State Board of Pharmacy.

During the break we had a question, and I would just ask the panelists that as you answer questions, please utilize the microphones. Some folks had difficulty hearing one of the last panels.

So with that, I will leave it to our first panelist.

SGT. MC ELHANEY: Hello. First of all, I want to say thank you very much to DEA and to HHS for having me here. They may regret it. Just kidding.

First of all, for those of you who don't know me, my name is Lisa McElhaney. I am a sergeant with the Broward County Sheriff's Office, which is located in the Fort Lauderdale area of Florida. We are sandwiched between Metro Dade or Miami-Dade and Palm Beach County.

I have been in law enforcement 17 years, actually with the Sheriff's Office for 17 years and three years with

the state attorney's office prior to that. I am going to tell you a little bit about what I do and how I got involved in the field of pharmaceutical diversion, because it is very paramount to why you should listen to what I have to say to you.

I have been drug diversion investigations and been involved in drug diversion investigations for approximately 14 years. I currently am the manager and administrator of our drug diversion unit for the Sheriff's Office. Our Sheriff's Office is an extremely large, almost metropolitan type agency. We have approximately 3200 sworn officers. We have 17 contract cities that we provide law enforcement services to. My unit services the entire county, which is quite large.

I am also the National Secretary of NADDI, which is the National Association of Drug Diversion Investigators, and I have been a member of NADDI for approximately 13 years. I am on the Board of Governors for the Broward County Commission on Substance Abuse, and the chairperson of their prescription drug committee. Also I have testified before the Florida House and Senate on several matters related to drug diversion, and been instrumental in getting several laws passed. Unfortunately, our prescription monitoring program was not one of them.

I am also considered an expert witness in state court as well as federal court in the field of drug diversion, and have been certified as such on several occasions.

As I stated, I have been doing drug diversion investigations for approximately 14 years. The one thing that I gleaned from yesterday from hearing the testimony from the vendors and the medical community and the pharmacy community is that I live in a whole different world.

I see the worst of the worst. I see what you don't want to see and what you don't want to happen. I get that on a daily basis. That is my job. That is what I do. I have conducted hundreds of undercover narcotics investigations dealing with your traditional street level drugs as well as pharmaceutical drugs. I have been involved in everything from your minor hand to hand buys to very large scale undercover operations involving -- I think the largest one was 18 months, dealing with doctors and pharmacies and wholesalers.

I see that one percent the DEA says is not the norm of the practitioners. That is primarily what I deal with. I also work with the Drug Enforcement Administration, also with FDA. MFUCU is Medicaid fraud, Office of the Inspector General, every designator you can imagine, state and federal, also U.S. Customs.

The problem that I as a local law enforcement officer face is, most of the federal agencies look towards the providers or the larger scale operations. What doesn't fit that criteria generally falls toward local law enforcement, not just myself, but the city agencies, other county agencies as far as law enforcement. A tremendous amount falls in that direction.

Basically we deal with the majority of non-provider investigations, and we work as an assisting agency with the federal agencies on all provider type investigations. The trends that I have seen in the time that I have started in diversion has exploded. It is epidemic proportions. It is not just within the state of Florida, it is across the United States, and actually worldwide.

It involves teenagers, organized sells in rings of teenagers diverting pharmaceutical drugs. I'm not talking -- there was a comment made the other day about, the majority get them out of their medicine cabinets; not anymore.

It also involves through the entire realm into the elderly population. I have 70- and 80-year-old drug dealers on the street that are supplementing their income through diversion. So it is not just a once in a awhile thing anymore; it is becoming more of a norm.

The street level sales, the hand to hand buys, a lot of the street teams or the set teams as we call them handle a lot of the one on one type possession cases, the street level buys. The organized sells of individuals. We are talking organized crime. We are talking multilevel structures of individuals that are diverting billions of dollars of pharmaceuticals. Controls as well as non-controls are handled by task forces such as the one I operate out of. By the way, I am also involved with the HIDTA Task Force in South Florida. I forget to mention that.

The problem with that is accessibility to information, the paper trail. All of that is paramount towards structuring a criminal case. The majority of the drug laws at the state level as well as some at the federal level, they have been a little bit more flexible in the last several years, deal with trafficking on certain substances. There are only certain controls that there is actually a trafficking standard for at the state level. Everything else falls into a lower level third degree felony. It doesn't matter what the quantity is.

Again, I am speaking from the state of Florida, so it doesn't apply to the other 49 states out there. Some of them are different.

The large scale diversion involves doctors,

pharmacists, employees of doctors' offices and the pharmacies. It deals with wholesalers. It deals with the transportation of the product from one end to the other. It is not all about the prescription end, but the prescription end of it is a significant feature in the diversionary aspect that we are looking at.

The primary drugs that I become -- actually, the biggest problem that we are having right now that we focus on are the controlled substances, dealing with Oxycontin, hydrocodone, hydromorphone, methadone and Xanax. The majority of those are schedule twos. Hydrocodone is a schedule three drug. For the state of Florida, for purposes of prosecution, it has been rescheduled at the state level to a schedule two, because of the potential for abuse and the magnitude of the abuse in the state of Florida.

The only other drug outside of those that I named is alprazolam or Xanax. I apologize for using the brand name, I should say alprazolam. That is the only one that is not falling into a schedule two realm. Unfortunately, alprazolam is probably the most abused pharmaceutical that I see in the state of Florida.

My primary focus when I work a drug investigation is, number one, my evidence, either the drugs or the paper trail leading to the drugs. I need a positive ID on all

realms, meaning from the beginning source of supply to the ending possession. If it involves a fraudulent prescription or a series of fraudulent prescriptions, and I'll go into those a little bit more, I'll need a positive ID on everything from point A to point B. Anybody that comes in contact with that prescription or that individual, the suspect so to speak, I need to gain positive information and identifying information on those individuals, obtain statements from them, and work up my case for prosecution.

The integrity of the evidentiary information is paramount. To date it is primarily the hard copy scripts that we are dealing with.

The information contained on the prescriptions that we are obtaining is not something that can be captured in an electronic format at all times. In your perfect world, if we go to an electronic format, I lose handwriting, I lose fingerprints, I lose half of my identification process, it is gone. There is no way of tracking that.

I need a solid chain of custody, from beginning to end, and I need to document that. On a small scale, a one count prescription fraud case, it takes an investigator approximately eight to 12 hours to work up that single count case.

In the state of Florida I have access by statute to walk into a pharmacy, review all of their prescription records upon demand, as long as I am enforcing the drug laws of the state of Florida, that is the little disclaimer there, and seize anything that is reference to an evidentiary issue on a criminal case. If I don't have specifics on what I need, I will obtain a subpoena for all the records, take them with me and review the information at will. So you can see where a few problems are starting to surface if it is all in electronic format.

From what I heard here yesterday and today, from my perspective an electronic format will almost cloak the information that I need access to. When I say cloak it, it is standardizing it and desensitizing it to a point that it is very difficult for one person to distinguish who touched it, who sent it, who received it. I can't do it on my own. I have to make inquiries to a vendor, inquiries to the pharmacist, inquiries to research all this information.

It is very time consuming enough to retrieve the physical evidence when it is in your hand, so to speak, and to process it that way. By putting it in electronic format, you have extended the investigative time on the cases significantly. You have added additional statements that need to be required. It is not exactly a point to point as explained because of the processing mechanism in

between. I now need to identify who the individuals are working for the vendor that came in contact or who would be processing that information. Not only do I need to identify them, I need to record them in a report, and I also need to be able to tell a prosecutor that they are going to come in and testify if this should go to trial.

They are not registrants under department of health for the state of Florida or HHS. I have no control over them for non-compliance with an ongoing criminal investigation at the state level. If the vendors are outside of my jurisdiction, which is outside of Broward County at this point, or any city jurisdiction, I have just compounded problems significantly. My subpoenas at a state level, you can either honor them or not honor them when you receive them four counties away. I can't serve them on you. I have to rely now on an outside law enforcement agency for service and compliance. So there are several issues there.

As far as identification of employees, again I have to rely on compliance from a vendor to tell me whose initials or whose electronic signature that is related to, who has come in contact with the evidentiary information.

The next thing is encryption and deciphering of the information. Is that changing the format, and again is that going to be qualified as a standardized document or a

legal document for court purposes. Making reference to the birth certificate earlier on, that is a legal document. The prescription, that is my evidence for my criminal case. An electronic prescription coming through the system does not necessarily fit that format. I don't know whether it will be honored by the court system or not. At the state level I can see some significant questions arising.

The next question is, and I didn't hear anybody mention it yesterday or today, computer viruses, problems with the computers, breakdowns, fried hard drives, all of this wonderful technical information that everybody just hates when their computer isn't working. Vendors are not immune to that, the pharmacies are not immune to that, computer systems are not immune to that. If the system is compromised, my evidence is compromised. How do we deal with that? How can we insure the integrity of the evidentiary process as we proceed?

What about bulk records? Historically, although the pharmacists on one hand and the county love me, there are those who do not like to see me walk into their door. I do subpoenas for bulk records. I'll drop a subpoena on a pharmacy for a one-year period of time, all schedule two, threes and fours. The reason for that is, I have several targets under investigation. Not only do I not want the pharmacist to understand exactly what I am doing, it will

compromise my ongoing investigation to provide that information to them.

How do I get bulk information on electronic records? You put it on a disk, I have to have computer access and capabilities of working with that information. I have to access the vendor to decipher what I am looking at, who is this, what is that, what does this mean, who touched this. You have just added about 20, 25 witnesses to a long term case.

For example, on one particular case I am working at this point in time, I have one set of clinics that we are looking at. I have 17 physicians, approximately 15,000 schedule two prescriptions only, we haven't gone into the threes and fours yet, for less than a one-year period of time.

Electronically, and that is all automated, it would be wonderful to have a printout and say, this is great. Unfortunately from a criminal standpoint, the integrity of the evidence, I need to have everything that was included from the point that that prescription was transmitted from point A until it reached the pharmacy.

I am talking about a tremendous amount of additional time in a law enforcement investigation. Unfortunately, there are very few of us that actually do diversion. I am the only diversion investigation -- let me

put it this way, my unit is the only diversion investigative team in our county, actually within a tri-county area, that is specifically assigned to diversion investigations at a local level. It is a very large area, and we are as I said hitting epidemic proportions.

Time, availability, all of this is pertinent to us working our cases, getting in and getting out. We know what the trail is. We just have to have all our T's crossed and our I's dotted. Again, the cost. We have heard about the doctor's cost, we have heard about the pharmacist's cost, we have heard about the vendor's cost. The cost to law enforcement is phenomenal. If you are extending it to a point where I have to do additional subpoenas, and I have to get copies of records and I have to get all of this information, my agency ends up paying for all that. Not only will they not be happy with me, it is extremely taxing.

The cost for the copying of the records, the reproduction of the records in keeping with the integrity, the cost for an expert witness from the vendor or from outside to come in and testify in court, the complexities of the technology needs to be addressed in the criminal case at this point in time, access to the system. As I stated, I have the right to walk into a pharmacy and upon demand they need to make the records available to me.

Generally how that works, I walk in, they point me to the schedule twos or whatever I want. I pull them out, I either hand search them if it is a short term case, I may seize them, take them back to my office, leave them with a receipt, in some cases a subpoena, depending on the nature of the case.

In an electronic system as you are describing, I walk in there, the pharmacist is working on that system. Is he going to step aside for me to go through the records for two to three hours? Is he going to allow me access on his system to review the information that I need to look at reference to my criminal case? That is a point that I just wanted to throw out there.

Again, the review of the records would be compromised. A sensitive type investigation of a nature that I do not want the employees of the pharmacy or the pharmacist to know what we are looking at. If I have to stand in a pharmacy to review these records, there is a compromised feel there. And again, the jurisdictional issues.

Diversion is a multi-billion dollar industry. It is not just in the state of Florida, it is across the U.S. It is not going to go away. It is not going to be significantly impacted by an automated e-prescribing system or prescription monitoring program. There is not one

answer to it.

It is going to take multilevel changes across the board, dealing with federal agencies, state agencies, legislation, the health care institution. I believe e-prescribing is inevitable, and on many fronts it is a wonderful thing. I can't enumerate the benefits; we have heard them all here yesterday and today.

An issue that I take notice with is, let's just get started, and we will deal with it as we go along. It sends chills up my spine, because I know on the flip side what I am dealing with. I have a tremendous amount of investigations now dealing with Internet pharmacies, dealing with the computer systems of doctors and pharmacies, and it is a nightmare, and law enforcement is not set up forensically to take that taxing work in. That affects the crux of the criminal cases, which allows it to fuel and to continue on.

The bottom line is, we need to maintain controls over the controlled substances. We need to have extremely strict standards from the get-go. I understand that the industry wants to deploy a wonderful system over a large scale on a very short period of time, but to do it appropriately -- I heard mention of PKIs and smart cards and things of that nature; if we don't start out with a strict control from the beginning, we are going to have a

nightmare on our hands as this gets up and running. It is going to significantly impact the field of diversion.

No system is secure. Anybody can sit here and say it is the securest system, we have taken this precaution, we have done this. No system is secure. We take preventative measures, we put up firewalls, all sorts of technological dream things. We are open to identity theft, we are opened up to the manipulation of information, viruses, hackers, all of this across the board.

We are dealing with a significant problem with identity theft in the South Florida area, well, in the state of Florida. When there is a will, there is a way. I am seeing more intricate schemes that are ongoing at this point. I have to give credit to some of the criminals out there, because they thought up things that I didn't think would ever exist. They could teach us on how to prevent a lot of this. In fact, I can give you the number of a couple of them, they are in jail right now.

Not to upset anybody, which I know I am about to do in about 30 seconds, the vendors, their companies, their employees, I don't know what these people are. I know we can introduce each other. We are talking about PHI information, we are talking about controlled substances, we are talking about a wealth of information here.

None of these individuals are registered through

the state or the federal government for handling any of this information. Are there any criminal background checks done on any of this? From my provision you are probably a bunch of very, very wonderful people with a tremendous amount of technological information, and you want to do a wonderful thing with a good business.

On one hand, that is the most admirable thing I can think of, especially in the field of medicine and health care. On the other end, you scare me to death, because I don't know who I am dealing with. From a law enforcement perspective it could be a veritable nightmare.

I have no control over dealing with a private vendor. You contract with a physician or a doctor. When I am dealing with a doctor, a pharmacist, somebody that is a licensed health care professional, I can go to HHS or to our department of health. I can go to DEA. There is some recourse there. When I am dealing with a private vendor, there is no recourse. So that is an issue.

I believe there should be some type of certification registration, documentation, some type of cataloguing exactly who all this information is going to. You are talking about PHI information and maintaining it for eight years, ten years, 50 years, I can't remember what the highest bidder was.

You are in a contract with a physician or a

pharmacy. If they are not happy with you, you're gone. Where is that information going? They hold the primary records, they own those, but all of the switching and all of the information and all the audit trails, that goes with you. So if there is a tremendous turnover, we have some issues.

From where I stand as a law enforcement officer in dealing with the legislative issues, if we are talking about e-prescribing in any of the states, I would restrict it to only the states that have prescription monitoring programs. That puts us one step ahead of the game. That gives us a little bit more control over what we are dealing with.

On the second factor, I don't understand all the technology; evidently the PKI is the wonder chip that is wonderful for the doctors as far as identity. The network vendors that needs to be incorporated into the language through HHS are held to the same standard as the pharmacies and the same regulations as the pharmacy, meaning for accessibility of records, that it is somehow adopted into that.

I honestly believe that schedule two prescriptions at this point in the game, especially the schedule two prescriptions of all the schedules, should not apply to an e-prescribing format. I think we need to stay

with the hard copies until a program is up and running and it is working. That would seriously compromise law enforcement, what we are doing, and would significantly fuel the diversionary process.

The gentleman on the end said you were going to throw tomatoes, so thank you very much.

MR. NICHOLSON: Good afternoon. My name is Robert Nicholson. I am an Assistant United States Attorney from the Southern District of Florida. I am presently on detail to the Executive Office for United States Attorneys, where I hold the position of affirmative civil enforcement coordinator.

Among my program areas of responsibility are drug diversion and health care fraud. I have been a federal prosecutor since 1992, and during that time I have prosecuted a variety of offenses, including drug trafficking, computer fraud and general fraud offenses. During the last eight years I have concentrated mostly in the areas of health care fraud, drug diversion and violations of the Food Drug and Cosmetic Act.

During the course of this last eight years, I have lectured and presented extensively on health care fraud and drug diversion issues in a variety of settings, including our own National Advocacy Center, the Federal Law Enforcement Training Center, HHS, OIGs, new agent training

program, DEA and Department of Justice joint training on drug diversion. I have also been asked to speak at a number of private industry conferences, including the American Bar Association, the Food Drug Law Institute and the American Health Literacy Association conferences.

Prior to joining the Department of Justice, I worked a job similar to Sergeant McElhaney. I was a local police officer and deputy sheriff for ten years, so I can personally relate to a lot of what Lisa talked about. On a side note, some of the cases that Lisa has worked over the last eight or so years have been with me, and have been some rather complex and disturbing cases, and time permitting, I will discuss a couple of those.

I have been asked to share with you today a prosecutor's perspective of the drug diversion landscape, to discuss with you the applicable federal criminal statutes and law enforcement's evidentiary requirements in pursuing drug diversion cases involving questionable prescriptions.

Before I go into the substance, I do need to interject a disclaimer, however. Although I am appearing here today in my official capacity with the Department of Justice, the opinions that I express today are my own personal opinions, and they are not necessarily those of the Department of Justice, and are not binding on the

Department of Justice in any future litigation or matter.

Formalities aside, before embarking on a discussion of the regulatory landscape and the issues, I think it is important to describe for you the seriousness of the drug diversion problem in the United States. According to a rather extensive study that came out in July 2005 by the National Center on Addiction and Substance Abuse at Columbia University entitled, Under the Counter: The Diversion of Controlled Prescription Drugs in the United States, our nation is in the throes of an epidemic of controlled substance diversion and addiction.

The study reported that as of 2004, 15.1 million people admitted abusing prescription drugs during the survey. That was more than the combined number who admitted using cocaine, hallucinogens and heroin combined.

As alarming as that statistic is, the report concluded that that number significantly understated the extent of the epidemic. That was so because the survey excluded incarcerated individuals. Also, it was known that the data from surveys from teenagers living at home, it was a self reporting survey, was under reported.

In any event, that number represented a 94 percent increase in the number of people abusing prescription drugs between 1992 and 2003, and a 212 percent increase among teens during that same time period. The

population of the United States however only increased 14 percent during that time. The report concluded that prescription drug abuse now eclipses all illicit drug abuse combined with the exception of marijuana abuse.

What are the consequences of these statistics? According to the report, in 2002 controlled prescription drugs accounted for 23 percent of all drug related emergency room visits in the United States. Moreover, in 2002 controlled prescription drug abuse was implicated in 20 percent of all single drug related emergency room deaths. The drug most often mentioned in connection with these overdoses were opioids, the Vicodins, the Oxycontins and the similar opioid drugs.

More recent data from the Drug Abuse Warning Network, referred to as DAWN, reveals that the number of emergency room visits involving opioids increased tenfold between 1996 and 2004.

Now, what is the federal legal landscape? The principal federal law applicable to prescription controlled substance diversion is the Controlled Substances Act, which is found in Title 21 of the United States Code. Among other things, the Controlled Substances Act makes it unlawful for anyone to distribute controlled substances except as authorized under the Controlled Substances Act.

One of those exceptions to the prohibition on the

distribution of controlled substances is the prescribing of controlled substances for a legitimate medical purpose by a intervention acting in the usual course of professional practice. For a physician to qualify under this exception, it is required that the physician have established a legitimate patient relationship with the patient, for the physician to have medically established the existence of a legitimate and accepted medical need for the use of a controlled substance, and for the physician to prescribe a medically appropriate type and quantity of controlled substance within the authority of his or her state license and DEA registration.

A related exception under the Controlled Substances Act exists for pharmacists who dispense controlled substances pursuant to a valid prescription from a physician. In order to qualify for this exception, the pharmacist needs to reasonably believe that the prescription being presented was issued for a legitimate medical purpose by a physician acting within the ordinary course of professional practice. If the pharmacist does not believe that the prescription is valid, he is not legally authorized to fill the prescription, and would subject himself to civil, criminal or administrative sanctions under the Controlled Substances Act if filling the prescription.

Because of the serious consequences caused to society by the unlawful distribution of controlled substances, the penalties under the Controlled Substances Act are also quite severe. Violations of the Controlled Substances Act, depending upon the type of quantity of drug unlawfully distributed, are punishable by maximum penalties ranging from three years on the low end to mandatory life on the high end, and even the death penalty in cases of drug trafficking murder. There are also alternative civil penalties under the Controlled Substances Act, ranging from $10,000 to $25,000 per violation.

With that backdrop, let me turn to the issue at hand, that is, law enforcement's evidentiary requirements in investigating and prosecuting Controlled Substances Act violations involving questionable prescriptions.

As I see it, e-prescribing presents two main evidentiary issues for us in the law enforcement realm, the issue of authentication and attribution. Authentication refers to our ability to lay the necessary legal foundation to establish that the document we seek to introduce is what we say it is. In other words, that the document sought to be introduced is the original unaltered document or an exact duplicate or copy thereof.

Since we are dealing with the electronic records in the e-prescribing world, that means we will need to be

able to establish that the electronic record we seek to introduce is as originally transmitted from the prescribing source, and establish that it was not subjected to undetectable alteration after the original transmission. Absent that, we may lose the ability to introduce the prescription into evidence.

Attribution refers to our ability to establish beyond a reasonable doubt that a particular person was responsible for creating the document in question. In other words, with respect to e-prescriptions, we need to be able to establish that a particular person authored the prescription in question.

In the paper prescription world, by and large we have this ability. With respect to authentication, there are regulatory requirements that pharmacies retain the original prescriptions, as Sergeant McElhaney discussed. As a consequence, in most cases we have the original prescription in question physically available to us, and we have the ability again in most cases to call a custodian of records to authenticate the prescription. That is, we call the pharmacist or someone from the pharmacy to trial and have them vouch that this is the document that was maintained by them in the ordinary course of business.

With respect to attribution, we have the ability to compare signatures on hard copy prescriptions to known

examples from the purported prescriber. We also have the ability to forensically examine the prescription for evidence of alteration or forgery. By and large, this gives us the ability to determine whether or not the purported prescriber was actually responsible for issuing the prescription.

If we are to maintain our ability to effectively enforce the Controlled Substances Act with respect to the diversion of prescription controlled substances, it is imperative that any system of e-prescribing adopted provide law enforcement the ability to authenticate prescriptions, to hold prescribers accountable, or to definitively identify alterations and forgeries within the legal parameters that I have just discussed.

Quite frankly, it is also in the best interest of the medical and the pharmacist communities as well. It is in the interest of legitimate and well-meaning physicians to have the assurance that their prescriptions are not subject to alteration or forgery. Not only does this protect the health of their patients by assuring that they only receive the drugs and quantities of drugs the physicians intended, but it also reduces the likelihood that the physician will be the subject of a criminal diversion investigation, or some sort of licensure or DEA registration action or sanction. Likewise, it is in the

interest of pharmacists to have a higher degree of assurance that the prescriptions they receive are less likely to have been forged or altered.

To switch gears for a minute, although I understand that the focus of this hearing is on the diversion of controlled substances, I would be remiss in not mentioning other areas of law enforcement interests that would be affected by the decisions made regarding e-prescribing.

As I mentioned in the introduction, I have an extensive background in health care fraud prosecutions, and also Food Drug and Cosmetic Act violations. The prescription plays an important role in many of those health care fraud and Food Drug and Cosmetic Act cases.

Turning for a moment to non-controlled substances, controlled substances account for about ten to 11 percent of the prescription drugs filled or dispensed during a calendar year. That means the other 90 percent out there are non-controlled. Just because they are non-controlled doesn't mean that they aren't subject to abuse. Among the non-controlled substances that are subject to abuse are some of the so-called lifestyle drugs, including Viagra and other performance enhancing drugs, and also muscle relaxants such as Soma, which drug addicts often use to enhance the effect from abused controlled substances.

As a side note, since Lisa is here, Florida actually scheduled -- didn't they ultimately schedule Soma as controlled?

SGT. MC ELHANEY: Yes.

MR. NICHOLSON: Because it was such a drug of abuse in Florida, they actually scheduled it as a schedule four.

As I suspect, you may not be aware, there are now rogue websites out on the Internet that provide instructions how to mix and combine non-controlled drug and over-the-counter drugs to make a combined substance with hallucinogenic or mood altering effects. Any kid out there with access to the Internet has access to this information.

Also, I think one need look no further than local news to learn about farming parties, and from Lisa's remark I assume that someone has already mentioned the farming parties out there. I would echo what Lisa said, that it is not just coming out of medicine cabinets. It is much too big of a problem. We have empirical evidence to show that it is not just drugs coming out of medicine cabinets.

Likewise, one need only open their e-mail box, I suspect, to find solicitations from online pharmacies or a simple web search defined a number of so-called online pharmacies that are willing to provide controlled and/or non-controlled drugs based on a prescription that was based

only on an insufficient online questionnaire.

If we are acting today out of concern for the harm caused by the diversion of controlled substances, I would respectfully submit that the same safeguards should be placed on the prescriptions for non-controlled substances to address the harm posed by their diversion as well.

Another area of concern, and one that I think argues very strongly for a uniformly secure standard for all electronic prescriptions, is the area of fraud on health care payors, including the Medicare and Medicaid programs.

As reported in the September 2005 report on the use of health information technology to enhance and expand health care fraud activities, which was prepared for the Office of National Coordinator for Health Information Technologies at the U.S. Department of Health and Human Services, our co-invitees here today, fraud has a significant impact on the U.S. economy.

The National Health Care Anti-Fraud Association estimates that of the nation's annual health care outlay, at least three percent, or in real dollars, $51 billion, was lost to fraud in calendar year 2003. Other estimates by government and law enforcement agencies place the loss as high as ten percent of our annual expenditure, or $170

billion on an annual basis.

I will tell you, coming from South Florida, I think both of those estimates are low, at least in my area of the country, where health care fraud is truly at epidemic proportions. I hate to keep using that epidemic word, I know it has been bandied about, but it really is an apt description.

The report concluded that it is essentially that fraud management programs be built in the National Health Information Network infrastructure as part of its early design, to echo something that Sergeant McElhaney said. This reports states that designing fraud management functionality into the National Health Information Network has the potential to significantly reduce health care fraud losses.

The report contained a list of specific recommendations that were compiled by a cross-industry group of 22 stakeholder interests. I would like to quote from a few of them to you, since I understand there is a lot of vendor folks here today, and I would commend this report to you in considering your options.

The report's first recommendation was that the nationwide health information network's policies, procedures and standards must proactively prevent, detect and support prosecution of health care fraud rather than be

neutral to it. The specific sub-recommendations were, develop enterprise management and development policies for all stakeholders that will render the National Health Information Network inherently resistant to fraud and support fraud management. Fraud management is defined as the prevention, detection and prosecution of health care fraud.

The next sub-recommendation was, build in as part of the National Health Information Network infrastructure standards procedures and prototypes to facilitate nationwide health care fraud management. Finally, to certify electronic health record software features and functions that are required or prohibited in the National Health Information Network infrastructure to enable effective health care fraud management.

The second recommendation was that electronic health records and information available through the National Health Information Network must fully comply with applicable federal and state laws and meet the requirements for reliability and admissibility of evidence. Specifically they recommended that standards be established for the electronic maintenance, submission and disclosure of health and financial information contained in the electronic health records. Standards should address accuracy, completeness, accountability, access and

availability, audit availability, identification, authentication, non-repudiation, integrity, digital certificate, digital signature, electronic signature and public key infrastructure.

Finally, there is actually a list of ten of them, but I am only going to read the three that are most pertinent, under seven it was that electronic health record standards must define requirements to promote broad management and minimize opportunities for fraud and abuse consistent with the use of electronic health records for patient care, and it basically reiterated what was in recommendation two in terms of the ability to authenticate the records for use in prosecutions and other government events.

With respect to Medicare Part D, the report states that prescription drug plans are expected to be the new target for health care fraudsters. Part D is expected to cost $720 billion over the first decade of its existence. The report went on to note that prescription drugs are especially vulnerable to fraud, waste and abuse.

To put the loss to health care fraud in perspective, the report notes that identity theft, which is accurately stated, perceived as a huge problem. The amounts lost to identity theft amount to $788 million annually. Health care fraud by contrast costs the public

100 times that of credit card fraud on an annual basis.

I can tell you that from firsthand experience, the Medicare and Medicaid systems are highly vulnerable to fraud involving prescription drugs. The key document in many of the prescription drug schemes is the prescription itself. Accordingly, our ability to investigate and prosecute those fraud schemes is often dependent upon our ability to authenticate and trace prescriptions.

The same holds true in the area of durable medical equipment fraud. I can say with a high degree of confidence that tens if not hundreds of millions of dollars are lost annually in DME fraud schemes nationally. In fact, coming from South Florida, that number probably applies to my area alone, forget the rest of the country.

I have prosecuted a number of those cases. I can tell you, there is one under investigation right now. One scheme, $250 million lost in six months. It is a big problem. Again, like prescription drug diversion fraud and Part D fraud, the prescription is one of the central documents in perpetrating these schemes.

Given the human toll and economic loss being experienced under our current paper based system, any change to an electronic system that would lessen the safeguards currently existing, in my humble opinion, would be irresponsible. The costs of implementing a secure and

closed system for e-prescribing are dwarfed by the amount currently being lost to fraud on the health care system. In my opinion, and based upon the findings of the Office of the National Coordinator report, would also be dwarfed by the potential savings realized in the reduction of fraud on the health care system.

If you take nothing else away from my comments today, I would ask that you at least leave with the understanding that any weaknesses in security of the e-prescribing system adopted will be found and will be exploited by the criminal element and the cost to society of a lax system will be tallied in billions of dollars of taxpayer dollars stolen, and in many lives lost to addiction and overdose.

Thank you.

MR. WINSLEY: The good news is I am the last speaker on the last panel on the last day. The bad news is I'm the last speaker on the last panel of the last day. We are ahead of time, and I have got three hours worth of slides. The good news is, Mandy told me I would be lucky to get three minutes on my computer time, and that is my only set of notes right up there.

I am Bill Winsley. I am executive director of the Ohio State Board of Pharmacy. Since everybody else has given their pedigrees and their background, I will run

through mine quickly. I am a pharmacist as you can see. My grandfather was a pharmacist. My mother and my father were pharmacists. My wife is a pharmacist. My wife's sister and her husband are pharmacists. My oldest daughter is a veterinarian.

My grandfather had a retail store in Zanesville, Ohio. My mom and dad bought it when I was nine. I grew up in a retail pharmacy environment. I turned traitor and got my masters degree in hospital pharmacy administration. I worked hospitals for 14 years, and then I came with the Board in 1988, where I started as a pharmacist investigator in the field. I worked the field for about three years, and my predecessor, Frank Wickham, somehow dragged me into the office as assistant exec, and in 1998 I took over as exec.

I tell you that just so you will know where I am coming from. I have had experience retail, hospital, the enforcement side. As you will see, I spent a great deal of time while I was in the field testifying in criminal court as well as administrative board hearings, participated in criminal investigations, administrative investigations, plus I got to play the bureaucrat and walk in and do inspections. So I have a little bit of idea of both sides of the fence here.

There is one thing about the State Board of

Pharmacy in Ohio that makes us a little different than most of the others, and probably slants our viewpoint a little bit. As all other boards around the country, we are a licensing administrative type agency. We license pharmacists, pharmacies, wholesalers, prisons and jails, EMS squads. If it moves and has drugs, we do our best to charge it money.

But the other part of our duties, Ohio does not have a state police. We have police forces in our local jurisdictions, and we have county sheriffs, but we do not have a state police. So the Board of Pharmacy is also a law enforcement agency. We are the only state agency charged with statewide drug law enforcement.

We specialize, if you will. Our area of expertise is prescription drugs. We do not go out on a street corner and arrest the street corner drug dealers, although those types of drugs are quite frequently involved in our investigations. We have nine pharmacist field staff, and we have 15 ex-law enforcement officers, many of whom had narcotics and vice experience before they came with us.

If you will pardon the expression, we are what I call an equal opportunity abuser. We pick on doctors, nurses, veterinarians, dentists, pharmacists and the general public if they violate the drug laws. So we come

at things maybe just a little bit differently than some of the other administrative agencies. I have listed the Ohio Revised Code chapters that we enforce. We also push the federal laws when we get a chance.

The question that has been running around, nobody has ever asked it, but I kind of hear it in the background sometimes so I added a couple of slides last night, why do DEA and the boards exist? And my apologies to DEA for speaking for them. If I say something wrong, I know I am going to get my legs cut off here. But I tried to phrase it as succinctly as I can, so I have combined things.

But basically, our job as you heard this morning is protection of the public. We are a licensing board, but our job is not to protect pharmacists. Our job is to protect the public, primarily from our licensees who act in an illegal, immoral, incompetent or impaired way. That is for the Board. DEA I don't believe has a moral turpitude clause in their enforcement section, so they can't do that. They specialize primarily in the illegal. We have a great deal to do with that, too. But that is our role.

Most health care professionals -- and as my father used to say, I am preaching to the choir here -- but most health care professionals, the people that are at this meeting, most people are truly honest, they truly care about their patients. But there are those who do not, and

those are the people that DEA exists to deal with, that the police force exists to deal with, that we exist to deal with. We need the tools to be able to do that, hopefully in a way that allows us to deal with the dishonest people, but it minimizes the effect on the rest of you that are trying to do a good job and trying to take care of patients, trying to get your business done.

That is pretty hard to do. Sometimes we feel like this individual right here. The example I use is, I have a good car, the roads are well built, my car will do 75 or 80, and I drive a lot of miles every year, I can handle that car. The speed limit is 55, and if I go 75 or 80 I am in a heap of trouble, but there are some people out there that can't even drive 25 and do a good job at it, so 55 is a compromise, and we all have to learn to deal with it.

It is the same with our laws. As you have already heard, we have got to have the ammunition or the evidence that we need to deal with the bad people. Hopefully we can get it in a way that minimizes the effect on the rest of you.

We have been involved in this computer access business for a long time. Back in 1991 I sent a letter to a hospital outlining the fact that we had some principles about computer access. The first one, we have heard for

the last two days, the current paper and telephone system has some major flaws to it on the user end, it has some pluses from the law enforcement end, but we made the determination back in 1991 that as we were looking at electronic systems and as we were approving electronic systems coming into us saying it is as good as the current system is about like saying my ingrown on my left toe is as good as the ingrown toenail on the right toe. It doesn't help you any.

Electronic systems can and must do better than the current system. This is our basic premise. Passwords are worthless as a means of computer security in a health care setting. Please read the whole sentence. I am not going to quibble with you. If you or I are sitting in our private office and we know who is behind us, we know who is in the room and maybe, although you will see later that is a big maybe, maybe we have a secure password.

I do my banking at home over the Internet. I'm afraid my password isn't very secure, but I know who is in my office and I have the blinds shut behind me, so at least I have a little bit better chance. Think about your typical health care setting. If you don't work in a hospital and never have, you have visited patients in the hospital. Think about the nursing unit. When have you ever seen the terminal in a nursing unit where it has been

private? Think about a pharmacy. Where is the computer terminal in a pharmacy? It is all out in the wide open spaces. Usually on a nursing unit what you have to do is elbow your way into the terminal, excuse me, excuse me, and get your hands in there and get started before somebody else grabs it.

Another caveat. Passwords only protect honest people from other honest people. I don't look when you enter your password. I deliberately avoid looking. I don't want to know what your password is. When I was out doing investigations, that was a different matter, but I don't want to know. But the problem is, for most health care professionals, we have a specified method of choice for entering our password, and it is best defend by this phrase: Seek and ye shall find. That is how we enter our password. Most of us are not typists, and we can't do this. You computer people can do it fast. This is humorous, but it is serious.

We are not able to generate a password by calculating the hexadecimal equivalent of our dog's birthday raised to the 27th power and then divided by the Julian date. You guys from the computer end can do that in your heads; we cannot. That is a password off of one of my old Semantec things, and that is what I had to type in in order to allow my Semantec Norton to work. I couldn't make

that up, and for heaven's sakes I couldn't remember it. I am a health care professional, I am a pharmacist or I am a doctor trying to get into my computer system. The phone is ringing, somebody is talking to me, I have got to remember that? Or as I heard this morning, if I mess up three times, I'm locked out? Meanwhile the patient is convulsing on the floor and I need that drug. We have got a problem here, folks.

Then you are really secure. So six weeks later you come in and tell me, it is no good, I've got to learn this one. I hope I have made my point. Passwords are worthless. Some of you are really nice and you let us make up our own. What do we use? The first one I made up, although I'm sure it is there. The second one, one of our guys was in a hospital in Cincinnati. You know the football team in Cincinnati? Back then we used to call them the Bungles instead of the Bengals, and nobody in Cincinnati liked them.

But anyway, this nurse was showing how secure her floor stock machine was. She took our agent, and he stood back a ways away, and she entered her password to show him how secure it was and he said, I see you are a football fan. Bears.

I was in a doctor's office looking at a prescribing system, because as you will see, we approve

them before they can use them. The office manager was really proud about how secure it was and how she and the doctors were the only ones that were allowed to transmit the prescriptions come in and watch me enter my password. Her first name was Kim. Guess what her password was? Real life stories. I don't make up stories, I don't have to. We have plenty.

Bears, Kim, that's ours. Or as a couple of other people have admitted and as I have done in the past when we have had non-repetitive passwords that we have to change, for awhile my password was WTW01, 2, 3, 4, every time I had to change it. Some of you in this room are looking at the floor because you do it, too. How secure is that?

Anybody that is within five feet of a health care professional in the environment where the terminals are located can pick up that password, because if it is too long we write it down, and if it is too short we got it on the first time. I only gave you two examples of picking up passwords. Our guys have done it a lot, because of the environment. In fact, some of the floor stock machines require a nurse, if she is going to return a product, to have another nurse there. They both enter their passwords. They both are standing right next to each other while they enter their passwords.

To go to criminal court with a case, and you have

already heard the need for evidence, but we need to prove something beyond a reasonable doubt. I cannot -- and I have testified a lot in criminal court -- I cannot sit on the witness stand, swear under oath that because your password said you issued that prescription, you filled that prescription, you administered that dose to the patient, that you are the one that did it, if the only access is a password. I cannot in good conscience swear that that is the case, because I don't know that.

We have had cases of people stealing drugs using other peoples' passwords. It was very unpleasant for the original person for awhile until we realized that there was a problem. We can't even use it in administrative hearings where the burden of proof is reliable, probative and substantive, which is a whole lot lower burden of proof than beyond a reasonable doubt. I can't even get up in a board hearing and say it looks like you did this, because I know that you didn't necessarily do so.

In 1995 therefore, we promulgated a rule. We put in a definition of positive identification, and throughout our rules, every place where the word signature, initials, anything appeared, we switched it to the words positive identification. We require positive identification for every individual who prescribes, administers or dispenses -- we call them dangerous drugs, you can think of them as

prescription drugs, including controlled substances.

We started off with this paragraph. It may not rely solely on the use of a private personal identifier such as a password. It may not rely solely on a password. We have had that rule since 1995. You also have to have a secure means such as -- and this list has changed a couple of times since 1995, but we list a few things, magnetic card reader, bar code reader, thumbprint reader or other biometric. One of the additions was a proximity badge reader. Those just came out recently, where you have an ID badge that has a transmitter in it so the computer knows when you are within a certain distance and you walk away, the computer screen locks, so we know that at least your badge is there.

A board approved system of randomly generated personal questions, which sounds a little weird. The last thing that you will see is other things people come up with that the board approves, because we knew that when we did our original list, there are a lot of bright minds out there, and we weren't thinking of everything. Sure enough, the people at Ohio State University hospitals came in to us and said, what if we come up with a list of 75 personal identifier type questions, let the person pick out 15 that they can answer right now, and we will give them two, non-repetitive. We did the calculations, and if I remember my

statistics, combinations and permutations, right, that means that if I am looking over your shoulder and I find out your dog's name and your mother's maiden name and I go to another terminal, my chances of getting the same two questions in either order if I did the math right are one in 105. We thought that was pretty good odds, so we allowed that.

The trouble is, we didn't anticipate the problems in advance, like you are being asked to do here. We forgot to have them program in that they had to be unique answers. One of the bright medical students at Ohio State University Medical Center found out that he could enter Brown for every question. You know medical students, they are the same as pharmacy students, nursing students and general human beings; it didn't take long for every intern and resident in that place to know the secret. All you have got to do is enter one word, and then you don't have to remember your mother's maiden name and the city where you were born. Obviously that has been fixed now. But the reason I tell you that is that we have to anticipate ahead of time. It is a lot harder to go back and change things.

We have been forced, pending the resolution of this issue that we are here today, to allow a printout, because some of the electronic prescribing systems particularly have no way, those with PDAs, for example, it

is hard to put your thumb on a PDA and get it to recognize you, so we do allow a printout of all of the prescriptions transmitted under the doctor's name.

We require the doctor to print them out and store them. They have to be mindless printouts. In other words, everybody comes in and says, we can do this report. We don't want to hear you can; we say you will, and it needs to be mindless. A doctor walks in and says print my report. The system knows when the last report was printed, prints it out with that date and time range on there. The doctors or office managers are responsible to be sure they are consistent.

One of the ways you gyp that system is to come in on Saturday. You know the doctor's password because everybody knows the doctor's password, I don't care how you much you tell the doctor not to give it out. So the nurse or the receptionist comes in on Saturday, transmits scripts, prints the report, throws it out. So we have the signin sheet dated and time, from-to, and they need to be consecutive. That is not something I recommend that we adopt in federal, because it is a pain and it generates paper, but for a short term solution, pending a resolution here, we have allowed that. Then we do have anything else that applies.

We have been doing two factor for quite some

time. In other words, if you have something physical, we also require a password. So you have got to have both. Think of your bank card when you get money out of the ATM. You've got two things, you don't just have one. If I am looking over your shoulder and get your password, which is fairly easy because they are out in the open, I still have got to knock you upside the head and steal your card in order to get money out of your account. Two factor.

I didn't have access to the SureScripts fancy slide, which I thought was very good, and I would have liked to have had it to use here. But I had to make my own last night.

This is the system that we are looking at. Doctor's office, vendor and switch to pharmacy, and there may be a couple of other computers in there. You go to the vendor, then to the switch. You may go from the switch to the headquarters to the pharmacy.

I don't want to address what goes between the doctor's office and the pharmacy, whether we do PKI, whether we do some other kind of super encryption. That is for you experts that know what you are doing. I am looking at cases that we have worked, and what I am here to tell you is that if all you have is a password, you can't tell me who is sitting at that doctor's terminal. You can guess, and if the doctor is honest you will be right. But

I can't go into court and say, Dr. Smith wrote this prescription.

I forgot to tell you, we have a lot of experience in court. Over the four-year period that ended in 2005, our 24 pharmacists and agents combined, we caused the arrests, either investigations we did ourselves or in which we were the lead agency, we caused the arrest of over 200 nurses, over 50 pharmacists, 35 physicians, several dentists, a couple of veterinarians, and quite a few of the general public. The nurses were primarily theft of drugs, pharmacists and doctors were drug trafficking, false prescriptions. Before you start feeling sorry for the doctors, they were not doctors taking care of patients. We have them on tape saying what drug do you want and how much money do you have, for that much money I'll write you this many scripts. Or mostly male doctors providing drugs for personal favors from female patients, I guess that is the polite way to phrase it.

We have a lot of experience in criminal court, and we need to take evidence in there that we can convict. A lot of those doctors' convictions involved false prescriptions, writing prescriptions not for a legitimate medical purpose. If we don't know who is sitting at that doctor's terminal, all we know is that somebody in the doctor's office sent that script out, and if the doctor has

a good defense attorney, which they can afford, their first statement is, I didn't write that, somebody must have got my password, and where are you?

In the paper system, you already heard it; we have got handwriting experts. We can get in there and we can say, sorry, doc, you wrote this. But unless my people are in there right after the order is entered with their handy-dandy fingerprint kit, which we don't have any of, by the way, we have no way of knowing who is sitting at that terminal. So the bottom line is, you can't tell me who is sitting there.

My final comment. I hope we have some good questions, because there is a lot more, but I really wasn't allowed three hours. If you are going to do security, you need to come up with security at the order entry point. That is for all prescriptions. Our rule applies to all prescriptions because as you heard, it is not just controlled substances that we have problems with.

Your security needs to start at order entry, otherwise you are wasting your time with the rest of the system. If garbage goes in the front end, it doesn't matter that the rest of the system is secure. It does help the person putting it in, because they know it is going to come out the other end, but it doesn't help the pharmacist a bit if it is not secure going in the front end. That is

the only way you are going to help the pharmacist.

I heard several people here saying, leave it up to the pharmacist. I'm sorry, but when you get a hard copy scrip, the way pharmacists pick up forgeries is, there are different colors of ink, there is different handwriting, there is something funny about the scrip.

The best example is, we had a prescription brought into a pharmacy written for TALL ONE. The pharmacist filled it. The pharmacist got in a heap of trouble. But they pick up on those differences, like bad verbiage, ink, handwriting. When it comes out over the computer, it is spelled perfectly, it is written perfectly, it is very legible, it is very safe. But that pharmacist isn't going to be determining whether a prescription is fraudulent or not from what comes out of the computer, like they can with a handwritten.

We like electronics. We have approved over 22 electronic prescribing systems in the state of Ohio. We have reviewed however over 30. That is the other thing I was hoping somebody would ask me, but I am going to sneak it in here. What you saw here today was the cream of the crop. If every vendor acted the way the four vendors we had on this panel, I would have to go find a real job.

There are vendors out there we have not approved because they cannot meet our security requirements. There

are vendors out there who leave it up to the office manager to certify who can have access to the computer. They don't all do in there and do the doctor face to face and get copies of licenses. I wish they did.

The bottom line is, we need to know who is there, we need to be able to prove who is there, and we need to be able to do that for all scripts, not just controlled substances.

My final slide. I am to the point where I am getting AARP requests to join, which I have proceeded to throw. I am also a grandfather, so I have prerogatives on my final slide. That was a year ago, but usually that is the effect I have on my audience.

So with that I'm done, and we will go to questions. Thank you very much.

MR. CAVERLY: Now I have to play the straight man after that. Thank you, panelists, for your participation in our process this afternoon. We are going to once again have questions posed by our questioners on the stage. Tony, I'm going to start with you.

MR. TRENKLE: Thank you, Mark. I appreciate all the comments and the insights that you brought in terms of law enforcement and some of the challenges you face.

One of the questions I did have was concerning evidence today. You mentioned the key pieces of evidence

you need to do prosecution today. What are the key things that prevent you from getting that type of evidence today? In other words, you talked about how you could define authentication, how you could deal with non-repudiation. What are things that cause you to fail when you try to prosecute someone today, and what are the reasons for that?

MR. NICHOLSON: I assume that is directed at me?

MR. TRENKLE: You would be a likely target.

MR. NICHOLSON: I'm not sure I fully understand the question. I didn't really follow you.

MR. TRENKLE: If you prosecute someone and you don't achieve a conviction, what are the reasons today in the paper world why that wouldn't occur?

MR. NICHOLSON: Well, thankfully I haven't had that circumstance yet when I haven't secured the conviction when I brought the prosecution. But each case is so factually unique, I don't know that I can identify one particular thing or even a group of things that would impair ability to authenticate in the paper world.

One of the things that you look for is -- the problem is, there are so many different schemes that it is difficult for me to answer your question, because I would have to overly generalize.

MR. TRENKLE: I am just trying to draw an analogy between the paper world and the electronic world. I know

there are certain ways in the electronic world, such as was discussed this morning with the audit trails and other types of activities that you don't have in the paper world. One of the things is obviously recordkeeping at the pharmacy or the providers.

SGT. MC ELHANEY: If I can for a second, some of the things we all run into regarding the paper trail, I may seize 3,000 prescriptions relevant to a particular investigation. Of those 3,000 I may only get a positive identification on ten percent, that I can positively link the individual to that ten percent. A lot of it is because of the transition of employees in the pharmacy, the memory of the individuals. I have to do photo lineups with each and every item that comes through. Then the chain of custody.

I'll be honest with you, some of them we can't find in the pharmacy. It is a rare instance that we can't find them. They are usually misfiled, and again that is just a recordkeeping issue. But from there one of the primary pieces of evidence is the signature cancellation of the pharmacist on that evidentiary piece of information.

Now, I have a prescription there, and when the pharmacist fills it, he is required by law to cancel that with his initials and an identifying signature on that. It does not always match what is in the computer. If he is

logged onto the computer as John Doe but Bill Smith is the pharmacist filling it, he may go into the computer, fill it, if he cancels out the prescription the sticker on the back may say one pharmacist but the cancellation on the front says another.

So the integrity of exactly who you are dealing with, you can't rely on what is always in the system. We will find -- I don't want to say a tremendous amount of discrepancy, but discrepancies of that nature.

I only file criminal charges on what is black and white. There is so much gray involved in positive identification and relationship to the evidentiary information, that although I know an ongoing scheme where they may have gotten 300,000 dose units, I may only be able to prosecute them on charges that equal out to maybe 30,000 dose units.

MR. WINSLEY: In Ohio, because of our positive ID requirements, we don't have the problem with ID'ing who is doing that quite so much.

The only other reason we have had problems is one investigation I was doing. I had the pleasure of walking through a burned-out pharmacy a couple of days after I was in there, and amazingly enough, all records and the computers had melted, but that is what you need to expect.

Mis-files are a problem that electronic would

certainly help. Another part of our requirements that came up with the electronics, we do require daily backups because of the fact that it is pretty easy to manipulate.

With the paper records we haven't had much problem, given the ability to walk into the doctor's office and say, did you write it. We have the ability to walk into the pharmacy and grab the scripts. There is not that much problem with the evidence disappearing unless it is intentional, and sometimes you lose.

MR. CAVERLY: Questions from DEA?

MR. GALLAGHER: I have to admit that this is the first panel that totally speaks my language, so it is hard to come up with lots of creative questions because I get it, I understand it. I have learned so much the last two days.

But my question would be to you all, in your experience of doing investigations, have you seen a large number of cases that involved office staff? I know in my personal experience I have seen office staff forging doctor's prescriptions for their own addiction as well as distributing to other patients who come to this doctor. So I was just curious if you could comment on that.

SGT. MC ELHANEY: On an average, we arrest one to two members of an office staff, whether it be doctors or a pharmacy staff, a week. That is just in my county, that is

just my jurisdiction. So I would say that is a significant issue, yes.

MR. WINSLEY: It has been a significant issue. I say in talks quite frequently that one of the worst mistakes that we ever made as regulators was letting an office person serve as an agent of the physician. Politically speaking, trying to change that now would get me shot, but that is a very big problem.

We have prosecuted a lot of doctor's office people and a lot of pharmacy technicians and clerical staff who are masquerading.

SGT. MC ELHANEY: If I can compound that for just a second, also one of the problems that we have ongoing is, in many instances even if we don't go to the route of prosecution because we don't have sufficient evidence for a prosecution, the termination of that individual, they go around the corner and they hook up with another doctor's office or another pharmacy. They are repeat offenders. Their primary goal is the obtaining of the drugs, and they will find a way to do it.

So I have licensed and non-licensed individuals that we deal with repetitively, again and again.

MR. NICHOLSON: Just to echo what Bill and Lisa said, although they certainly have seen a much wider range and volume of cases than ultimately make it to me, I would

say that in at least a third of the diversion cases that I have been involved, controlled or non-controlled, have involved an office member who has either obtained prescription pads laying around, forged prescription, or called in unauthorized, or been in some way involved in the diversion. So I would say it is a fairly high rate of incidence.

MR. TRENKLE: Just following up on that, one of the advantages I would see of electronic prescribing would be the ability of the audit trails to pick up anomalies. If an office person went from one place to another, would it not be possible to pick up somebody's anomalies a lot easier with electronic prescribing than it would be otherwise? Do you have any thoughts on that?

SGT. MC ELHANEY: Not necessarily. A lot of times they go unreported. The physician terminates them on suspected abuse or fraud. They don't want to make a full report that they have been compromised in some manner, and they just let the individual go.

A tremendous amount of time, I run into the factor of the doctor says, I don't want to press charges. I say, you don't understand. The way the statute is written, the state of Florida is actually the victim, so you are a witness in the case and you are required by statute, by regulation, to cooperate with law enforcement.

They don't want to do it. So the problem progresses. It just festers and grows.

MR. WINSLEY: Unless they are feeding a personal addiction, usually the quantities are not that much to create an anomaly. They are treating family and friends, they are providing drugs, either controls or non-controls. They are calling in scripts. But as Lisa said, if the doctor even has the suspicion, they are fired, they go someplace else and there is no tracing.

With an electronic system, if they are dumb enough to use their own password, if that is all that is required to get in, then yes, that would be easily traceable. But the ones that are doing things illegally are not going to use their own password.

MR. NICHOLSON: I would say that the potential for detection would be there if there was a sufficient volume. But I think Lisa and Bill are correct, there is not going to be that much of a spike generally that it is going to be detected, except for with some incredibly sophisticated analysis. I don't know how much that would add, but it is certainly not a panacea.

MR. CAVERLY: Questions from the DEA side?

MR. GALLAGHER: One more. This will be the last for mine, I believe. This goes to Bill. The doctors who are now having to do a two-factor security level, what is

the response from them? Do they embrace it, do they not adopt it, has it become a hindrance?

MR. WINSLEY: As politely as I can phrase this, we don't give them a choice. The way that we handle the prescribing systems, we have got a rule written that they can only use an electronic prescribing system if it is board approved. We bring the systems in, we review them, we take them to the board and the board finds the system to be approvable pending final inspection. It is installed. At least the first doctor or two were in there with the system. We basically pound it into their heads that we will be back, and do it.

Most of them, once they understand the reason -- I have talked to a lot of doctors about their prescribing system, and once they understand the reasons and the fact that it is for their own protection, they are really not -- we do our best to make it as harmless as possible, but they understand that it does protect them, particularly when I tell them about all the office staff that have been getting drugs. So we really haven't had a lot of complaints about it.

MR. TRENKLE: Bill, you had raised the issue of a number of e-prescribing systems that had gone before your board, and that you had approved 22 out of a larger number. Are you saying that you would support a certification of

the e-prescribing systems much as the CCHIT has been looking at EHRs?

DR. WILLIAMS: Basically, certification is what we are doing ourselves. So if it were done, and if it were done effectively, it would save us a lot of time.

I'm not saying that the other eight or nine that we have seen are not at some point going to meet it. Nearly every e-prescribing system that has come in to see us has gone out with repairs to do, because they all come in with a password system, except for one guy that pulled out a fingerprint reader and a card reader out of his pocket, and a couple of other things, and said, which one do you want me to hook up. But one system out of all of those that came in with something other than a password, most of the time they go away and they are back in a few days with the response.

So we have some that are still out there pending, but there are some that were so far out of line that they weren't going to make it. So yes, if there were some certification that were appropriately done, that would be wonderful.

MR. TRENKLE: These systems that you have approved, would you also -- would they meet the requirements that DEA is looking at under the Controlled Substances Act?

MR. WINSLEY: Probably not. If PKI is thrown into the mix, I don't think so. Quite a few of them right now are using that written report we talked about, which on a nationwide basis I think DEA would have trouble with. We have trouble quite frankly with 25 people, 24 people in the field.

So that is not a good solution, but that is what most of them are using right now. Everybody is waiting for this issue to be resolved. Then I think we will see some fixes. But right now most of them are using the report, and that is not something that I would expect DEA to go along with in the long run.

MR. CAVERLY: Questions from DEA?

DR. MAPES: Bill, you have had some experience in your state with prescribing electronically non-controlled substances. We heard this morning from the vendors that they haven't seen any instances where there have been prescriptions that were sent through the systems that weren't legitimate.

Have you seen any of those in your staff that were office staff? And have you seen any that were other than office staff, where somebody used the systems illegitimately?

MR. WINSLEY: No, we haven't. Part of the reason is that we are back to -- well, we just haven't. There

haven't been -- in talking to pharmacists, they are not getting that many yet. We have approved the systems. They have been sold. There are some docs that are using them. But in the overall scheme of things, the overwhelming majority are still walking in the door on a piece of paper.

So we have not had a problem yet. I say yes, because like everything else, I expect some soon.

MR. TRENKLE: Just to follow up on that, Bill, what would you propose to put in place to prevent this from happening in the future? You said yes; I guess you are referring to the fact that the volume is not there at this point? What can we done as the volume inevitably increases?

MR. WINSLEY: We need to get away from that paper report. That is why I say yet. If there are doctors in the audience, I apologize to them, but the problem with that paper report is, we all know that the doctors, some of them, are signing them, and the office manager hands it to them, and they are not looking at it.

It is still a password-based system. We have got to get away from that password-only system. We have got to have something secure at that computer terminal so that the doctor himself or herself assumes responsibility and liability for that prescription. Office staff can be involved as far as we are concerned, I don't know about

DEA's opinion, but that doctor has got to have a way to securely assume responsibility and liability for that prescription, be it controlled or non-controlled.

Right now it is a password system. In some of those offices, the office manager runs a report, takes it to the doctor and says, sign it. You have heard how busy doctors are. So it is not an ideal solution. We need to go something that is a little more secure in the long run.

MR. BARBER: Robert, I think my question is primarily directed to you because of your experience with issues beyond controlled substances and diversion with health care fraud and other fraud issues.

What is your experience as far as the increasing use of electronic records and their effect on fraud and forgeries generally, whether it is controlled substance or otherwise?

MR. NICHOLSON: I have not been directly involved in any case with electronic prescribing, so I can't really comment on what impact it is going to have. To my knowledge we don't have that in my home jurisdiction, unlike in Bill's state.

In terms of the effect of electronic records in fraud, I think one need look no further than identity theft, scams involving the Internet or Internet pharmacies to see that there is an increased level of anonymity

involved when you move to a purely electronic record, for the reasons that Lisa and I both mentioned. When you move away from paper you lose that level of forensics that we have in terms of handwriting, ink analysis, fingerprints and the like.

So I think that there is no question in my mind at least that any time you inject that level of anonymity that comes with an electronic system without adequate safeguards, knowing who it is you are dealing with on the other side, it increases the vulnerability of any system to fraud.

I think we all probably get those e-mails that when you open them up they say, do you know who this came from. I'm not sure how much any of us when we click that yes or no, do we know who it is coming from. I will defer to the technical folks here, but it is very difficult in that electronic world to know, unless you saw it sent, who sent it, what is attached to it.

So I think it most definitely increases the level of vulnerabilities, unless additional safeguards or a very high degree of safeguards are implemented.

Does that answer your question?

MR. TRENKLE: Let me just follow up a little further with you on that. I am just going to use an analogy with the non-health care world. Obviously there is

a lot of fraud that is going on in the banking industry and other financial industries, and much of this gets prosecuted. A lot of it obviously slips through the cracks.

How do they deal with some of the issues that we were just discussing here with not just detecting fraud, but also prosecuting, dealing with the same issues of authentication, non-repudiation, other areas to establish this chain of evidence.

MR. NICHOLSON: Most of the cases that I have been involved in, well, actually all of the banking or financial service electronic fraud cases, there have been human witnesses that identified the individuals involved. Either you are able to catch the person picking up the money or pulling the money out of the bank or doing a search warrant or a wiretap, or something that allows us to go to the person, physically catch them in possession of some implement or the proceeds or actively engaging in the activity.

Because of that level of anonymity involved with just the electronic transmission, and not even be able to know in the current environment where that transmission came from and having no idea who sent it, absent that other piece of evidence, we are really at a loss. I think that is why there is so much identity theft that goes undetected

-- perhaps not undetected, but unprosecuted, because we just don't know who is doing it.

MR. CAVERLY: DEA, additional questions?

MR. BARBER: Robert, I'll come back to you again, and our state folks as well if you have any thoughts on this. One of the issues that we explored earlier today was the issue of recordkeeping.

Those of you who are not plugged in directly with the DEA diversion control issues on the panel, our current statute provides that records of prescriptions are maintained by the pharmacies and are not required to be maintained by the prescribing physician. We have talked about audit trails for evidentiary purposes.

My question to you is, with the landscape as it is currently, where the doctor or the practitioner does not have to maintain the prescription record under the law, and that the vendors in between are not under the jurisdiction of DEA for recordkeeping purposes, how would that affect you as a federal prosecutor, if all you had was the ultimate prescription that the pharmacy had, as far as proving the things you were talking about, authentication from a legal perspective, not the technical authentication and admissibility?

MR. NICHOLSON: I'm sorry, the question was from a legal perspective?

MR. BARBER: Right.

MR. NICHOLSON: Well, it is going to increase the number of witnesses that I am going to have to bring into court to authenticate any particular record at issue, and it is going to inject a level of complexity and uncertainty in authenticating the record.

In the current paper-based system, I subpoena the pharmacy records, or we obtain them by way of search warrant or administrative warrant, so I have a live body witness that is bringing in and can authenticate that hard paper record.

In a purely electronic world, I think we are going to have to bring in additional folks. We are going to have to bring in the pharmacies to say what you received, we are going to have to bring in the intermediate vendor or vendors to certify that there was no potential for alteration as the document was going downstream, and that no alteration occurred, and then have them point back to where the electronic document was originally transmitted from.

Then it may very well, depending upon the system being used, and I don't know the technical details here in terms of what is ultimately going to be done obviously, but we may actually then have to go back to the point of origin and do a forensic analysis of that computer, look for any

records of transmission.

Putting it in a different context, in electronic filling to Medicare, one of the things that we will do is, I will subpoena the phone records to show that in the world of dial-up modem, which we don't have as much anymore, we would show that they dialed up that number on the date and time in question.

Now, with broadband and such, that is not as prevalent, but then you go to the Internet service provider, we look for those records to show each step of the way that it went from point A to point B. So the more points there are along the way, the more complicated it gets.

SGT. MC ELHANEY: I just want to add a note to that. You made a statement that the physician is not required to keep a copy of that record, but they are required to document it in the patient file.

In our investigations, evidentiary information is as much what you have as what you don't have. So if something is not documented, that could be as pertinent to the case as the fact of the actual evidentiary information that you have there.

MR. WINSLEY: It seems to me that Lisa Robin said in an earlier panel, and I thought it was true, those records are required by every state, because the doctor has

to keep records of his or her treatment of the patient. So the records are available. It is not a federal requirement, but as far as I know, and I thought Lisa said that earlier, it is a requirement in every state. So the records are there, or are supposed to be there. As Lisa said, that is sometimes evidence when they are not.

MR. NICHOLSON: And I concur on that. That is pretty standard in my investigations. I will obtain the patient files by one means or another, most principally search warrant or in appropriate cases, subpoena, to look for the existence or the absence of the records. So that is clearly an issue.

Although, similar to something that happened in one of Bill's cases, they had a mysterious flooding accident in one doctor's office that we subpoenaed for the records as well.

MR. TRENKLE: Bill, I'm going to pick on you again a minute. The issue of passwords that you have discussed at some length, the shortcomings of them, and some of the anecdotes, most of them are funny, but there is obviously a serious side to them as well.

But something it points out to me is, it is not the password in and of itself, but it is the procedures surrounding the use of that password and how that password is developed, that seemed to be the issue more than the

actual use of the password. I guess my question to you is, even if you go to a PKI solution or smart cards or other types of technologies that may at least in theory offer better protection than the plain old password, if you don't have the procedures in place to safeguard the certificate or the smart card or anything related to that, would you not run into the same risks as you would with the password? Recognizing that you can have a password with weak ID proofing or a password with strong ID proofing, the same thing could occur with PKI and also with any revocation of the certificate as well.

So is what you are arguing more an issue of procedure as well as the fact of passwords? Or are you just saying inherently that you feel that passwords in and of themselves, regardless of the strength of the procedures around them are worthless?

MR. WINSLEY: I guess the answer is, all of the above. First off, my premise is that passwords are worthless, period, bottom line. If that is all you have, it is worthless in a health care setting.

I am not going to address the banking industry where somebody is in their private office. I am not talking about me sitting in my basement office moving money from checking to savings or usually the other way around. But I am talking about a health care setting where

everything is out in the wide open. They are worthless, because there are too many people around.

It is just like your bank card. You try to get your bank card, and you go to some of these ATM machines where the keyboard is up here, you can't protect that password. You can protect that physical card, so you are safe. But if I am anywhere within ten feet of you when you enter your password in that ATM machine, I got it.

So I don't care how secure a password you have in a health care setting; they are worthless. The PKI, if you remember that homemade slide I had of the computers, the PKI kicks in at the computer.

MR. TRENKLE: Right.

MR. WINSLEY: But it is the personal identifier of the individual sitting at the computer that we are talking about. You can have PKI where the personal identifier is a password, is the way I understand it.

My final slide was, if that is what you have got, don't waste time on the PKI because it is not telling you anything. The smart card, if you are in possession of a smart card like your ATM card, I can hold you accountable for the use of that card. If you lose it and you report it, we can turn it off. If you give it to somebody else, then shame on you.

MR. TRENKLE: Right, you can give it to somebody

else in the office.

MR. WINSLEY: You can, but you are assuming liability because it is something physical that you have agreed in writing that you are accountable for. If you agree in writing that you are accountable for your password, I can't hold you to that because you may do everything you can, and that password is still out there.

Your ATM machine is the best example. If you sign with the bank that under no circumstances would you give anybody your password, I have still got it. So the difference is, when you are getting to something physical that you hold or that you wear on the end of your finger or thumb, something physical that you can hold like a card, I can hold you accountable for the use of that card. If you know that going in and you give it away, then I don't have any problem personally with holding you accountable for that. But I do have a problem with holding you accountable for the security of a password, because you can be as security conscious as you want, and they come out.

Back in 1991 and '92, I had all kinds of people telling us we were crazy. But most of the computer people now agree that passwords just by themselves don't make it. My health care examples were humorous, they were intended that way because it was the end of the day. But they are also truthful.

If it is a long secure password, we are going to write it down. The passwords that I have, I have got one for my bank, I've got a different one for the credit card because they have got different rules, different one for another credit card. At work I've got a couple. I can't remember all those passwords. I've got other things I need to do, and my mind just doesn't go that way. So I have trouble with passwords, as do a lot of people.

In a health care setting, we deal with passwords not only on writing a prescription, but we are talking about nurses who are trying to get drugs out of a machine while the patient is in convulsions. So you are excited, you are upset, and now you have got to try to remember some 20-digit password that has capitals and letters and numerals, and your patient is in there having a convulsion, and all you want to do it get out some Dilantin to go in and -- or some Valium to administer to them, you have got problems. If you have some secure system where you go in and swipe a card and enter a few digits, you are probably going to do okay, and you will get the drug. If I'm the patient, then I am happy.

So that is our concern. It is walking a tightrope. It needs to be easy enough for the health care setting, because you are dealing with human lives.

MR. TRENKLE: Right.

MR. WINSLEY: But it needs to be hard enough because you are dealing with human lives. So we just decided 15 years ago that something physical and something that you know can be easy enough, and yet still be secure.

MR. NICHOLSON: If I can add on to something that Bill said here, Bill said that he will have no problem holding someone responsible if he has got that two level, that physical biometric and the password.

For administrative purposes, licensure action and maybe other levels of administration action, that may hold true. But from a federal prosecutor's perspective and needing to prove a case beyond a reasonable doubt, the loss of the written prescription is going to inject an element of doubt in any of our criminal cases. Even with that two level system, smart card or some sort of biometric, I would say short of a fingerprint with a very, very short timeout, I am going to need additional proof that it was that individual. I am going to need some sort of -- whether that be a person saying yes, Dr. So-and-So was the one that was at the terminal, or it is a solo person in their office and it is unlikely that any other person was involved, some other circumstance or witness to tie them into that, because short of that there is going to be that little bit of doubt injected.

I think the other thing to remember here, this

isn't just about proving a criminal case. The other thing, at least from my perspective, also this double layer system is preventing unauthorized prescribing. As Bill said, I agree with what he said that a password is basically useless because everybody writes them down, and all the reasons that he said, and I won't repeat them. But I would echo that at a minimum, this double system with a biometric is the absolute minimum to add the element of provability, but also to prevent the unauthorized prescribing by third parties to begin with. I think there are salutary benefits on both fronts.

MR. TRENKLE: Would you still require witnesses even if you had that?

MR. NICHOLSON: Again, it is going to depend on the circumstance. The likelihood is that I am going to need some other piece of evidence over and above that dual system, either circumstantially, a witness, the person who got it.

Oftentimes we have to get the person receiving the drugs' cooperation to build the case against the doctor, or some other piece of evidence through statistical analysis, the quantity of drugs involved or some other eyewitness to prove that case, even with the hard copy prescription. It is just going to be that much more that is going to be needed if we move to a paperless system.

MR. TRENKLE: So it is a similar type of -- you are just saying the degree is much greater.

MR. NICHOLSON: Again, it depends, because there are cases where the paper prescription is pretty definitive because of the handwritten, because of the fingerprints on it, whatever, where you don't have to have that level. There are certainly occasions even in the paper world where we need to have the additional evidence. What I am saying is, I think there is going to be far more cases without the paper record, probably all of them where we are going to need that additional level of proof.

MR. WINSLEY: I need to go just one step further, though. You mentioned biometrics. From a legal standpoint, I agree with you 100 percent. I have told people for years that at some point I think our positive ID rule is going to say biometrics, period, wipe out all the other stuff.

But the trouble is, we are in a health care setting. We are dealing with peoples' lives. I hate to sound liberal, but I am being liberal here. The biometrics aren't there yet.

We had a hospital in Ohio that went out and spent a lot of money and put in fingerprint readers all through the hospital, and the nurses threatened to walk out, because the fingerprint readers repeatedly told them that

they weren't who their driver's license said they were.

When they work, they work great, but biometrics to my understanding, unless you spend lots and lots and lots of money, just aren't there yet. So from a health system standpoint, we have got to be darn careful about saying you have to use biometrics at this point in time.

MR. CAVERLY: We are out of time for this panel. However, I will offer one last question to DEA if we have any questions.

MR. BARBER: Bill, who writes your material for you?

MR. WINSLEY: Actually I sat in my room last night until quarter to 11 finishing this.

MR. CAVERLY: Thank you all for your time. We will take a 15-minute break. I have approximately 25 til, let's come back at ten minutes to four, and we will have a time for open microphone and comments.

(Brief recess.)

Agenda Item: Open Microphone

MR. CAVERLY: Let's begin this last portion of our last day. We are going to have open microphone now for some period of time. On my part, I think it has been very interesting to hear the different perspectives over both days, so I appreciate everyone hanging around here until the bitter end.

Why don't we start on this end of the table? I would just ask folks to be mindful that there are other commenters that would like to get on the record as well.

DR. ZUCKERMAN: I am Alan Zuckerman, representing the American Academy of Pediatrics. So much has happened the last two days, I just want to make it perfectly clear for the record that we do still believe that current electronic prescribing security practice are substantially superior to manual prescribing. We do believe that on an interim basis it would be appropriate to allow electronic prescribing to begin while additional security requirements are being investigated.

Every day that we put this off, patients suffer harm and we further delay the implementation of electronic prescribing. The only changes that might be necessary are to set some bare minimum standards for passwords so that you are not using four-digit pins without minimal password change, and requiring the vendors to do some identity proofing.

I have listened very carefully to the last two panels, and I am very heartened to hear as much reinforcement to my own personal commitment to the need for better encryption technology to support regulation and law enforcement. But at the same time, my opinion that we are simply not ready to do this immediately has not changed.

If we don't begin, we will never get there.

But also, very much as a physician, I am much more focused on prevention of the fraud, abuse and diversion that I believe can be done with electronic systems, and am willing perhaps to accept short term some compromise in the ability to prosecute after the fact.

It is also important to remember, we have said so much about PKI, but PKI is just encryption. There are three different security uses that can be thought about separately. One is authentication. That can be done with a password or even in place of a password. The second is signature. That does give us a permanent record. It can stay in the pharmacy and later be used. The third is secure messaging. Almost everyone using SSL is actually basing that on the use of PKI.

One of these new security practices might well be PKI done at the vendor. The first fact in doing that would be to have DEA test substance of these networks and clearinghouses as well as EHR vendors and potentially put the smart cards at the level of the systems, and we would at least know where prescriptions had come from.

The issue of translation on the network which is essential is not really a barrier. If the networks were registered, then they could re-sign the translated prescription, keep both the original and the translation on

file, and the pharmacies would need to make no changes in their system. They would simply have prescriptions signed by the original EHR prescribing system and some signed by the network. But they would all have the same permanent proof of non-repudiation and message integrity.

Pilot studies are going to be absolutely essential. I think there is very little need to continue talking about biometrics, because this is even less ready than other technologies. NIST in their levels of security, the highest level, level four, acknowledges only the hard tokens, the smart cards that are self contained. Biometrics which I have worked with for many years have too great a failure rate and really aren't going to add anything to what we can accomplish with smart cards, either for authentication, signature or even just for secure transmission.

Again, we need these pilots because of small examples of 50 physicians in a VA hospital. They are some highly motivated people. A pharma company simply don't support the needs of a practice.

The final important thing we need to wait for is the development of the National Health Information Network. That may be our key to getting the two-factor authentication and signature. One of the things that came out today in terms of modifying retail pharmacy systems is

that if we build into the network the validation of the signatures and the validation of the right to prescribe, we don't have to go about modifying every retail pharmacy system. One nationwide network could enforce and validate signatures and anything received from that network could be considered to be validly signed. It waits in the logs of the pharmacy, and if needed for future prosecutions or evidence, the signature could be revalidated at that time without spending tens or hundreds of millions on rebuilding our pharmacy information systems.

Thank you very much.

MR. CAVERLY: Thank you.

PARTICIPANT: I am with the Department of Veterans Affairs. Just a minor correction. It is only 40 physicians, not 50. However, since 1998 VA has had an electronic health record, and we have used electronic prescribing throughout the federal government. We currently have 95 percent of all our prescriptions being electronically entered. That is over 100 million prescriptions a year. This includes schedules three through five.

In the time that we have had those electronic prescription systems in place, where we have gone to look for waste, fraud or abuse or potential diversion, it has occurred only with paper records.

Now, we have been a pilot for four years, and have been fairly successful for that limited number, as you mentioned. However, I have got 30,000 part time and fulltime physicians who are ready to switch over at such time as DEA promulgates the final regulations.

What I think everybody is asking for is a security framework. Whatever the framework is, whether it includes PKI or not, we can identify who is going to be the prescriber, that they have a secure method of transporting the prescriptions to the pharmacy and be assured of non-repudiation, and have security throughout the system for both law enforcement and for medical care.

I think we have had enough time that if you at least tell us the direction of the security framework, then the different vendors and government agencies that have been using electronic prescribing can move forward.

MS. THOMAS: Michelle Thomas from the Virginia Department of Mental Health. I am also representing NASTDS.

I just wanted to say to the panel on both sides, DEA as well as HHS, that what I have heard mostly today and in the last few days is how prescription claims and transactions are monitored for these type of programs, to monitor the medical history and things that are available to prescribers. But the population that I deal with and

other departments of mental health, that is the population that wanted to make sure that everyone keeps in mind, the state governments are at the table in helping to move forward with this thing.

I do agree with this whole program, but I am on the fence because I know the structure and the infrastructure in state and county and local governments and within the pharmacies are not there. We are still reeling from Medicare D. I know that for the most part, the majority of all the state departments of mental health, and IMDs are not billing Medicare D because we simply don't have the systems in place. I find it difficult to understand how we could participate in this type of a program without those infrastructures in place.

I just wanted to put in a plea that we don't forget state and local governments.

MR. GRAY: Steve Gray, Kaiser Permanente. Just a little bit of background so you understand my perspective. Kaiser Permanente has nine million members nationwide. As mentioned yesterday, we do operate our own hospitals, pharmacies, medical offices, laboratories. It is an integrated health care program.
In California for example we sell over 15 million prescriptions a year.

There are a couple of points that need to be made

in balance. While I certainly appreciate the difficulties of prosecution of criminal cases -- I am a pharmacist and an attorney, I am a lecturer at several schools of pharmacy, past president of the Local Pharmacists Association, I have a real good perspective about some of the problems that you are going through and have participated in some of those prosecutions myself.

However, from the practitioner's side, we can't lose fact that although your mission is to protect the public and that there is suffering that happens with addiction and overdose deaths and so forth, there is also another type of suffering that is going on. That is, the patients, where the time to get the medication is causing them in my opinion unnecessary and unwarranted delay in pain relief and sedation and in other issues where they need those drugs on a better timely basis that they are not getting now because of the requirement for written prescriptions for schedule two items.

That is a fact that is getting worse as the population ages, as we get more patients in hospice programs, as hospice programs go to non-facility type hospice programs, as we have an increasingly elderly population and a lack of geriatricians and oncologists to treat them. It is an increasing problem to get the patients in a timely way the schedule two medications that

they need. We can't lose track of that balance in preventing pain and suffering and protecting the public, because it is a very serious matter.

Secondly, I think that there are some things that the DEA can do in terms of asking for additional authority that would tighten the whole system. In some of these comments, I have to qualify that they are my own personal opinion, not necessarily those of my organization, blah, blah, blah.

For an example, there is a competing technology. Earlier today a person held up a piece of paper and said, this is what we are competing against. There is a competing technology that is evidenced by a recent law that was passed in Washington State, where they mandated that all written prescriptions have to be printed in order to avoid the problems they are having with adverse drug events, errors, et cetera, for written prescriptions.

That competing technology is voice recognition. Right now, some of the physicians are finding that I'll just pick up the phone, I'll phone it in. Pharmacies are reacting to this increased work load on their part by installing phone actuated voice recognition systems and it prints out the prescription. That is another technology that we are competing with. It is much better to have that all in a computerized system where it is trackable and it

is traceable and it is audible, than it is to have the schedules three, four or five in a phone or voice recognition type system.

So you may keep that in mind, of the way the technology is going.

There is also a problem, if you are thinking about state pre-emption, I know that has come up, there is another type of pre-emption that you might want to consider. There are state laws for example that are actually more liberal, that actually are a detriment to some of the controls. For example, there are state laws that allow patients to opt out of electronic tracking systems for controlled substances. There are state laws that require prescribers to offer a paper prescription when they could have sent an electronic prescription that would have been much more trackable.

Those laws put in place for various political purposes need to be considered as a detriment to the tracking and enforcement that you are trying to achieve. In certain cases we are trying to get those repealed, but it may be that federal pre-emption is necessary.

I also believe that there is a significant opportunity for improving the enforcement system, the quality system, by changing the DEA rule regarding the registration of medical students, residents, et cetera. As

you know, that rule was adopted a long time ago to allow these types of individuals to prescribe including controlled substances in hospital environments, when the hospital environment was the location of their residencies.

That is no longer true. Residency programs are throughout the ambulatory care environment as the nation sees the need for more family practitioners and other community based physicians. So there really is no reason anymore to presume that the hospital is keeping control.

Those systems by the way are really problematic for the state based tracking systems. The Cure system in California cannot handle any system where it is the hospital's DEA number with a suffix, as prescribed by DEA regulation. Wouldn't it be just better to require those individuals to get a DEA registration, get them into the system and let all of that be tracked just like any other prescriber? I think that would help in some ways.

There has been a lot of discussion, and I think it is valid discussion, about the responsibility and the ability of pharmacists to act as a control in making sure that prescriptions are written for a legitimate medical purpose, that corresponding liability that we keep talking about and has been a confusing enforcement matter for 30 years that I know of, because everybody asks about, what the heck does that mean.

Well, electronic health record systems and electronic prescribing systems that passed additional information about what the indication of the medication was for would go a long way to helping the pharmacist determine whether there was a legitimate medical purpose.

It doesn't have to be the diagnosis. I think that has been where the problem is. Diagnosis and indication are not synonymous terms. Indication is pain, diagnosis might be cancer. It is difficult to get a prescriber to commit to a diagnosis when they first see a patient, but they know if they are using Vicodin that they are treating pain. So you can start getting them used to getting that medical information along with, and that might be part of the issue.

Again, I would like to repeat, I believe strongly that we need to move forward. We need to move forward with the current systems and partial systems. I think a lot of the things that Ohio offered in terms of making the whole system a lot tighter, I think that consideration of special situations where states approve systems might be something you should also consider. States are looking for -- boards of pharmacy for example are looking for some reason that they can justify the expense of approving systems. The federal regulation required that that might provide the ability for them to get that kind of funding.

Thank you very much.

MS. JEANSONNE: Good afternoon. My name is Angela Jeansonne. I am with the American Osteopathic Association. I think that this has been really a great meeting, and to hear the different points of view and everything.

One of the things as I was sitting and listening to the comments made during this meeting, costs and what is going to be entailed and involved in terms of some of the admin and other requirements. I think those are questions that will be of great interest to everybody, and certainly I think that is something that is on everyone's mind.

As an example, one of the things I thought was interesting, I think it was the individual from ATP that was here, she talked about some of the smaller practices and the adoption of EHR and stuff. We have a lot of members that are in small rural practices, small businesses, so that is definitely questions and items of great interest.

I guess my other question I would have, as you go through this process, this has been a process that has been awhile in the making and that you have talked to a lot of groups in addition to today's meeting. I was just wondering if you had a time frame as to where you go forward from this.

Thank you.

MR. CAVERLY: I'm not sure we can answer that question. I'm not sure we have the ability to answer that question. Does anyone want to address that?

MS. JEANSONNE: I guess I was just wondering if you see this as a long term process, or --

MR. CAVERLY: Gosh, I hope not. We can both agree on that. I had lunch with somebody yesterday that said they had attended a meeting on this issue eight years ago. I will speak on my own behalf. I recognize, whether DEA does or not, I recognize that this is a very important issue, and we will work to expedite this as quickly as possible.

One thing I have learned, and I am a 25-year bureaucrat, I have never seen bureaucracy crawl so slowly as I have in the last five months in the section that I have been in. I understand that there are reasons for that, but I think we can agree that this is an important issue and that we will try to push it along. But there have to be decisions made. We have to take the information back from this meeting and see what we can do with it.

MS. JEANSONNE: I only ask that because I know it has been discussed over time, and I didn't see anything that indicated to me if you had a specific time frame or if it was open ended. That is why I asked.

MR. CAVERLY: No one is pushing us to have this done by next week. We are getting pressure both from within and without the agency, and I understand that. But unfortunately I can't realistically give you a timetable.

MS. JEANSONNE: Thank you.

MR. KAZZAZ: Dan Kazzaz from Rapid Data Interchange. Again, I want to thank DEA and HHS and everybody else who has been here. It has been a most enlightening if not entertaining couple of days. I hadn't imagined that I was going to be listening to the plot for the next Miami Vice movie here, although I do have a hard time picturing my mother-in-law selling drugs on the streets of Florida.

Anyway, on a serious note here, one of the things that occurred to me as people were giving testimony today is that people talked about the costs of moving over to a PKI infrastructure in health care, which is basically what we are talking about.

One of the things that was left out of the comments here is the cost of the current system. There are a lot of leased lines in place, a lot of dialup lines, and a lot of paper that are there because we cannot move data securely over the Internet. If we start moving towards secure Internet based transactions, the pharmacies for example, every pharmacy I have ever heard of has a series

of leased lines to various places, because of the way that they are networked. Similarly for Medicare and Medicaid; there is just an awful lot of leased lines out there to communicate securely to these various entities.

So as we move forward, that is just one piece of the cost savings. There are other cost savings in terms of paperwork cost savings, the amount of money we spend on postage and paper because we cannot communicate in a standard way between payors and providers. So those are big costs in today's system that would be saved if we moved to a PKI infrastructure.

Another area in terms of the fraud and abuse, level two through level five of controlled substances. One of the things that it brought to mind was credit cards and credit card abuse and what happens. I don't know if you have had the experience of having your credit card be misplaced or having your number be picked up, but the fact that you get a phone call within a day of people fraudulently using your credit card is amazing, because the systems that they have to detect fraud and abuse based on patterns is pretty neat these days. It is a little bit too neat, because if you go overseas without telling them ahead of time, they call you, which is a little hard when you are overseas.

But it is a very serious concern in terms of

being able to detect what happens with prescription drugs. The copying of the prescriptions electronically to a centralized point or 50 centralized points or whatever it is going to be could certainly help in detection of fraud and abuse much faster than they are doing today.

So I just wanted to bring up a couple of the benefits of moving towards electronic systems that hadn't been talked about.

MR. DONFRIED: Paul Donfried, SAFE and Strategic Identity Group. I wanted to clarify a couple of points that were discussed that I think may have been a little obfuscated in the discussion.

One was a reference to comments I made during the first panel. The reference was that a digital signature is not the only way to be secure. I completely agree. The comments I made in the first panel were that through the risk analysis that we did, and then comparing symmetric cryptography systems to asymmetric cryptography systems, our conclusion was that a digital signature and asymmetric cryptography were the only known techniques to achieve a high level of non-repudiation.

Clearly there are other elements to security beyond non-repudiation -- integrity, privacy, et cetera, and symmetric key or other mechanisms are perfectly adequate for that.

So just to be very clear there, the comment I made in the first panel was that through our conclusion, digital signatures and asymmetric cryptography were the only known technique to deliver a high degree of non-repudiation, and specifically to use that to support legally enforceable evidence.

The second thing I wanted to clarify was this language that we have been using around passwords and secure IDs, biometrics, all of which mathematically and technically fall into the category of symmetric key systems.

What I mean by symmetric key is, I have knowledge of it, and the counter party, the password authenticating me has knowledge of it. In the case of a password, it is something I know, and that is somehow stored in the system. In the case of a secure ID, it is a revolving one-time password that is on the device I have, and it is also known to the system that is authenticating me. In the case of a biometric, precisely the same. Something scans my finger, recognizes my retina, recognizes my face. The system authenticating me has an image of that.

As was discussed very eloquently, different forms of symmetric keys have different degrees of compromise capability. Passwords, very easy for other end users to compromise. They can look over your shoulder, they can

grab the posting note you wrote it down on, et cetera. Secure ID a little bit harder, because you have to have access to that device. But many times from the hotel I have called my wife and had her read me the little revolving number so I could get into a system.

Biometrics are a bit harder. In the movies, people pull out eyeballs, chop off fingers, so there certainly are ways for end users to compromise them, but it is a little bit more difficult than a password.

What was not discussed at all was from an enforcement perspective, a much more realistic attack on symmetric key systems, which is an insider attack. Someone who administers the backend system masquerading as me using the image or the symmetric part of the key, the copy they have, to do that.

Someone else made the comment today that they weren't aware of any precedent or case law about symmetric key systems being challenged. DOJ v. Microsoft is perhaps the most notable one, where there were e-mails that Joel Klein U.S. tried to introduce as evidence that were not admitted. They were solely not admitted because of the weakness of a symmetric key system.

The next thing I wanted to mention was, PKI. We should come up with another word, because clearly that has a lot of baggage it drags with it. PKI is pervasive and

prevalent in society. Every DVD player uses PKI. Set-top boxes use PKI with smart cards. Ipods use PKI. European Union and Japan have deployed many consumer system using PKI and smart cards. We perhaps have been particularly dysfunctional at being able to apply it in the U.S. in health care, but there clearly is precedent for being able to do that.

The next thing, and I'll be brief here, the point that I seem to see over the last two days, this should not be a technology debate or any religious type of debate. Ultimately the patient is waiting for us to improve the system. I think what we have heard today is, improving the system towards the goal of efficiency is not enough. We need to insure that as we improve the system, we make it more resilient and we improve our ability to not only prevent and detect fraud, but to enforce it.

The point was made yesterday that enforcement is a way of modifying behavior. To the extent that we can create a community where people know someone is watching and know that there is a recourse for inappropriate behavior, that system will become self correcting.

The last thing I wanted to mention, this was great over the last two days. I hope that it is a beginning of a dialogue where at the center of that dialogue is the issue of evidence and legal enforceability.

What are the artifacts that we are left with after a transaction happens, because ultimately that is what the basis of the veracity of the resilience of the system relies on.

Thank you.

MS. RYAN: Hi, I am Mary Ryan from Metco Health Solutions. Metco is a PBM. I just wanted to make a comment about testimony earlier in the day. PBMs have never routed electronic prescriptions to pharmacies that the patient did not choose, nor have we ever altered a prescription record with regard to the name of the drug, the product or quantity.

In the early days of electronic prescriptions -- and I would point out that the scrip standard was passed in 1997 -- in the early days of electronic prescribing, pharmacies expressed these concerns and fears, and as a result of those fears, totally without substance, many state laws were promulgated that essentially put a stop to e-prescribing, because they were so onerous. Otherwise, we would have been having this conference at least five years ago, if not before. So I think we need to stop expressing these fears and move forward.

Subsequent to the testimony that happened today, most of the subsequent testimony rather, was related to substance abuse. But I would point out that substance

abuse is increasing under a paper-based system. So maybe there is something we can do in the electronic system to prevent the substance abuse.

All the subsequent testimony was not about preventing it, but rather about prosecuting it. So if prosecuting is really the key here, then why don't we talk to the system vendors about what kind of evidence can be produced from those systems to aid in prosecution?

Thank you.

DR. MARTIN: Good afternoon. My name is Ross Martin. I am the Director of Pfizer Health Care Informatics. A couple of very brief comments.

First, I don't think I mentioned yesterday that I am also on the executive committee of a organization called Manbiquitous. I think it would be worth you taking a look at MEDBEC and any DBIQ.org and having a conversation with them. They create standards centrally about medical education standards and medical objects, but the other major part of their work is around physician credentialing, licensure and the sharing of those things. Also, how do state medical boards and specialty societies exchange information about credentials. It could be something that would be useful in how especially the DEA enforces the status of someone's license and their privileges based upon their board certification, et cetera. So it is something

worth looking at. They could not be here today to provide that testimony, so I thought I would offer that.

Another role that I play is in the consumer empowerment work group of the American Health Information Community. One thing to think about, as we try to look at how this fits into the big picture, I think everyone has established in this conversation that some unified solution is what we are looking for and need.

Again reiterating some of the comments from yesterday, the DOJ and the DEA could provide a very central role in that, along with the HHS support for that, of getting medications systems for providers within the health care system.

It may be worth exploring the notion of creating a breakthrough in the subsequent rounds around this issue, because it is one that comes up with ever-increasing frequency, and is a fundamental building block around so many things beyond just this particular issue about controlled substances. I would hope that the DOJ and DEA could play a substantial role in that, along with Health and Human Services.

Thank you.

MS. HELM: My name is Jill Helm. I am with AllScripts Health Solutions. We are a leading provider of electronic health records. We have a unique distinction in

this audience of providing stand alone electronic prescribing systems as well as the higher end or Cadillac complete electronic health records.

We have approximately 30,000 physicians. We also have an FDA licensed repackaging facility and we are regulated by the DEA, so we have had the opportunity to experience some of those DEA inspections firsthand.

But that being said, what I wanted to do is share with you some of our perspectives. First of all, a call to action. In recognition that the standards that are developed here for electronic signature will be applied not only to all prescriptions, but also to all records that are signed within an electronic health care system.

We are very physician centric. From a physician's perspective, a physician's signature is a physician's signature. So he wants to sign a prescription in the same manner in which he signs a progress note in order for a laboratory test, an X-ray or a procedure. So I think it is important for us to at least look on the horizon and begin with the end in mind.

Secondly, I do want to share with you some of the providers' experience in Ohio. Bill Winsley and the Ohio Board of Pharmacy have been fabulous in establishing regulations, but also, we have customers in Ohio that have implemented the entire electronic health record, with the

exception of unfortunately electronic prescribing. That is because in very large groups, the ability to create a paper based record, have it signed and have it archived is such an administrative burden, at the end of the day they have decided simply not to do it.

At AllScripts we have a motto that says, if physicians don't use it, nothing else matters. So I couldn't agree more that this is not a technology issue, but really should be an issue of physician adoption, and that we need to seriously consider the risks versus the benefits in the burdens that we are placing on the health care system.

We have enabled biometrics in our electronic prescribing application. We have no one that is using it, simply because of the costs involved with the technology, and also the time involved with scanning your thumbprint on a biometric reader. The physicians found that it slowed them down too much, that they couldn't see as many patients per day, so they abandoned that technology.

So I would just encourage you to keep the dialogue open. In any regulations that are developed, I would encourage you to work collaboratively. It was a process that I was first getting in with NCVHS, and it worked beautifully, and would welcome participation, would also offer up any of our physicians, if you would like to

get a practical perspective from an end physician user.

Thank you.

MS. FOURQUET: Lori Reed-Fourquet. Today I will be addressing you as a subcontractor on the ONC initiatives for security and privacy, where we are looking at barriers to enabling health information technology.

It seems based on the discussions today there are a significant number of legal issues surrounding drug control and prosecution and tracking, and all of those things that may have been appropriate, but may have been appropriate when they were established many years ago, that may need a broader view and overhaul to help enable health information technology while still getting you the forensic evidence and whatnot that you need.

I would encourage you to -- as a number of other non-HHS agencies have done, to participate within the standards technology panel. We have contributions from DoD, from NIST, from GSA. They are all actively participating in a public-private sector cooperative initiative addressing the needs to enable health information technology.

We are working on identifying standards, and within the next week we will be addressing something such as managing user credentials, very related efforts, and we would welcome that type of participation. CCHIT, where

they are trying to identify what sort of certifications would be required to help support that. This is all related work, and I think it would benefit to have the participation in all of those levels.

Thank you.

MR. SCHUETH: I am Tony Schueth. I spoke yesterday, but just for the record, I will restate my credentials. I am managing partner and CEO of a small consulting firm called Point of Care Partners. We work with any stakeholder in electronic prescribing that you can think of. I have personally been in this business for 11 years, so this is the baseline of where I am coming from.

What I want to do is make a couple of points. The first point I would like to make is, I guess I would agree with Bill Winsley in one of his comments today when he said that the folks that have testified to you are the cream of the crop, both of the front end software systems as well as the intermediaries.

I would suggest that one of the things that might benefit the panel would be to look at what they do and also what the other organizations that weren't here today, and look at best practices. I have never done a security audit of any of these companies, but my impression is that it is not uniform, that some of the security procedures that were described today aren't uniform across all of these

companies.

So I think it would merit the view or an audit or a survey or whatever of best practices in some of these companies. I think that would help you guys in implementing policies and procedures that would help to reduce fraud and abuse and some of the other things that we talked about.

The second point I would like to make, and I haven't heard this today, I would like to point out that upwards of 65 percent of doctors in this country are either solo practitioners or practice in two to five physician groups.

So when Kathy was asking earlier about the cost of security measures, yesterday we talked a lot about costs, and I am glad she brought that up, but the other thing we talked about is adding complexity. I want to make a point about the importance of adding any kind of complexity to what the doctors do today is a substantial burden on these solo practitioners or two to five group physicians.

They don't have IT groups. Dr. Zuckerman showed you his smart card, but Dr. Zuckerman received that smart card from the IT department at Georgetown University. If it is lost, he can contact the IT department at Georgetown University. The small group practices don't have that kind of IT support. They don't have the sophistication to

understand how to manage that situation. It is a burden on them. It is a burden such that if the burden is substantial, they simply won't use it. They will simply continue doing the things the way they are doing them today.

That may be okay, but I need to point out the fact that most of the doctors in this country are in these smaller groups. Even yesterday when we threw up some statistics about number of doctors that are prescribing electronically or have EHRs, those are by and large in the bigger groups that have more support. We still aren't seeing an increase in adoption in the smaller groups.

So what I would like to suggest is, if there are ways that we can enhance security, enhance the ability to prosecute some of those kinds of things, without adding substantial complexity, that that is the sort of solution that I think would ring true in some of these small groups, in rural areas. You can't leave those folks out of health care. Otherwise we are not going to see the overall benefits of health care.

I think that the last point I want to make, there was some discussion about certification. I'm glad that was brought up. I guess as it pertains to physicians, I would suggest that if the requirements for electronic prescribing of scheduled medications are greater than that which are

required for EHR, or that which they are required to do today, it is just not going to -- most doctors aren't going to use it. That is just something that is a reality that I think every health care provider in this audience will tell you.

I guess my last point is this. I think Jim Chen had it up yesterday, and I just want to underscore. He had a bullet point that said the enemy of the good is the perfect. I just would like to leave you guys with that thought.

Thank you very much for your time.

MR. NICHOLSON: Hi, I am Kevin Nicholson with the National Association of Chain Drugstores. I spoke on the panel yesterday, and I just want to make a few followup points.

First of all, I want to respond to a comment made by the gentleman from Rapid Data Interchange. He spoke about lease lines and comparing the cost of lease lines to PKI, and specifically the cost of lease lines to chain pharmacies. For the record, I just want to state that chain pharmacies really don't see the lease lines as a significant cost. We certainly wouldn't want to have the cost of a lease line added into the determination of whether we should go with one type of security measure over another, because lease lines just really aren't that great

of a cost for chain pharmacies. So I just wanted to make that point clear.

Second, while I am up here, I heard the testimony from Mary Ryan from Metco. If any of you are familiar with chain pharmacies and PBMs, it is quite remarkable that I am going to agree with what Mary Ryan said. Yes, we are in agreement.

I think Mary made some good points that the current system -- we heard testimony this afternoon from investigators and prosecutors that by their own words there is an epidemic of drug abuse and diversion, and that epidemic gets worse every year under the current regime. So I think it would be logical for us to consider making changes to the system, and I think technology is probably the way to go.

So my followup to that point is, and also agreeing with what Mary said, I think we can all find a way to make the system work. I think we should try to find a way for the vendors to give DEA what DEA needs under its mandate.

That's all I have to say, so thank you.

MR. WHITTEMORE: Ken Whittemore from SureScripts. There is one notion that kind of got lost in today's discussion. Dr. Zuckerman touched on it a little bit, but the discussion about enforcement and the needs of the law

enforcement entities to be able to prosecute these cases forgot that the basic process is going to be changed. It is entirely likely that the security that is going to be brought to bear is going to prevent a lot of the occurrences of diversion and fraud and those type of things, so that there won't even be a need for diversion enforcement per se.

One of the other things related to enforcement, because of its paper based system, there are a lot of inefficiencies built into the process. I think the mention was made, I know I'll get the number wrong, but I think 28 states have prescription monitoring programs. These programs are retrospective, and I would suggest pretty severely so. That information doesn't become available to law enforcement for weeks after the fraud and the activities have taken place.

With the e-prescribing infrastructure that is being put into place, the potential is there to intercept such activities much earlier in the process. I don't think anybody really touched on that today.

I think related to that, people should consider that the electronic prescribing infrastructure could be used as a tool of enforcement. Ms. McElhaney said that she often has to go to pharmacies and subpoena records for certain time periods, and she is asking pharmacists to go

through their files and pull all the threes and fives for two or three weeks' time.

That type of thing with an electronic environment can be done very quickly. She could go to somebody involved like SureScripts or RxHub or one of the others and say, I want to see all prescriptions for three through fives for Broward County for this time period, and it is something that can be done very quickly and efficiently, and you wouldn't have the issue of the pharmacist going through it, and perhaps errors of omission or intentionally not putting prescriptions in the record.

So again, I think there are a number of issues with regard to law enforcement that can be benefited by e-prescribing that really didn't get touched on today. That is all I have. Thanks.

MR. KAZZAZ: Dan Kazzaz again from Rapid Data. I'd also like to give you a couple of other credentials. I am the IT department for my wife's three or four person practice, and I am also the chair of X12.

A couple of points. One is that from a small physician practice perspective, getting reasonably priced software from different vendors that interface to each other is a very difficult thing to do. In fact, getting software to interface in the health care environment is a very tricky thing, which brings me back to being the chair

of X12.

What we are trying to do in the standards community, and we certainly need the help of DEA and CMS and the folks, is to push harder and harder on making all the SDOs, of which X12 is one, work towards and plug and play environment. So it is not just standards, it is plug and play. As we work towards that environment, then the cost for the providers will go down significantly for all the things that you guys want to do.

So I am back to Mr. Brooks' point yesterday, which is working collaboratively and working with SDO is a good way to try and get to the point that you guys want to get it.

MR. DONFRIED: Paul Donfried. One thing I forgot to say. I thought it was very illuminating, some of the examples that law enforcement gave, some of the deviant behavior. It was mentioned a couple of times today that for the most part in the health care community, the vast majority of physicians and licensed practitioners are good people. There are however an element of bad people.

I think in general in these sort of meetings and dialogues, you have a propensity to attract the good people. I also think that in general, we tend to be extremely naive to how bad and how smart and how deviant the bad people are. I think it would help keep things into

perspective as you are trying to make these very difficult decisions to illuminate some specific and dramatic examples of how malicious people try and attack and exploit these systems.

I would also suggest, seeing this be effective in other communities, you may even consider engaging and getting testimony from some of the more well-known criminals who have perpetrated these crimes, and let them talk from the other side of the fence, how easy it can be to attack some of these electronic systems. That has helped in homeland security and a number of forums to hear from people who perpetrate these crimes how it is they exploit people.

A very simple example. The easiest way to exploit password systems is to find the system adman, who typically makes about $35,000, and bribe them. It generally is not the cryptography or the firewalls or the audit logs or the data centers that people attack. It is whatever the weak link in the chain is, which normally is the human beings who are responsible for keeping the stuff running and operating correctly.

I'll end with that. But I thought illuminating some of those adverse use cases was very helpful today, and I think in general, many of us hopefully because we are good people are somewhat naive to the fact that there are

grandmothers selling drugs, and the fact that there are teenagers engaging in organized crime.

Thank you.

Agenda Item: Closing Remarks

MR. CAVERLY: Thank you. There is a portion at the end for closing remarks in our agenda. I will offer an opportunity to Tony if he has any comments. Frankly, on DEA's behalf we are just going to let the record stand as it is. We recognize the forum; this is an opportunity for us to listen to you. On our behalf, I appreciate your attendance and your attention to this. This has been a very valuable process for me personally, I think for all of us. I certainly learned something new, a thing or two, over the past couple of days, and I hope that you have as well.

But with that, Tony, if you have any comments that you would like to make?

MR. TRENKLE: Thank you, Mark. I would like to echo your remarks that you made, and to thank everybody for the testimony and for the informative discussion we have had. I think it is up to us now to work with the DEA and take the information we have got today from the NCVHS here and from some other venues, and work together to move ahead in this area.

I think as you heard from much of the testimony,

there is certainly good discussions on both sides, both from the law enforcement perspective, and also from the proponents who want to push ahead with e-prescribing. We need to work together to develop solutions, develop strategies that not only benefit the electronic prescribing area, but also insure that we meet the requirements of the law enforcement community, because ultimately we all benefit from moving ahead this way.

MR. CAVERLY: Thank you all.

(Whereupon, the meeting was adjourned at 4:50 p.m.)