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

ELECTRONIC PRESCRIPTIONS

FOR CONTROLLED SUBSTANCES (EPCS)

July 11, 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

PROCEEDINGS [8:30 a.m.]

Agenda Item: Welcome

MR. CAVERLY: Good morning and thank you for your patience. This place is not the easiest location to find. So, for those of you who successfully found us, congratulations. You have passed the test.

But, anyway, good morning and welcome. Let me be the first to extend my welcome. My name is Mark Caverly. I am the chief of the Liaison and Policy Section for the Drug Enforcement Administration. And on behalf of DEA and the Department of Health and Human Services, I welcome you to this two-day public meeting on electronic prescribing or electronic prescriptions for controlled substances.

We have six panels set up for you during the next two days to address this issue from various perspectives; pharmacy, medicine, technology, vendors, the states, and law enforcement. We look forward to the information that is presented during these two days of meetings.

Just so you will know the structure, we have set up the six panels, obviously. The panelists will be in the center. We will have VA folks and HHS folks. Each panelist will have approximately 15 minutes to make a presentation and then at the end of the presentations, be questioned by individuals from DEA and HHS.

There will be opportunity at the end of each day for public comment. We will have open microphones, roughly an hour or a little bit more at the end of each day. These proceedings will be taped. There will be a transcription made of these proceedings and our intention is to post the transcript on DEA's web site once it is complete.

I would ask certainly the panelists and any of the audience members so that we can hear you and we also can get a record of what is said here to please use the microphones and to identify yourselves so that we know who has asked the question and there is no issue as far as the response later on.

So, once again, I want to thank you. I am not going to take anymore of your time. We have a busy two days. We have a lot of ground to cover, but it is my pleasure to introduce to you Mr. Joseph Rannazzisi, who is the deputy assistant administrator for the Drug Enforcement Administration.

Mr. Rannazzisi.

Agenda Item: Welcome

MR. RANNAZZISI: Good morning. I have 15 minutes allotted and I am only going to take a couple of minutes of your time because, obviously, we have much work to do in the next two days.

On behalf of the Drug Enforcement Administration and Administrator Karen P. Tandy, it is my pleasure to be here today to welcome to this public meeting to address the important issue of electronic prescriptions for controlled substances or as we call it, EPCS.

Once DEA implements regulations, EPCS will grant physicians the authority to electronically create and sign controlled substance prescriptions. These prescriptions would be sent to the dispensing pharmacies for delivery to the ultimate user. Pharmacies would then retain those records of controlled substance prescriptions electronically.

In 1970, Congress enacted the Controlled Substances Act, giving DEA the responsibility to prevent, detect and investigate the diversion of these controlled substances. In the past few years, prescription drug diversion has received a great deal of attention. Most recently, the 2006 National Survey on Drug Use and Health estimated that 31.8 million Americans have used pain relievers, non-medically, in their lifetimes.

In 2004, the danger posed by pharmaceutical controlled substance abuse was recognized as a nationwide priority with the publication of the National Synthetic Drugs Action Plan. As we explore the issues concerning electronic prescriptions for controlled substances in the next two days through the use of various panels and public comments, it is my hope that we will lay the framework to implement a system consistent with the goal of preventing diversion of controlled substances while ensuring legitimate patient access.

Thank you for your attendance and your participation at this very important hearing. Thank you.

[Applause.]

MR. CAVERLY: Now we have some opening comments from Kelly Cronin, with the Department of Health and Human Services. Ms. Cronin is director of the Office of Programs and Coordination, the Office of the National Coordinator for Health Information Technology.

Kelly Cronin.

Agenda Item: Opening Remarks -- Department of Health and Human Services

MS. CRONIN: Good morning. Welcome to everyone. On behalf of the DHHS, I am glad that there is a good turnout today to talk about, I think, an important issue that is facing many of us working on the health IT agenda, trying to figure out practical and needed solutions, in particular, with regard to e-authentication that will work not only for important areas, such as controlled substances, but also for a variety of health care functions and really public health functions, as well, as we start to consider the various ways that e-authentication needs to enable secure health information exchange.

So, I guess I should almost apologize for starting off with the power point today, given that the initial comments were so brief and I will also try to keep my comments brief, but I just wanted to take the opportunity to set some context.

I think as many of you know, the executive order that was established back in April of 2004 established the position of the National Coordinator in addition to the office within the Department of Health and Human Services and the executive order called for a variety of deliverables and gave a variety of responsibilities to the National Coordinator a couple that were related to policy and policy development. It specifically said in fulfilling its responsibilities the work of the National Coordinator shall do a variety of things, including improve the coordination of care and information among hospitals, laboratories, physician offices and ambulatory care providers through effective infrastructure for the secure and authorized exchange of health care information.

Then as well, to ensure that patient's individually identifiable health information is secure and protected. I think both of those apply to the conversations and the deliberations over the next day here, to just keep in mind that we are not just talking about health information exchange or exchange of prescriptions for one particular use or need or subset of prescriptions that ultimately we need to be enabling security and privacy policies that will allow for health information exchange across settings of care. So, whether it is skilled nursing facilities, inpatient, outpatient, whatever the setting of care, we need to be thinking broadly about the whole framework that we are creating with our policies and technologies as they are developed and deployed.

Since 2004 and the President's call for having most Americans getting access to electronic health records by 2014, the Office of the National Coordinator has launched a variety of initiatives. I have only highlighted a few here, just to point out that we have many ongoing funded projects and public processes to try to address this concept of and the issues around e-authentication from a variety of perspectives. The American Health Information Community is a federal advisory committee that is chaired by Secretary Mike Leavitt.

He has convened since last October a variety of health care leaders, both from the public and private sector, in addition to leaders from public health, from the state and federal level. So, they are considering a variety of issues that are facing us, including many of the outputs of the contracts that are listed up here regarding the nationwide health information network prototypes, the Health

IT Standards Panel that is doing standards harmonization now across the public and private sector.

In addition to the output of the Certification Commission for Health Information Technology, they are also playing a role in priority setting and trying to establish some early wins, if you will, to try to communicate what might deliver the most value to consumers in the shorter term, meaning in the next one to three years. So, they have identified four what they have called breakthroughs, which have translated to use cases, which are guiding a lot of our contract work to date.

E-prescribing was talked about quite a bit early on in the community deliberations. However, it was decided that there was already a fair amount accomplished through the CMS regulations, through some pilot projects that are being funded through AHRQ and CMS and a variety of other activities across the federal and private sector space.

So, what did get prioritized was a variety of other use cases, including enabling the monitoring of care remotely and with a specific focus on secure messaging between clinicians and patients, biosurveillance to mobilize data from clinical care into public health at all levels of public health, as well as patient centric lab data exchange that is now currently a barrier to EHR adoption.

Finally, mobilizing medication history and the registration summary for patients to have easy access to that. So, there is a variety of use cases that are under consideration for next year. We have not yet had a fully public discussion around those, but the point is that there is many different use cases or situations where e-authentication is going to have to enable the appropriate and secure health information exchange.

Just to touch briefly on the Health IT Standards Panel, this is a contract that was awarded to ANSI several months ago at this point. They are well on their way to developing a harmonization process. They are expected to have deliverables on this first set of use cases that I just mentioned in September.

They are addressing e-authentication through this process and the standards that are necessary for that. I should point out that this is an effort that involves all the standards development organizations. Many of you in the room are probably involved with this effort or at least very aware of it. So, I won't say too much about it, but I think it is important to keep in mind that this really is the harmonization effort or the organization that will be considering a lot of the not only named standards that are necessary for use cases that are prioritized, but also the implementation guidance, so that when they complete their work, there should everything that is necessary to fully adopt standards.

The certification process is being developed and the criteria is also being developed right now by the Certification Commission for Health IT. This is an organization that was created close to two years ago, has received federal support through HHS, through a contract in this past year and they have already finalized their first round certification criteria for ambulatory electronic health records and they expect over the next week or so to have the first round of ambulatory EHRs on the market that are certified. There are privacy and security requirements that have to be met for this process to be certified. There are also requirements for functionality and interoperability.

We also have recently formed a Health Information Security and Privacy Collaborative through a contract to RTI. RTI has recently subcontracted with 34 states and they will be looking at the variations in privacy and security practices and laws across those states. Within a given state, they are going to be doing their own analysis and then having a public discussion across states in this collaborative as they identify solutions to any barriers that they identify.

So, again, this is another process where issues such as e-authentication are going to be looked at, not only from a policy perspective, but a practice level. What is currently happening? What is compliant with federal law? What actually goes beyond what federal law requires and how do we create a landscape where we can develop policies and business processes that will allow for health information exchange based on all this work?

You also are probably familiar with the Nationwide Health Information Prototypes. There are currently four consortia that are working on prototypes. They all have their own processes in place. While there is consistency around each contract in terms of the deliverables and what is expected of them to develop an architecture and to participate in public meetings, such as the one we had about a week and a half ago to discuss functional requirements, they are all developing their unique approaches in terms of the architecture.

So, we plan to in the next five months accomplish quite a bit. We will have recommendations on the data, the technical standards and privacy and security requirements before September. There will be an operational plan due over the summer. We will have a complete technical design and architecture for these prototypes due later this year and they are also scheduled to show some level of demonstrated health information exchange, not only within the four or the three markets that each contractor is working in, but also across the total of 12.

They should be able to exchange data from, for example, North Carolina to New York or New York to Cincinnati or Mendocino. We also expect in 2007 to have a much more expanded effort through additional funding and have a production quality version be more fully deployed.

Then we expect by 2008 to know enough about the common architecture and the requirements to then make it part of the certification process similar to what has been started for ambulatory electronic health records and will continue this year for inpatient electronic health records and then will go on to certification of the NHIN, which should include specifications regarding e-authentication.

So, just to tie this altogether, we have a lot of different contracts that are in place and many of the ones I just mentioned are really more geared towards standards and the technology aspect of what we have to do. We are hoping that collectively, they all lead to industry transformation over the next several years through, you know, trying to really not only name the standards, have the implementation guidance ready to go, but also have the certification process that is going to require the formal adoption of those standards in addition to coming up with a common architecture for the NHIN.

But in the short term, through the American Health

Information Community and the key health care stakeholders, we are trying to identify what are the top priorities, how do we need to demonstrate progress in the short term so we can show the consumers this is meaningful to them, that there is a reason for them to be paying attention and to be engaged and that they do stand to benefit from this. So, again, that is what has resulted to date in the four use cases or what the community calls breakthroughs, which we hope in the next few years will really demonstrate some value to the public.

We have a variety of coordination mechanisms. We have a federal health IT policy, which considers a lot of issues that are going through the policy development process. We have the Federal Health Architecture Program that is now much more tracking with this national health IT agenda. So, for example, the health IT standards panel and the work of the NHIN will feed into what is going to happen at an agency level so that ideally we are going to have a system that federal agencies can participate in and get the day-to-day need over time from what is created in the private sector.

So, I just wanted to close with a few comments. I think that it is obvious we are taking a holistic view. Not only has the executive order set forth a very broad charge, a very ambitious charge for not just the Department of

Health and Human Services, but really across the Executive Branch to try to coordinate with the private sector to create both the policy and technical framework needed for health information exchange across settings of care so that we can truly have an interoperable health care system over the next several years.

We think it is important that controlled substances are considered as a part of this framework. There are some special needs that need to be taken into account, but we don't want to be creating too many special circumstances that may be overly burdensome to clinicians or may not be feasible to implement on a broad scale. So, we need to be very mindful of what we need to do to ensure security to take into account the law enforcement concerns. Yet, we need to make sure that we have workable practical solutions given the President's goal that he set forth for all of us.

So, I would urge all of you to participate over the next day and really voice your opinions and concerns and make sure that we have an open dialogue about this issue. It has been quite some time that we have been talking about, you know, trying to get this meeting off the ground. I think it is a really good opportunity to really get into the issues and identify what the real workable solutions are, given everyone's perspective.

So, thanks for being here today. We look forward to taking whatever comes out of this meeting into consideration as we get further into our policy development on the HHS side.

So, thank you.

[Applause.]

MR. CAVERLY: Now we will hear a few remarks from Michelle Ferritto. Ms. Ferritto is the acting chief of the Regulatory Drafting Unit for the Drug Enforcement Administration.

Ms. Ferritto.

Agenda Item: Opening Remarks -- Drug Enforcement Administration

MS. FERRITTO: Good morning. I also would like to take the opportunity to welcome all of you today to this meeting. We look forward to having discussions for the next two days to hear input and to listen to the questions that are going to be asked regarding electronic prescriptions for controlled substances.

Electronic prescriptions are the focus of this meeting and specifically electronic prescriptions for controlled substances. So, for the next two days, we look forward to the specific dialogue on this topic.

As many of you already know, prescription drug abuse is a significant issue in the United States and it is a significant national priority. The National Survey on Drug Use and Health is a survey, which is conducted by the Department of Health and Human Services on an annual basis. This survey examines the use and misuse and potential abuse of all sorts of prescription medications. It specifically looks at Americans, who are over the age of 12, who are part of the civilian population and who are non-institutionalized.

The 2004 National Survey is the most current survey available today and that survey demonstrates that an estimated 6 million individuals over the age of 12 or approximately 2 1/2 percent of the American population use prescription medications non-medically in the last month. Of these, a significant number are determined to be controlled substances. For example, pain relievers were estimated by the survey to have been non-medically used by 4.4 million individuals.

Pain relievers typically fall into Schedules II and III of the Controlled Substances Act. Anti-anxiety medications were estimated by the survey to have been misused or used non-medically by approximately 1.6 million individuals in the last month. Anti-anxiety medications typically fall into Schedules III and IV of the Controlled Substances Act.

Stimulants, which typically fall into Schedule II and III of the Controlled Substances Act were estimated by the survey to have been used non-medically by approximately 1.2 million individuals over the last month and sedatives were estimated to have been used non-medically by approximately 300,000 persons over the last month. Sedatives typically fall into Schedule III and IV of the Controlled Substances Act.

So, as you can see, there is a significant abuse of controlled substances and this abuse is documented. The difference in the overall estimate of abuse presented in the first bullet and the estimates for each specific type of controlled substance can be caused because certain individuals misused more than one controlled substance in the last month. That is why you see the difference in the sum of 6 million versus each individual.

With that context, if I could have the next slide, please. Congress recognized the potential for misuse and abuse of controlled substances through its enactment of the Controlled Substances Act in 1970. The Controlled Substances Act specifically addresses controlled substances and Congress specifically differentiated controlled substances from other legend drugs, which are non-controlled substances. Those substances are handled by the Federal Food, Drug and Cosmetic Act.

The Controlled Substances Act establishes a closed system of distribution. It establishes cradle to grave type control for DEA. That means that DEA knows from the time of importation or manufacture through distribution all the way to dispensing where controlled substances are in its system. Part of this controlled substance cradle to grave type system is established through registration. The Controlled Substances Act specifically requires that every person who handles controlled substances must be registered with DEA or must be specifically exempted from the requirement of registration.

That means that every importer, manufacturer, exporter, distributor and dispenser, including prescribers of controlled substances and pharmacies and other entities, which dispense controlled substances must be specifically registered with DEA or must be specifically exempted. At the dispensing level, controlled substances must be dispensed for legitimate medical purposes. They must be dispensed upon the prescription of a practitioner, who is acting in the usual course of their professional practice.

If a prescription for controlled substances is written, it must be manually signed. This slide presents examples of controlled substances. Most of you are probably already familiar with these examples. As you probably already know, Schedule I controlled substances are typically referred to as illicit controlled substances.

These substances have a high potential for abuse. They do not have currently accepted medical use in treatment in the United States and they have a lack of accepted use in safety. Schedule II controlled substances have currently accepted medical use in treatment in the United States. However, they have significant potentials for misuse and abuse and that misuse and abuse can lead to severe physical or psychological dependence.

Because of this, the handling of controlled substances in Schedule II at the manufacturing, distribution and dispensing levels is closely regulated by DEA and by states. Schedules III, IV and V controlled substances have lesser potentials for abuse and misuse. They have currently accepted uses for medical treatment in the United States and they have lesser potential for physical and psychological dependence as compared with Schedule II controlled substances.

They are also regulated by the DEA and by states. The National Survey, as I noted previously, has demonstrated that all controlled substances, which have accepted medical use in the United States and current legitimate medical purposes have significant potential for abuse and misuse. Therefore, the control of all of these substances is important, regardless of the schedule in which they reside.

Controlled substances represent a small portion of all prescriptions being prescribed in the United States. Controlled substances represent approximately 11 percent of all of these prescriptions. This estimate is created by examining the list of the top 200 drugs prescribed both at the generic level and the brand name level, looking at the percentage of controlled substances out of all of those drugs being prescribed.

So, while controlled substances represent a comparatively lesser number of substances being prescribed, i.e., 11 percent, it is important to realize that the vast majority of persons who are eligible to prescribe are authorized to prescribe controlled substances by the state in which they practice and by the Drug Enforcement Administration.

Approximately 90 percent of all persons, including physicians, dentists. veterinarians and where authorized by their state, nurse practitioners, advanced practice nurses and even pharmacists are authorized to prescribe controlled substances. The vast majority of the prescribing by these prescribers, includes controlled substances. This is an important element to consider as we continue our discussions.

The Controlled Substances Act has specific requirements regarding controlled substances prescription.

The Act and its implementing regulations require that certain information must be contained in all prescriptions. This information includes the date that the prescription was written and the signature of the prescribing practitioner, the name and address of the prescribing practitioner, as well as their registration number. The full name and address of the patient is also included, along with the drug name, the strength, the dosage form, the quantity prescribed and the directions for use. All of these elements must be present on a prescription.

The Controlled Substances Act and its implementing regulations have certain requirements for the prescribing of controlled substances. For controlled substance prescription to be legitimate, it must be issued by a practitioner, who is authorized by the state in which they practice to prescribe controlled substances and who is specifically registered with DEA to prescribe controlled substances. The prescription must be issued for a legitimate medical purpose by that individual practitioner and that individual practitioner must be acting in the usual course of their professional practice when they authorize that prescription.

Schedule II prescriptions are required by the Controlled Substances Act and their implementing regulations to be written and manually signed. There are special limited circumstances in which a facsimile of a written, manually signed prescription for Schedule II controlled substances is permitted.

Schedule III through V controlled substances may be written or manually signed. A facsimile of that written, manually signed prescription is also permitted. Schedule III through V controlled substances may also be subscribed orally, with that prescription being transmitted orally by the practitioner, who is authorized to prescribe the controlled substance. The pharmacist must specifically receive that oral prescription and must immediately reduce that prescription to writing.

All written prescriptions regardless of the schedule for which they are prescribed must contain all of the information presented on the previous slide, including the name, address, registration number of the practitioner and the manual signature of the controlled substances prescriber. Oral prescriptions contain the same information except for the signature.

The responsibility for prescribing of controlled substances rests specifically with the practitioner, who is authorized to prescribe by the state in which they practice and who is specifically registered with DEA to conduct that prescribing. However, a corresponding responsibility rests with the pharmacist. The pharmacist must ensure that the prescription, which was written by the prescriber contains all elements mandated by the Controlled Substances Act and its implementing regulations and that that prescription is issued for a legitimate medical purpose by the practitioner. That practitioner must be acting in the usual course of their professional practice.

So, there is a responsibility incumbent both on the prescriber and on the pharmacist dispensing the prescription. A practitioner writes the prescription. The pharmacy is required to maintain the prescription and prescription records. These records must be maintained for two years. The only way that DEA can access these controlled substances prescriptions is through registrants. DEA cannot reach the non-registrants for an immediate access to a controlled substance prescription.

The Controlled Substance Act specifically requires the controlled substances prescription records must be maintained by pharmacies. Thus, even though the practitioner writes the prescription, the pharmacy is the one responsible for retaining the record. The only instance in which prescriptions for controlled substances are retained by the prescriber who wrote the prescription is if those prescriptions were written for narcotic treatment. Other than that, all prescriptions must be retained by pharmacies.

Thus, the sole record of dispensing is held by the pharmacy and it is this record, which DEA must look to in its enforcement of the Controlled Substances Act. The Controlled Substances Act is unique among laws. The Controlled Substances Act specifically stipulates acts which are permissible. If an act is not explicitly stipulated as being permitted, then it is prohibited under the Controlled Substances Act.

Violations of the Controlled Substances Act can be administrative, civil or criminal in nature. DEA must be able to meet evidentiary requirements for all of these types of violations, including criminal violations. Criminal violations have the highest standard of evidence, that of beyond a reasonable doubt.

The Controlled Substances Act specifically designates certain acts as illegal. It is unlawful for any person to knowingly or intentionally manufacture, distribute, dispense a controlled substance as authorized by the Controlled Substances Act. It is also unlawful for any person knowingly or intentionally to possess controlled substances unless those controlled substances were obtained pursuant to a valid prescription issued for a legitimate medical purpose by a practitioner, who is acting in the usual course of their professional practice.

It is unlawful for any person to obtain controlled substances by fraud, forgery, deception or subterfuge. All of these things are important to DEA as it investigates controlled substances diversion.

It is unlawful for any person knowingly or intentionally to use a DEA registration that has been fictitious, that is revoked, that is suspended, that is expired or that is issued to another person in the course of dispensing or acquiring controlled substances. Finally, it is unlawful to refuse or negligently fail to make, keep or to furnish records, which are false or fraudulent or contain material misinformation or omit information from those records. This is particularly important since it is the pharmacy that maintains the record of dispensing and that record was written by a practitioner.

Based on all of the requirements of the Controlled Substances Act and the potential for diversion of controlled substances, particularly as evidenced by the National Survey on Drug Use and Health and other similar surveys, controlled substances have a significant potential for abuse and diversion. Diversion at the prescribing level can occur in a number of different ways. Prescription pads may be stolen from practitioners. Legitimate prescriptions for controlled substances may be altered or may be copied.

These types of alterations and copying are often detectable to DEA and other law enforcement agencies. This ability for detection is critical. Legitimate prescriber information may also be altered. Again, this type of alteration needs to be detectable. Prescriptions may be forged. Prescriptions may be written for other than legitimate medical purposes or controlled substances may be stolen by persons and legitimately dispensed prescriptions maybe altered to cover that theft.

The diversion of controlled substances is a critical concern for all law enforcement agencies. Prescriptions and prescription information can be used in the investigation and prosecution of these types of cases. At the federal level, DEA looks to prescriptions and prescription records for the enforcement of the Controlled Substances Act. At state and local levels, law enforcement agencies also require this same type of information for enforcement of state and local laws and regulations regarding controlled substances.

State and local regulatory authorities also look to these controlled substances prescriptions for enforcement of their regulations and for disciplinary type actions Finally, prescriptions and prescription medications may be used by law enforcement agencies for Medicare, Medicaid and prescription fraud and other cases.

Those controlled substances prescriptions are not just a concern of DEA. They are a broad concern across many law enforcement entities. Based on these concerns, based on the requirements of the Controlled Substances Act and based on the potential for misuse and diversion not only of controlled substances themselves, but of the prescriptions, which are used to authorize their dispensing, DEA believes that there are three performance standards, which are necessary for the electronic prescription of controlled substances, keeping in mind that these electronic controlled substances are written controlled substances in the same manner as any other written controlled substance prescriptions are.

These three standards are authentication, which is the ability to positively identify a signer; nonrepudiation, which is the ability to determine that a signer cannot deny having signed a specific prescription; and record integrity, the ability to determine if a record has been altered after signature.

For DEA and for other law enforcement agencies, it is more than just authentication. It is looking tot he records and keeping in mind that those records must be retained by persons other than those who wrote the records and that those records must be maintained for a minimum of two years.

The authentication of the prescribing practitioner is required by the Controlled Substances Act in its implementing regulations. The Act and its regulations require that Schedule II controlled substances must be written and that written controlled substance prescriptions must be manually signed by the prescribing practitioner.

A pharmacy is not permitted to dispense those prescriptions unless they are written and unless they are written for a legitimate medical purpose by a practitioner, who is authorized to prescribe. A pharmacy can look to those written prescriptions for Schedule II controlled substances and the written prescriptions, which are permitted for Schedule III through V controlled substances to determine whether there have been alterations.

They can examine the signature. They can examine the other elements of the prescription, including the DEA number, the address, the name of the practitioner and other elements, both on that individual prescription and they can either compare it to other prescriptions that they may have in their possession. By conducting these comparisons, a pharmacy may be able to determine whether there is concern about a particular prescription. If a pharmacy has concerns, a pharmacy can take certain steps to verify the elements of the prescription by contacting the prescriber.

This same ability must be present in electronic prescriptions for controlled substances. Record integrity and nonrepudiation are also critical. I have already discussed how DEA requires controlled substances prescriptions to be maintained by pharmacies, even though they are written by practitioners. Both the pharmacy and DEA looks to these prescriptions for the ability to determine whether these prescriptions were altered.

Accountability is also critical. DEA must look to pharmacies for prescription records. These records must be maintained for at least two years after the date of dispensing. It is important for a pharmacy to dispense a controlled substance and a pharmacy has that corresponding responsibility to dispense the controlled substance only if it is written for a legitimate medical purpose.

Pharmacists and practitioners all have legal liability and responsibility under the Controlled Substances Act. They can all be held liable for dispensing. So, accountability is critical for DEA and for other law enforcement agencies.

Finally, as I noted previously, there must be legal sufficiency for these prescriptions. Prescriptions for controlled substances may be used in the administrative, civil or criminal violations of the Controlled Substances Act. At the criminal level, DEA must ensure that it has the ability to make sure that it meets standards of beyond a reasonable doubt. Electronic prescriptions for controlled substances must be substantially similar to written, manually signed paper prescriptions.

With that, as I have discussed throughout this presentation, DEA must have appropriate law enforcement tools to enforce the controlled substances act. Electronic prescriptions for controlled substances must meet performance standards, which are substantially similar to the authentication, nonrepudiation and record integrity present in written, manually signed prescriptions.

DEA and HHS both look forward to the next two days of meetings and DEA invites input on how its law enforcement needs and the needs of other law enforcement agencies may be met without undue burden.

Thank you very much and we look forward to the next two days.

[Applause.]

MR. CAVERLY: We are going to take a break in a moment. Before we do that, I would invite our HHS colleagues who will participate in the questioning to join us at the table and those panelists, who will be participating in the technology panel to join us as well.

So, let's take a break. I have approximately 25 minutes after. Let's meet back here at 20 minutes to 10:00, please. Thank you.

[Brief recess.]

Agenda Item: Technical Framework Panel

MR. CAVERLY: Once again, let me thank the panelists, as well as the questioners from both agencies in participating in this process. We will be addressing the technical framework for electronic prescriptions for controlled substances in this next hour and 40 minutes or so. As panelists, we have Steve Bruck, who is president of BruckEdwards, Incorporated, Donna Dodson, computer scientist with the National Institute of Standards and Technology, Mark Gingrich, vice president of information technology at RxHub -- I am sorry -- Ken Latimore, is that right, Ken? No. Rick Ratliff. I am sorry. Let me correct my notes.

Rick Ratliff, chief executive officer of SureScripts and Paul Donfried, a partner with Strategic Identity Group. Representing the Department of Health and Human Services as our questioners for the panelists are Steven Posnack and Karen Trudel. For DEA, we have Michelle Ferritto, Linden Barber, Michael Mapes and Cathy Gallagher.

So, with that in mind, let's go ahead and get started. I am going to turn this over and I understand that, Donna, you are going to start us out.

Thank you.

MS. DODSON: Good morning. My name is Donna Dodson. I am with the National Institute of Standards and Technology and I hope everybody went out and had a refill of coffee because usually when you start talking about the underlying technology for this, you can put people to sleep.

I am not an expert on the rules and regulations for FDA. I am not an expert in the health care community and on the HHS side. So, I am going to talk a little bit about the security considerations in building an e-authentications framework. That is my role here today.

So, I am going to start out -- anyway, I am going to start out by talking a little bit about some work that we have done at NIST in the area of e-authentication. Really, e-authentication or any technology should not drive the solution. It really ought to be about the business requirements and when I talk about business requirements in the security area, really what I am thinking about are the laws and regulations that one must consider when looking at that business, the policies that are in place by the organizations and then from a security perspective, looking at risk management. So, you need to look at what your assets are.

You need to look at the threats in the system, the vulnerabilities that may come about and the needed security controls. So, really when you are looking for an e-authentication framework, you really have to start after you look at your laws and regulations and policies and then you need to move into a risk assessment and think about how you are going to manage your risks in the system.

When you are looking at those risks and you are looking at, say, what security services you may need in an e-authentication framework, I find and I heard some different definitions in the discussions today, where people were talking about e-authentication but then also you start thinking about additional security needs that you have. And it is really important to understand what some of these terms mean. For example, authentication, I have a definition and these are some of my definitions. It doesn't mean that they are absolute, but authentication, the process of establishing confidence in user identity.

While sometimes an e-authentication solution doesn't stop just by knowing a user's identity or will it be used to provide things like excess control? I may know who you are, but I may not give you the -- I still may not give you that information. So, excess control is another important feature that one might consider when developing an e-authentication framework.

The idea of signatures is very important in this area and there is a broader definition of an electronic signature meaning a sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with intent to sign the record. If you look at this broad definition, things like a password could be used as a signature. When you look at this definition, you can have things like when you check off an intent box, you know, we all when we load new software, we all get to the point where it says you promise to follow all the rules and regulations, click here.

Some people consider that a signature. You need to go back to your laws and regulations and say does this meet the intent of what I need a signature to be about. NIST and my real area of expertise is in the field of cryptography. So, to me, there is electronic signatures is a broad class and then very particularly there is a digital signature based on cryptography that provides authentication of the signer or message integrity and nonrepudiation, nonrepudiation being that I can go to a third party and show who actually signed the information.

The term "nonrepudiation" in a legal standpoint might mean something else, but just from a technology standpoint. When you are looking at an e-authentication framework, are you really looking at developing a security framework, where you have needs for things like confidentiality so that unauthorized individuals cannot read or review sensitive information? Are you looking for integrity and you can provide integrity without perhaps providing authentication but that the information has not been altered and that that authorization is where you can't detect it.

So, these are all very important questions that you need to consider when you are building your framework and that is the purpose of why you want to authenticate individuals and where you want to go after that. I think if you look at your business requirements and your risk assessment, that many of these security features will come out and you will see if you actually do have a need for these security services or not. You need to factor those in, I believe, when you are building that framework.

Now, when you really start thinking about authentication, you can actually think about authenticating yourself as the human user to something like a work station. You can think about the device being your computer as authenticating itself to the network. You can think about device authentication where you just say that this individual not only has a right to be on my network, but when you look over the entire Internet, you know where a piece of traffic came from.

The last one and the one that I want to focus on today is the remote authentication of individuals across open networks, like the Internet. And NIST has done a lot of work in this area. We have developed a special publication for federal agencies, Special Pub 800-63 Electronic Authentication Guidance.

This guidance came about as a companion document actually to the Office of Management and Budget put out a memorandum to federal agencies because they have been very worried about e-authentication. Also when agencies, federal agencies, are putting up solutions where they are authenticating their individuals and customers to their web sites and how are they doing that.

OMB had really in my mind two criteria that were important to them. It was the level of assurance that you knew who somebody was. So, what is that level of assurance? Then also because it was within the Federal Government, they were interested in promoting interoperability. So, both of these factors play into the OMB guidance policy for e-authentication for federal agencies and this guidance actually lays out four levels of assurance. The way you determine the level of assurance that you need is by looking at things in your business system, the privacy, the inconvenience if you incorrectly authenticated an individual, the damage to reputation, is there a financial loss, what harm would come to the agency, what harm would come to the individual, how much sensitive information, what kinds of sensitive information would be released, what are the personal safety aspects here, what are the civil or criminal violations.

So, in other words, going back, having federal agencies perform a risk assessment on their business applications in terms of the authentication, considering these factors in this second bullet and this will help determine what level of assurance is needed. We are, I guess, the opposite of FDA, if I understand correctly, because Level 1 is the lowest level of assurance. Level 4 is the highest level of assurance.

Right. One is the highest. So, for us, though, when you look at this for folks who are into the prescriptions, you have to look at lowest level of assurance is Level 1 for my presentation today. So, NIST got involved by saying, okay, now you have determined what your four levels of assurance are. OMB asked us to look at appropriate technologies. So, appropriate technical solutions or technologies that would meet each one of the four levels. So, what are the technical criteria when you are out looking for a solution that meets Level 1, Level 2, Level 3 and Level 4?

We identified five areas that we actually discuss. The first one is the registration and identity proofing for authentication. So, how you originally enroll the individual in the system. The second one is in the area of what we call tokens or tokens and credentials.

The third area is how those tokens and credentials are managed and then the appropriate technical authentication protocols. If you are going to assert someone's identity to a third party, how you would do that. So, this is all covered in the document in excruciating detail. I am going to give you a high level overview of each of the four levels and then a few other things to consider.

Level 1, the way it is defined in the OMB guidance, you really don't know the identity of the individual. It just means if I am Mickey Mouse today, I am Mickey Mouse the next time I come in. So, I have little or no assurance as to who that individual is. Basically, you could use a password in this. So, for our technology requirements, we say, okay, a password is okay. The difficulty of being able to guess that password by a bad guy doesn't have to be too great.

Most federal agencies are finding that many of their business applications fall out at either Level 2 or Level 3. There are not a lot of Level 1s. Maybe in this room we have some Level 4. I don't know. I don't look at the risk assessments. They can take a look at 863 and determine the appropriate technologies. So, Level 2 is single factor, meaning often when you think about authentication, you think about something you have, something you know and something you are as being the best way to authenticate an individual. So, if I have all three of those, if I know a password, if I have a smart card and that includes biometric and a cryptographic key on there, then I have something you know, something you are and something you have.

I have the card. I know the password. I have to put my thumb print in order to unlock that token. So, in this case, it is single factor authentication, meaning out of those three levels, you only need one and basically there are some threats that you need to be able to mitigate with that password and with your authentication protocols and your identity proving, et cetera.

Level 3, basically, you get into the area of cryptography and the cryptographic key can often be stored in software as compared to a really nice hardened module that provides additional security, but it also is more expensive. Again, we list out the threats that you need to be able to mitigate here.

Then Level 4 is you get into need for two factors authentication. Primarily, your secret that you are communicating across the Internet is a cryptographic key, but the embodiment or how that cryptographic key is held is usually in some sort of a hardware device, rather than just software on your machine.

So, if you are building the authentication framework, I think there are some other things that you need to consider. What are your requirements for your signature? Do you have a need for confidentiality? Do you have a need for integrity of the information?

I think you have to look at what compensating controls you can expect your users to have. I think you really need to look at your user community. These are all some of the security things that we would think about. In addition, you would need to think about interoperability and ease of use and convenience and cost. All of those things obviously are critical, but this is more with a security focus today.

I know I went over this briefly, but I think my remarks were supposed to be about ten minutes. So, I wanted to give you some background into our document. I should have put the URL up there but I will provide that to these folks. It is up on our web site.

Thank you.

[Applause.]

MR. BRUCK: Good morning. My name is Steve Bruck. I am president of BruckEdwards. We are a company that specializes in the secure business process improvement. Over the past seven years, I have not only been associated with the DEA's electronic prescriptions for controlled substances program, but I have also worked recently with the IGIS's Institute in collaboration with the Bureau of Justice Assistance on evolving the interstate exchange of information between state prescription monitoring programs.

I have also worked with Social Security and the FBI on identity management and document integrity projects and our company currently manages the enterprise PKI for the Department of Justice. Now, I am optimistic that I think it is possible that we can find a solution that would be acceptable to all stakeholders here.

What energizes me about all of this is finding that. Now, the very first speaker this morning used the word "enablement." And I think oftentimes information security gets a bad rap. It is in the news a lot. It is not very glamorous. But when you use this term enabling, then you start to talk about doing things that previously were impossible and they are impossible because you have a reliance on this tradition for a wet signature, some means of guaranteeing some integrity around the process. We are giving you investigative powers that you would not otherwise have.

So, eliminating paper, that is exciting to me, but more importantly, you know, having a prescription that is legible for my own child that I can understand, that is important. So, it is good to be around so many people here this morning that share that same commitment.

Today, I want to share with you some of my observations, based on my experience. Based on that, I will get into some recommendations that I think can foster collaboration, I hope, and help us all drive toward a solution. I was glad that Donna was here today because I think Donna provides some very good foundation for the topics that we are going to discuss here. She didn't mention it, but her name is actually on the front cover of that 800-63 document.

So, let me begin with what I believe to be the fundamental principle that just all have to acknowledge here and that is that the technology doesn't matter if the foundation, registration and identity proofing is done poorly. So, regardless of the technology solution and it could be a PIN password. It could even be PKI, you have to address this process and the technology simply overlays all of this.

So, to echo Donna's point, which is, gee, we need a common language for discussing this. I look back at the NCVHS testimony. I think what struck me was that a lot of folks were talking about the same thing, but using different terms. So, I think for substitute progress to be made, it is vital that the stakeholders use a common language when discussing these key issues. I, like Donna, would suggest that a very relevant guidance comes from NIST's Special Pub 800-63 Electronic Authentication Guidelines and I think this should be used as a reference to support these discussions.

It supplements OMB guidance on assurance levels and establishes the methods that should be used for each and this leads me to my first observation/recommendation. And that would be that in terms of process, it might be useful as a baseline to survey the e-prescription vendors that are out there today and map each of the vendors authentication processes to those defined in Donna's document.

Now, by "vendor," I mean whoever is registering the practitioner. This could be a form of the survey to answer questions that are similar to how is identity verified. Is it done in person? What type of credential is used for the authentication? When does the credential expire? Is the same registration process applied to the office staff? Once issued, how are the credentials safeguarded?

I think the most important outcome of this would be to give DEA and HHS more details regarding the state of the industry, what assurance levels are currently being provided and provide a much needed foundation for continued discussion. So, I think Donna's presentation pointed out that before you look at the solution, you need to look at the threat. So, I want to spend some time now shifting gears and talk about what I see to be the most obvious threats to e-prescribing.

These threats impact not only the practitioner's computer but also the networks. As I mentioned before, NIST's guidelines provide a good list of threats. At this point, these are simply imagined because as Michelle pointed out earlier, electronic transmission of C2s is currently prohibited. But let's just think about this for a second. The central idea here is that if you can compromise the practitioner's computer, then we have a problem. Everything else can be called into question.

I think it is fair to say that prescription drug abuse is a growing problem. Michelle talked about that. I will add one point and that is that on the Internet today one of the most popular subject lines for SPAM is pharmaceuticals. That tells me two things. No. 1, there is money to be made. People are willing to spend money. I think that is an important context for the discussion. So let me begin by just talking about medical devices.

There has been quite a bit of press about this recently, the fact that these devices are built on top of commercial off-the-shelf operating systems and that these systems are vulnerable to attack. Part of this is due to the fact that upgrading these devices is not simple. By doing that, you run into certification issues, but the take-away here is that nevertheless these devices have been compromised and it has happened on closed networks.

So, the obvious question then is, gee, how secure is a closed network? By the way, the common thread between closed networks and open networks, they are all managed by human beings and we all make mistakes. So, this raises the obvious next question. What about private practice computer systems?

Okay. You could say, yes, these systems are secured behind locked doors, but if these systems are by and large connected to the Internet, then how often are these computers being updated with the latest operating systems patches or more importantly virus definitions? Who is responsible for doing that? Is this handled by the practice? Is it a priority? Things get hectic.

So, if this is not being done, then you have a situation where the computer is at risk and it really doesn't matter if the secure protocol is being used to communicate with the e-prescribing network if the underlying OS has been compromised. So, even the best cryptography combined with SSL or virtual private networks isn't going to help. I think this is a topic that the vendors could address in their segment.

So, in this situation acknowledging that the Internet is a hostile place, the question becomes how can we prevent users from accidentally having mal-ware or spyware installed on their computer. One answer would be that simply as a matter of process, we are going to restrict the use of this computer to e-prescribing only. That is all they are going to use it for.

I am not sure this is very practical and this conclusion is consistent with the comments that were made on HHS's proposed rule on e-prescribing exceptions to physician self-referral. A number of commenters, including vendors, indicated that it was unrealistic to think that a physician computer could be restricted to comply with the sole use provision. So, acceptable and complementary uses that were suggested included clinical decision support to access online medical records and a number of the vendors provided a long list of alternative uses that they envisioned the computer to be used for.

So, I think it is clear that these systems are going to be used for more than just electronic prescription. Now, moving away from the practice setting, I want to talk a little bit about the networks. Now, Kelly talked about the NHIN and as we evolve to greater interconnectiveness, I think we have to acknowledge that the integrity of our medical records and the credibility of the entire community hinges on robust security and document integrity.

Looking again to comments on the sole use provisions, a number of vendors shared their vision that physician computer systems would ultimately be used to access other services from other vendors, not just e-prescribing. So, this adds another dimension, not only how is the office protected, but how are each of the networks that the computer accesses protected as well.

So, I think we end up where we started. I think we are left without a good answer unless we start to morph what we are doing today and supplement this with new techniques to mitigate these real threats. I think the gaps are an authentication in record integrity. How you do this really depends on your philosophy. Do you want to simply detect diversion using something like a prescription monitoring program that I think 20 plus states have in place already or do you want to give those folks a break and maybe the pharmacies a break, too, because what we are talking about is giving pharmacists good tools to identify bona fide prescriptions? Do you want to take a step further and prevent this from happening in the electronic world?

So, the question is how would you improve this system in order to prevent diversion? Maybe in the context of where we are today where we have so many competing priorities, maybe it is more like what kind of road map do we have to establish and how can we get there over time? Maybe we have to grow into this.

So, this leads me to my second and third recommendations, which are not so much on the policy side, but more on the technology side. Here you have a picture of an e-mail spoofing and this is an example of an Internet attack called phishing and it is not hard to think that maybe practitioners might be vulnerable to this kind of attack.

But it goes like this. You get an e-mail from your bank. They say something is wrong. In order to correct that problem, please follow this bogus link. It is easy to download CityBank graphics, by the way, create your own web site and you have the person go to that web site and enter their personal information. The fraudster simply collects this. That is an example of phishing. It happened to me.

So, my second recommendation is that the most effective method of improving authentication security as to use to factor authentication, what Donna said. Well, maybe Donna didn't say that. Donna defined a process. This prevents passwords from being stolen and it makes it obvious when the credential is missing. This is entirely consistent with what we see in the Federal Government, which has had some very high profile compromises lately.

First, faced with similar threats in online banking, FDIC was one of the first to formally recommend dual factor customer authentication in 2004, when they published a study entitled "Putting an End to Account Hijacking Identity Theft." You see the quote there. This was in part due to six separate phishing attacks. One, the FDIC within one year, in which fraudsters impersonated the FDIC with bogus e-mails. Like I said before, it is not hard to envision health care practitioners being targeted by these same verifier impersonation techniques. I am using a term there from 800-63.

In response to the latest VA laptop incident, OMB recently developed guidance that specifies the use of smart cards for Federal Government laptops and the Federal Government as a whole came to the same conclusion on a larger scale. Homeland Security Presidential Directive 12, HSPD 12 as it is known in the Federal Government, acknowledged wide variations in the quality and security of forms of identification. The directive calls for the establishment of a standard for secure and reliable forms of identification. It also establishes a baseline card format for all federal users.

My third recommendation is that record integrity standards should be implementation neutral and applicable to all transport methods. Now, Kelly mentioned some of the breakthrough areas. I think it is interesting. I think we all should watch the consumer empowerment area because, you know, one of the things that I have believed all along is that smart cards could play a role here.

Now, the one thing I can tell you with confidence is that the only constant in the IT industry is innovation and this applies both to the data format, as well as the transport. So, our collective IT future can be very hard to predict and it is dangerous to establish what will end up being a long term precedent based on a snapshot of what is happening today.

Now, for example, I think you have to ask the question how is the prescription going to get to the pharmacy. It is entirely possible that some meaningful percentage of the plans will adopt smart cards not only for rapid registration, but also for prescription transport. This is already happening in Germany. So, the performance standards that we develop need to ensure that we validate simply between the pharmacist and the practitioner and I believe digital signature is the most effective method for doing this. Digital signature working in concert with dual factor authentication not only binds the practitioner to the transaction, but guarantees the integrity of the original record and it is a method that will work for a network. It is a method that would work for smart cards.

I also think that the VANS, evaluated networks, might come to see this as a necessity because as EMR continues to evolve and more vendors join this interconnected network, then the number of insiders grows and, therefore, the risk of compromise increases and any compromise effectively, regardless of how far it spreads within the community, it is going to tarnish the reputation of everybody. So, to summarize my recommendations, Recommendation 1, document how we are operating today. Conduct a baseline survey of e-prescription vendors and map each of the vendors authentication processes to those defined in 800-63. I think that is a good starting point to get us all on the same page.

Recommendation 2, the most effective method for improving authentication security is dual factor authentication. I think we should look at that.

Third, record integrity standards should be implementation neutral. This is the only way that the networks can combat the threats against practices, systems and their networks.

I want to use the remaining time quickly to talk about the standards development process and if you agree that the future is hard to predict, then let's look to the past for guidance. I would point to the process that was used during the development of the controlled substance ordering system, which is used in the supply chain for controlled drugs. The system is now successful. It is entering its second year of production operation.

However, you might guess that during the initial meetings between industry and the DEA, industry was fairly cool to DEA's anticipated standards. But as the process played out, both sides were able to educate each other. I think that is important. There really is kind of a mutual authentication education process that goes on.

Now, I understand that some reformatting is done to the scripted transaction. I am not sure how the new 8.1 standard is affecting this. I would like to learn more about that. But during the CSOS design, I think it is important to note that the industry associations played a huge role. HDMA, HealthCare Distribution Management Association, identified first EDI-INT) as the technology they wanted to use for these electronic transactions.

Once they took that step, they adapted their EDI-850 data layer standards, to find how data segments within the EDI message would be used to meet DEA's anticipated standards. They participated in the pilot with DEA and they commented on the proposed rule.

So, I think the take-away here is that that was a very effective collaboration. When you get people into a room together and force them to work together, great things can happen. The end result was that software vendors had a very clear picture of what DEA wanted to do. They had the confidence to invest resources before the final rule, to invest resources for the development of this new functionality and once the rule went final, the entire supply chain industry actually had a variety of DEA compliant vendor products to choose from.

That is a great story. This happened where nothing existed previously. So, I think it is a great example of how to tangibly foster innovation.

That is all I have. I want to thank you for the opportunity to share these thoughts and recommendations with you and I will pass it to the next person.

[Applause.]

MR. GINGRICH: Hello. Mark Gingrich. I am with RxHub. I have been asked to speak today about what we are doing today in e-prescribing to manage the security risk. RxHub has been around for about five years, just over five years now. We were founded by the three largest pharmacy benefit managers and now we have additional coverage through other benefit managers online.

As you can see, the volumes are starting to go up. We are starting to see the hockey stick. Although we are focused on providing benefit information, formulary medication history on the front end of the prescribing process, we also have a -- are very interested in seeing consistency of work flow in process across controlled and non-controlled substances to further drive the adoption that we are starting to see.

Some of you have probably already seen this picture, maybe some of you have seen it three, four, five times. NCPDP, as well as Rx Benefits Coalition, have used this slide. I just wanted to point out our role in the transmission of electronic prescriptions. Our role is in the router segments, also that box known as the router server with firewall.

We provide basically a secure connection or secure channel from the prescribing software vendor to the pharmacy or pharmacy network. We are accountable at a system to system level for authentication between these systems. We also are accountable for our security and privacy management. We hold our network participants accountable as well to their responsibilities for security and privacy, as well as their customers hold them to as business associates.

We also on the point of care side, we expect that they are accountable for authenticating the end user as well as authorizing access to prescribing electronic script. Here is an overview of the features, practices we have in place and production today. Again, first off, it is critical that the authentication authorization is done on the front end and is done by the point of care vendor. Again, there is different levels. I am interested -- I have been tracking what is going on with the authentication partnership. I have been very interested in where that has -- but, again, that is the accountability of the front on the technology vendor.

We lock down at a IP level, static IP. We lock down the senders of systems sending prescriptions to us, as well as in the back and their receivers. Every network participant has an I.D. and a password and we authenticate that on every transaction. We use secure channels, SSL, HTTPS for our secure channel between participants. The audit trail again is very critical. With upfront authentication and a clear audit trail from prescriber to the actual pharmacist allows us to provide accountability and the integrity of the transaction from end to end. We manage that closely.

HIPAA, as far as HIPAA privacy, we are very much follow the reasonable and necessary clause. We have personal health information only for the necessary period for support and the actual PHI information is purged from our system. We maintain the audit trail for seven years. Again, we follow Script 8-1, as do all of the participants in our network and that has the identifiers for both prescriber and pharmacy or part of that. We have a provider directory, which includes a registry of all the physicians or the clinicians and pharmacies that are available through our networks so they know who is available to send prescriptions and who is available to send -- again, industry standard controls and processes, we will about that in another slide.

The last thing I want to talk about here is we primarily don't open a transaction. However, when we go through major standards releases, we will provide a translation feature from one release to the other. We are at this point too large -- have too many participants in our network to try to do a big bang. There has to be a graceful transition. We accommodate translation. However, our customers can opt out of that and do their own translation on the back end, say, pharmacy networks, for instance.

We also in the near future plan to provide translation to and from HL-7 for a particular customer of ours. Putting all these pieces together, having a strong upfront authentication and providing again the audit trail that is clean and from end to end in the process, we feel we definitely exceed what is available right now with the paper or fax type process and feel that with the audit trail that is available does add another -- we can pretty much have -- we do have nonrepudiation from end to end is what it amounts to.

Here is my nerdy slide to throw up here, just for fun. This is just to illustrate again our architecture. On the front end you will see a physician up there in the upper left corner. They are authenticated through whatever means, whether that is password or some sort of digital certificate, whatever that happens to be. The prescription comes through the network. It is locked down, again, down to static IP coming into our network, locked down to a specific secure port actually. Again, limited use -- we don't provide -- it is a very limited firewall. Our routing capabilities, we have that all locked down as well, no routes can make it through our environment without coming in and being authenticated.

The authentication occurs at a system level, user code and password. User code is the participant I.D. That is all again, hashed and secured and not visible in our system. Then on the back end, you have SSL out the other end to the pharmacy. One other thing in the middle, another level of assuredness, we have a contract management system that only allows contracted systems to transact with one another.

Here is a summary of administrative and physical security policy. You can see it is pretty much your standard best practices in the industry. Risk assessment, annual basis, training, annual basis, intrusion detection, if you have issues internally, daily encryption of backups and that is stored off site. So, no data is exposed externally. That is an encrypted, hardened operating systems like was mentioned earlier. To prescribe the actual switch is locked down to specific systems -- operating system capabilities that are required for the transaction processing when nothing else is available. Data retention, again, set for support purposes, as well as long term audit purposes.

A bunch of administrative and sort of office management policies as well and, last of all, change management and problem management to maintain consistency of our environments. I don't want to really dwell on this , but there is a lot of inconsistencies at the state level and the fact that prescribing occurs across state lines. There is just a lot of potential issues that a consistent direction policy from HHS, as well as DEA combined could really go a long way in helping get through some of these issues and increase the adoption rate.

Last of all, I just want to say that, you know, we fully support the evaluation of the emerging technologies, whether it is biometrics, whether it is digital signatures that can and will provide a higher level of assurance of authentication integrity. However, we do believe that what is in place today with authentication on the front end, as well as the integrity we provide through a robust audit trail from prescriber all the way to pharmacist, that that is definitely at a level that would support both controlled and non-controlled substances.

That is all I have today. Thanks.

[Applause.]

MR. RATLIFF: Good morning. My name is Rick Ratliff. I am the chief operating officer for SureScripts. So, just for the record, I am not the CEO. So, make sure Kevin Hutchison, our CEO, recognizes that. But I do appreciate the recognition for the day.

As the chief operating officer of SureScripts, I do have responsibility for the technology operations within the organization. So, I am going to review some prepared comments in line with the questions that were asked in preparation for this meeting. Just to give you some background before I do that, our organization runs an electronic -- a nationwide electronic prescribing network. It was launched in 2003. Our organization was actually launched in the fall of 2001 through the efforts of two organizations that represent community pharmacies, the National Community Pharmacist Association, who represents the independent pharmacies of the United States and the National Association of Chain Drug Stores, who represent the chain drug stores of the United States.

So, those two organizations came together, formed SureScripts in the fall of 2001 and we launched our network in mid year 2003 on a pilot basis and really went nationwide early 2004. So, I am going to give you a practical perspective very similar to what you just heard from Mark as to what we have put in place from an infrastructure and what we are actually operating today on a 24 by 7 basis.

So, as background to SureScripts, our organization is committed to building relationships within the health care community and working collaboratively with key stakeholders to improve safety, efficiency and quality of health care by improving the overall prescribing process. I think it is real important to note that last component. So, as I go through my comments, I am going to emphasize some of the aspects of the prescribing process that we focus on that are relevant to what happens actually outside of the network because it is our focus to ensure that eventually we are transmitting as many prescriptions electronically as possible.

So, at the core in our efforts is our network and as I suggested, it is an infrastructure that allows for communications between physicians and pharmacists and it is very important to note that these are communications. These are messages that move back and forth between these constituents. I will describe that in more detail in a minute. But it is not electronic mail. I think that is a real important point. It is also -- it is two-way communication. So, it is not -- it does not involve reduction of a prescription created electronically in the physician's office, the paper, at any point along the trail.

So, it is end to end electronic communications. Again, that is a very important point as we talk through how this infrastructure could enable the transmission of controlled substances.

So, today, more than 90 percent of the nation's community pharmacies have tested and certified their pharmacy applications on our network. What that means if you look at an analogy in the world of cable, a lot of our homes are enabled for cable TV -- or cable TV primarily and in order to turn on the cable TV, you will likely need to contact your cable provider and bring in a box and bring it up and start paying for the service. But the service is basically there in the walls of your home.

Similarly, we have enabled the majority of the pharmacies in the United States to do electronic prescriptions as I described a minute ago in a two way fashion and there were about 30,000 of the 55,000 community pharmacies approximately in the United States that are actually doing electronic prescriptions today. So, about 90 percent of the 55,000 are certified. That means they have the cable connectivity and about 30,000 of those pharmacies have actually turned it on in their pharmacies and are actually doing electronic prescribing.

In addition, SureScripts has certified out of 40 clinical solutions that enable electronic prescribing within the ambulatory physician practice, by the end of this year we will have around 60 different systems certified for connectivity into the network.

These systems range from stand-alone electronic prescribing systems that are -- some of you know of the mobile electronic prescribing systems to comprehensive electronic medical record systems available from some of the high end health information technology providers. We began, as I said a minute ago, the rollout of our electronic prescribing network in June of 2003 and we are now transmitting electronic prescription information between the prescribers and pharmacies as I also described in about 46 states.

So, we are pleased to report that today -- and remember, we have been doing this since 2003, using our electronic signature processes that I am going to describe in a moment. We have maintained the confidentiality and integrity of these transmissions for the prescriptions that can be transmitted electronically and have had no instances of tampering. So, before I address the specific questions posed by the DEA in the announcements for this meeting, I think it is important that maybe I walk through something similar to what you just saw a moment ago from Mark related to how the electronic prescribing network operates.

I am going to go into a little bit more depth to help address some of the points that were brought up by the first two speakers related to e-authentication. So, if you refer back in your memory to the network that Mark put up that was the NCPDP diagram that showed the end to end process, that is the process that is in place today. And SureScripts is an electronic prescribing network that acts similar to RxHub in that we are routing infrastructure to move the information again between the prescribers and the pharmacies.

What I want to do is kind of take you through the prescriber elements, the network elements and the pharmacy components and then I am going to describe to you in more depth what we do from a network perspective, but I think it is important to understand the NDN process. Before a prescriber can transmit an electronic prescription on our network, they have to be using a certified solution that has gone through our process. So, I mentioned, we have 40 certified solutions today. We have a very stringent certification process that each individual vendor has to go through in order to certify their solution and then each one of those vendors must register each one of their users in our network and there is an authentication process that goes on through that process.

Once a prescriber is registered, the prescriber is assigned a unique I.D. At least in our situation, we call that a prescriber I.D. So, it is an SPI. The prescriber is identified uniquely inside of our network and it is required in order to be able to send a prescription to a pharmacy or to receive refill requests from pharmacies. So, it is real important to note they have got to be using a certified solution. The user has to be registered in the network and that particular I.D. that is provided to the user then is attached to every prescription message that is sent to a pharmacy or received from a pharmacy in this case.

So, the prescriber accesses in their cases, as Mark was describing, typically their particular solution that they have contracted for and usually they are using an I.D. and a password to get onto that system before they write a prescription electronically. Some systems do use PINs. Some systems do use PKI technologies and other solutions for authenticating and securing that particular prescription.

Once the user is able to create the electronic prescription that gets it through the network, is sent through the network typically using the Internet to initially the certified solution provider's infrastructure and then from that point, there is a point to point connection similar again to what Mark described earlier, where there is a unique IP address, static IP address that is identified between our network and that aggregation point, if you will, of the certified solution provider. So, again, the user has to be contracted with a software vendor, using a certified solution, registered in the network, writing prescriptions electronically, sending those securely through the Internet to the certified solution providers network infrastructure and then there is a point to point connection between that particular provider's network and our network.

At this point, all SureScripts prescriber pharmacy CSPs connect to our network, utilizing secure connections, as I just described. There are some that use private lease lines and you saw some of that again on Mark's slide. Most are using the Internet, using different types of encryption techniques, whether it is DPN or SSL. Every message received from a prescriber or a pharmacy, again, must have the SPI attached to it, but in addition., every pharmacy is also uniquely identified. So, we not only have a registry for physicians, we have a registry for pharmacies. So, every pharmacy actually in the U.S. as they come on line is to sign an NCPDP provider I.D. That NCPDP provider I.D. is associated with every prescription message that moves through the network.

So, with these two unique I.D.s, no electronic prescription or refill renewal request can be without these two. They cannot be transmitted through the network as I have just described. We also require contractual agreements with parties on both ends of the network so we do have the appropriate business associate contractual agreements with prescriber and pharmacy vendors or pharmacy chains. These actually create the chain of trust relationships from the prescriber to the prescriber software vendor to our network to the pharmacy software or the chain pharmacy themselves.

So, again, there is a chain of trust relationship. On the pharmacy side, the pharmacy CSPs or the pharmacies themselves must register the pharmacy on the network, as I described a minute ago. We utilized the NCPDP provider I.D. Each pharmacy partner, including the pharmacy chain, software vendors representing independents or clinics as an example, are assigned a unique IP address as well. So, there is a static IP address and one connection between our network and the chain headquarters or the software vendors headquarters as well. This is how the messages are transferred, again, either using frame relay, private network connectivity or the Internet, using different encryption technologies.

Note that in almost all cases. pharmacies and pharmacy CSPs are transmitting electronic prescription messages to the actual system at the store location. So, it is important to recognize again most of the chains as an example will aggregate their store locations. They run their own network. So, CVS is an example that has 5,000 plus locations or Walgreen's, which has a similar number. We transmit messages to and from there central point if you will and they manage prescriptions to their store locations.

So, this gives you some idea of the infrastructure that is in place today and that is operational again. It is operational on a 24 by 7 basis. Again, prescriptions run out of 30,000 pharmacies in 46 states.

So, let me kind of hit some of the questions that were asked prior to the meeting. There was a question related to the current risk associated with electronic prescribing. Today, the current risks associated with electronic prescribing are really the same as those associated with storage and processing of other types of sensitive or valuable information. Patients and providers are certainly concerned with the potential risk of protected health information or PHI to unauthorized individuals or entities in all stakeholders in the process want to access PHI or want to make sure that access to PHI is restricted and only those that have a legitimate need are using or viewing that information.

So, in addition, prescribers, pharmacists, regulators, law enforcement professionals are aware of the use potential of the Schedule II through V controlled substances, as we have been discussing but as well as many non-controlled substances. So, given the ways to which criminals will go to obtain controlled substances by elicit means, one clearly must consider the unauthorized and illegal use of the technology by them to be a potential risk and we have talked about ways to help mitigate those risks.

We, as I suggested a minute ago, have a great deal of experience with electronic prescribing and we have identified potential risks through our efforts over time, but we have also brought in third parties to review our network infrastructure, provide security, audits and assessments and provide us direction on different areas of remediation and, again, addressing many of the key points that Mark brought up earlier in his comments.

Our provider that has supported us from a consulting perspective in this area has helped us a great deal early on and in our network evolution as well as on an ongoing basis as we look at our network and ensure that we are mitigating risk at all levels. We believe that the electronic prescribing process that I have already outlined does help minimize risk and greatly improves security for the prescribing of all prescriptions in comparison to today's written and oral processes for prescription information.

At the end user level, electronic prescribing does allow for efficient authentication as I have suggested, I.D.s, passwords, PINs, creation of a legible electronic prescription, association of these prescription with prescribers via an electronic signature, the SPI, as I discussed a minute ago. In addition, the end user systems document those electronic prescriptions and patient medication listings in a variety of ways. So, there is a record at the physician level today, although as we heard from the DEA comments earlier, the record is not necessarily a requirement at the physician level, but what electronic systems allow us to do is actually create a record. So, you should keep that in mind when you think about the end to end components and this idea of nonrepudiation.

Electronic prescriptions are captured in a standard format. I mentioned NCPDP a couple of times. We do use the NCPDP script standard Version 8.1 in our network. So, these messages are all -- the new prescriptions, as well as refill prescriptions are all captured in this format and authenticated using electronic signature functionality, as I described already.

So, electronic prescriptions are saved in our system. So, in a somewhat different fashion than what was described by Mark. We do save every transaction as it flows through the system. So, every transaction is saved in our system for seven years and, therefore, again, there is a record of the transaction at the physician's office. There is a record of the transaction in the SureScripts network. Those transactions are saved today purely for audit purposes. If required in the future, they could be used for other purposes, but today it is purely for audit purposes.

Pharmacy systems then receive the prescriptions from the trusted intermediary in this case, our network.. Proof of the efficacy of these procedures is again, as I have already mentioned several times, lies in the fact that we have managed prescriptions across a large number of pharmacies over the last several years.

So, one of the questions asked, you know, are there risks pertaining to prescriptions for controlled substances that are different from noncontrolled substances. SureScripts would agree that the criminal intent is more interested in using violent means going after schedule medications, no matter what mode of transmission. However, we believe the current system that I have been describing supports a highly secure transmission of prescriptions regardless of the schedule.

Our system allows for the tracking and auditing of prescriptions, which is not possible on a timely -- at least on a timely and scalable basis in comparison to processes today. Again, prescription informationists say that the physician level through their electronic system save in the network in the one piece I didn't mention is also these prescriptions obviously are saved at the pharmacy level. So, we don't believe that any -- SureScripts does not believe that any additional modifications we have currently in place would be necessary for us, our prescribing and pharmacy certified solution providers or client prescribers or pharmacies to be able to use the network for the secure and efficient prescribing of controlled substances.

We did employ a security strategy of proactive defense defined as a combination of standard security principles to ensure secure design implementation and operations of our network and these do align with accepted industry best practices in addition to our experience as I have been describing.

Very similar to a couple of the charts that Mark put up, I mean, we do have a number of standard practices in place and as our technical guys would describe them, I mean, we have -- we employ the best practice called defense in depth in that we have multiple layers of security built into our network infrastructure. We do things such as use different types of standard based firewalls and routers. So, we would use different manufacturers at different layers in the network to further ensure an ability to penetrate the network.

We also look at different processes to ensure that individuals are only given privileges and access to information that is necessary for their particular job functions. The network does have 24 by 7 monitoring, both from a physical security perspective, as well as network and application monitoring. We also employ standard practices for analyzing and understanding new threats or vulnerabilities in the network ensuring that servers and other systems are current on patches and other types of system level updates that are necessary to ensure we have plugged any potential holes that have been identified by some of the standard providers.

We also have intrusion detection services built into the front end, as well as to the interior parts of the network and we monitor potential threats and update those IDS, as well as virus kinds of signatures over time. So, as described above, the prescriber has to utilize a certified solution, must be registered in the network before they can transmit electronically. The subscriber must be using a CSP solution. All right. They have to have in that solution as we certify those solutions, at a very minimum must have an I.D. and a password type of authentication. They are provided in an SPI.

This is the type of authentication that is currently in place today. All right. The business and technical structure of our network provides a framework for the secure transmission of a prescription from prescriber to the pharmacy, as I have described. There are appropriate business agreements in place with all participants in the network. The combination of both the prescriber and pharmacist authentication are secure network transmissions, static IP addressing and other security types of services and processes we put in place today to protect the electronic prescriptions through the NDN process and the network.

Last, electronic prescriptions are stored within the different systems as I have described previously so that we can create a prescription, if needed, from the time that it is written through the network to the time that it is stored and processed and dispensed at the pharmacy. So, there is a question about future threats. We continue to evaluate security threats via, again, I mentioned our third party, security assessment. We look at our own risk analysis on an ongoing basis. We do have a number of risk management procedures in place.

The threats, the most likely to occur, such as viral infection, unauthorized access, denial of service attack, have been mitigated in our opinion through various means, such as anti-virus scanning, I.D. intrusion detection, port restrictions, at least privilege access, a number of other things that I have already described.

Relative to innovation in the use of other technologies, second factor authentication, smart cards and those types of things, a lot of those technologies will provide an incremental level of comfort related to authentication, nonrepudiation, et cetera, for the additional cost and complexity that are associated as well as given the interoperability of the different types of technologies or those things that are necessary to support many of those types of technologies that is needed.

We have supported and we have promoted and we have put the NCPDP script standard into actual execution and we have shown that messages can be moved back and forth between prescribers and pharmacies. We are now supporting other standards, such as X12. We have promoted the use of XML and are moving an XML specification related to the NCPDP script messaging through the NCPDP standards organization.

We are doing an HL7 to NCPDP script mapping today in the network for a few clients. So, we believe in innovation. We believe innovation is necessary but we also believe that the systems in place today provide a great deal of security and protection for prescription information as it is captured in a prescriber's office and moved to a pharmacy and communications happens back and forth.

So, I appreciate the opportunity to provide some vision of a practical implementation of electronic prescribing and our experiences and we will look forward to moving this discussion forward, as we have been working on this for some time and, you know, just to kind of reemphasize the point, I mean, there are 3 1/2 billion prescriptions written a year. About 1 1/2 billion of those are new prescriptions. Eleven percent of those are controlled substances. About 150 million prescriptions are written each year that could be transmitted electronically, that provide us additional audit trails, additional levels of security that are not available today with the current oral and annual process. So, there is significant opportunity here for us to streamline the process and provide actually greater securities.

We look forward to looking at opportunities to make this happen. Thank you.

[Applause.]

MR. DONFRIED: Thank you. Good morning and thanks for the opportunity to testify on the Technical Framework Panel at this public meeting.

Your focus for this panel, authentication, signature requirements, recordkeeping requirements and the mitigation of risks is an area that has been the sole focus of SAFE since October of 2001. It is my privilege on behalf of SAFE to share with you this morning our perspective on the risks involved in e-prescribing. During this morning's speech, I will outline the approach SAFE has developed and some of the key learnings identified to date as our members just now begin production and implementation of their own applications.

My name is Paul Donfried. I am a partner with SIG, the Strategic Identity Group. I specialize in the area of electronic commerce, with a particular focus on the area of legally enforceable electronic signatures and the underlying electronic identity frameworks. My education is from Renssalaer Polytechnic Institute in computer science and mechanical engineering. But I find my continuing education has been in law, governance, standards, user experience and other areas leading to a more anthropological focus.

The challenge I would suggest is not the availability of suitable technology, but the particular problem of shifting complexity away from the end user as we look to benefit from that technology. This has been and continues to be my particular passion. I am here representing SAFE-BioPharma Association, an initiative being supported by a number of biopharmaceutical organizations. I am a contractor that has been -- to SAFE BioPharma to support the executive management team. I was one of the founders of SAFE and have been a champion of this initiative for the last five years.

In spite of what it says on your agenda, I am not

Terry Zagar. We can discuss authentication of that separately. The views I share today only represent the perspective and the learnings that SAFE has developed. The critically important public policy issues, which DEA and HHS are addressing here have potentially different requirements in drivers than does SAFE.

I will limit my remarks to sharing our community's experiences and perspectives as we navigate implementation of a global trusted electronic identity infrastructure created to support legally enforceable authentication, signatures and recorded electronic evidence of those transactions. SAFE does not build applications. SAFE focuses exclusively on the trust infrastructure that applications need to support the three critical requirements that were mentioned by Michelle; authentication, nonrepudiation and record integrity. We work with vendors, such as Adobe, Document and Microsoft, et cetera, to ensure the commercial off-the-shelf solutions are compliant with the SAFE standard.

Our approach to this is based on open standards and as possible, open source software. One month ago, one of SAFE's members made available via source -- an open source implementation of the universal SAFE signing interface, a web-based signing solution that provides for an easy integration of electronic signatures into desired documents. This is akin to Pay Pal for payments in terms of a web service that you can invoke for many sort of application or web site.

This is very significant because, for instance, with a complex commercial document management system, it has reduced the engineering integration effort from months to days. Not only does it radically simplify the historically complex integration of sophisticated security mechanisms, such as PKI, it also automatically provides for the production of an electronically signed and independently notarized evidence of the signature transaction.

Now, let me address the specific questions that you requested the panel to comment on. What is our perception of the current risks associated with electronic prescribing and how did we identify them? We see two distinct areas of risk that need to be managed when moving from paper-based processes to end-to-end electronic processes. One, the need to ensure that the controls and risk level of the existing processes are at least matched in the new electronic processes.

Steve spoke very eloquently to this and his first recommendation was to do a baseline mapping of those existing processes and controls and ensure that those levels of risk are at least as adequately managed in the electronic process. The second area is the need to understand any new threats and risks associated with the new process that may not have existed or been possible with the old processes. Identifying and managing these risks associated with the first area is fairly straightforward because there is lots of experience to draw on with the existing paper-based signatures and systems.

However, identifying and managing the risks associated with the second area the new threats and risks that may be unique to the electronic processes and systems is not quite as straightforward and, in fact, requires applications of disciplines like failure mode analysis, penetration testing and ethical hacking.

In other words, to identify the new risks, you really need to think like a malicious, greedy, intelligent criminal or terrorist because as it turns out, they are quite interested in exploiting these types of systems. Let me use identity theft as an example. Has it always been a risk even in the paper-based world? Absolutely. Think of Pan Am and the movie "Catch Me If You Can." Now think of new systems like e-Bay, electronic banking, et cetera. Why have we seen such an explosion of electronic identity theft? Is it because all these electronic process operators are lax or ambivalent to the issue? No.

The problem is that with these new systems, there are new forms of threats and attacks that were not possible in the old paper-based systems. When we approach the design of new electronic systems, we cannot be satisfied with merely managing the risks we have always known about. How does SAFE address those risks? In June 2004, the President's Information Technology Advisory Committee published a report revolutionizing health care through information technology. The report stated that, "A robust NHII will require a firm foundation of trust. Americans must be assured that the confidential health information will not be misused and if there are adequate legal remedies in the event of inappropriate behavior on the part of either authorized or unauthorized parties."

Furthermore, the report goes on to state, "Health information can only be accessed with adequate security and privacy if there are clear means for verifying the identities of those accessing and altering data. The lack of defined standards for security and the lack of an accepted hierarchy of trusted authentication agents impedes the development of the NHII and associated cost effective data communication systems."

I reference the previous quotes because they stem from the following Medicare Modernization Act requirements upon which the SAFE standard has been formed. Support interactive and real time transactions. Comply with HIPAA privacy and security regulations. Be compatible with other standards. Include quality assurance measures and systems. Improve efficiency, including cost savings. Not present an undue administrative burden on prescribers and dispensers. Vendor neutral and technology independent.

In answer to the question that you posed to the panelists, how do we address risk, I would like to specifically focus on the trust insecurity objectives that I just quoted from the federal requirements. As I mentioned earlier, we sought two fundamental areas that required risk management. Managing the risks we already knew about and had established controls for on the existing systems and then those new risks that only existed because of the new electronic systems we were proposing to put in place.

The conclusion SAFE came to was that there are two essential controls, which end up defining the highest level of achievable risk management within our system or any system for that matter. Again, I would defer to the comments you heard from Michelle and Steve, who I think also eloquently spoke to this. The first of those conclusions was that an essential ingredient is the binding of an electronic identity to an electronic transaction. Electronic user X performs electronic action Y. We saw fundamentally only two cryptographic mechanisms for technically establishing that binding. Symmetric key or asymmetric key cryptography. Symmetric key works great if you never have to resolve disputes outside of the governance domain of the entity controlling the keys.

Unfortunately, for us, our members are independent legal entities, for profit companies, non-profit institutions and government agencies. Litigation happens and our system needed to support independent validation of evidence. In other words, a very high degree of nonrepudiation. Our conclusion, consistent with mathematicians, lawyers and judges, was that asymmetric cryptography or PKI was the only mechanism that can provide a high degree of legal nonrepudiation.

Secondly, the binding of an electronic identity to a human being. We looked very closely at global standards for the registration issuance and life cycle management of electronic identity credentials. Our conclusion was that we needed a high degree of due diligence for these processes, including person to person authentication and real time key generation in the control of the subject being credentialed.

As we evaluated NIST and U.S. Federal Government standards, we became convinced that SAFE needed to meet or exceed the U.S. federal bridge certification authorities medium assurance Level 3 requirements. Those require two factor authentication where one factor is a hardware token protecting the private key.

Our current requirements for identity proofing, authentication and credential issuance are designed to fully comply with these requirements as well as those of the European Union.

Another question you asked the panel are risks pertaining to prescriptions for controlled substances different than prescriptions for non-controlled substances? I will make my response here general since I do not presume to understand the risks associated with prescriptions of controlled substances anywhere near as well as the distinguished people in this room or your other colleagues at DEA, DOJ and HHS. I do know, however, that different transactions can carry very different risks. One dimension of this is the literal value of the transaction itself and this value can be influenced by the scarcity of the item, its direct and immediate financial value and/or the impact of its loss to the rightful owner.

In this context a life saving medicine that fails to be accurately dispensed to the patient in need has enormous value, even though it may not be a controlled substance. History would suggest that greed is a large motivator in the diversion of controlled substances. This would suggest that there is an economic motivation or perhaps an addiction associated with controlled substances that might compel criminals to invest substantially more in attacking an e-electronic system that might provide access to these medicines. There are, however, other motivations, as terrorism has directly shown us, where the motivation is to cause the greatest disruption, negative impact or to destroy trust in the systems themselves.

As merely a consumer of prescription medicines, it would seem to me the threats of the past, which may have been limited to controlled substances must now be considered in the broader context of the overall medicine delivery chain. So, I would answer your question are the risks different, yes. They certainly are different risks. I would also suggest that electronic prescribing systems by their very nature introduce new risks, which must be managed. But I would suggest that perhaps a more relevant question is as we move to electronic prescribing, are there new risks being introduced,. which could substantially impact the American people independent of what type of medicine is chosen as the target, controlled or non-controlled.

I must also mention that SAFE used appropriate application of policy, process and technology as yielding solutions with which we are collectively much better able to manage risk. You have heard some comments to this point already. Part of this is due to the transparency of these solutions. We end up with transactional systems that provide complete end to end legally enforceable audit trails. These audit records can be cryptographically managed with techniques that can ensure integrity, provide tamper evidence, tamper resistance and perhaps most importantly accountability with a very high degree of nonrepudiation at every point within the process.

I would now like to address the remaining questions by briefly describing the approach we have taken to the development of the SAFE system. In late 2003, several biopharma industry sponsors and the FDA came together to begin the process of determining if a meaningful business case existed for an identity assurance standard in the sector.

While the industry made progress on many electronic information exchange standards, the fundamental components still absent was trust. By trust, we simply mean reliably establishing the identity of the party with whom business is being conducted. It took the industry less than four months to determine that establishing an identity assurance standard under a shared cost model was essential to removing paper-based record constraints that have been plaguing the industry.

In early 2004, the SAFE Coalition was formed and sponsored by PHRMA, Pharmaceutical Research and Manufacturers of America, including leadership and resources from 12 biopharmaceutical companies, with development contribution and governance oversight from the FDA. The SAFE Initiative has been focused on the creation of an identity assurance standard for use by the biopharmaceutical industry in business to business and business to regulator transactions. What is a SAFE standard? SAFE represents a practical implementation of various open standards, such as ITU, X509, 6140 set of standards, ITF, RFCs.

The technical trust infrastructure is based on the use of digital signatures that will be certified by trusted third parties, such as commercial certification authorities, regulated financial institutions and SAFE BioPharma Association itself. SAFE's trust framework is based on a PKI bridge architecture, which provides technical interoperability between previously separate isolated domains. As an example, SAFE's bridge architecture has been developed to allow for cross certification with the PKI, such as the U.S. federal bridge CA.

This architecture also allows SAFE participants to leverage existing investments in internal credentialing solutions. For example, Johnson and Johnson has 70,000 employees worldwide, who are already credentialed with two factor USB-5s and those individuals are now recognized in the SAFE community through the SAFE grid CA, which is cross certified with the J&J internal CA.

Fundamental to electronic prescribing in SAFE is the ability to verify the identities of the physicians and the pharmacists engaged in the prescribing process. The SAFE standard includes a set of business policies and procedures, operational guidelines and technical compliance specifications. This standard set defines the elements necessary to manage the complete credential life cycle, apply electronic signatures to a document and technically deploy SAFE credentials.

SAFE is based on a closed contract model similar to that of a MasterCard or a Visa. Key elements of SAFE include high security. SAFE provides for strong security and data integrity through the use of two factor authentication combined with PKI. SAFE security specifications embrace international standards and best practices to ensure use of integration, ease of integration into user systems and applications.

Legal effectiveness, SAFE's credentials and digital signatures, they create are designed to be acceptable for use in data collection and exchange, development, authoring, review approval of regulatory documents and filing processes. This is accomplished through a contract structure through which parties agree to abide by the technical and legal components of the SAFE standard.

Regulatory compliance acceptance. SAFE has been designed to meet various regulatory, technical and operating compliance guidelines, such as those specified in PDMA, 21 CFR Part 11, HIPAA and other similar local, regional and international regulations.

SAFE, the company, is a member regulated not for profit enterprise. SAFE BioPharma Association operates as a shared cost platform for the benefit of all its users and members. The role of SAFE is to manage, maintain and enforce the standard, provide a legal and contractual enforcement framework, provide necessary technical infrastructure to bridge despaired credentialing systems into the same environment, provide a channel via direct contracted and accredited issuers for the issuance of SAFE credentials, promote the adoption and use of the standard by SAFE participants and with other messaging submission standards.

Lastly, support vendor supply of SAFE enabled applications and services. SAFE has been created as an independent entity to ensure that the safe standard is available for production quickly. Longer term, there is a potential that the safe standard might be positioned under the management and control of some existing standards organizations.

How does SAFE work? Credential issuers are formally accredited by SAFE. Once accredited, SAFE issuers verify and confirm the identities of legal entities and their employees. Participants enter into agreements to abide by the rules of the trust network. Issuers then provide digital signature credentials to the companies and their employees.

The SAFE credentials can be used to authenticate users and sign transactions to any enabled application in the system. SAFE requires issuers to provide validation responses and audit trails in real time to establish who signed what transaction, that the credential was valid and in good standing at that time and then using digitally signed OCSP responses and trusted time, to establish at precisely what date and time this occurred.

The SAFE infrastructure can provide response receipt messaging capabilities establishing an auditable chain of transaction validations with trusted time stamps from the point of signature through identity validation, to transaction archiving. The identity credentials are also validated without the data that is being signed needing to be transported across the network.

The SAFE implementation enables a physician or pharmacist who is transacting with multiple entities to use his or her credential with all SAFE enabled participants. This is a critical point because requiring a doctor to manage multiple identity credentials, especially multiple passwords, makes it much more unlikely they will be able to successfully comply with the individual policies associated with each identity credential.

Writing down passwords or writing down secure I.D. PIN codes is a classic example of this. Let me provide a specific example of how SAFE is being applied today by HHS through the National Cancer Institute. In alignment with the NCI Cancer Biomatics Information Grid, NCI is establishing a new application called Firebird. Firebird will use SAFE electronic signatures to automate the process of clinical investigators' registration materials for participation in clinical trials.

Firebird will eliminate the need for paper and wet signatures by enabling physicians, their staff, NCI and FDA to rely on SAFE electronic signatures applied directly to the electronic forms. Active participants in this, include a number of major cancer research institutions, major pharmaceutical companies and the FDA. Firebird is integrated into a broader plan for providing SAFE credentials to investigators and their staff globally, funded by industry.

SAFE has also developed ISSUE or accreditation and applications enablement certification programs. SAFE has been working with the vendor community over the last four years to ensure there is commercially available middle ware to deploy common standard and to minimize integration complexity. The example I gave earlier of the universal SAFE signing interface being made available as open source code is the most recent example of that.

SAFE is working with both financial and non-financial institution issuers and over 40 application vendors to manage the supply capabilities required to meet demand. Applications that are already PKI-enabled are fairly easy to SAFE enable. Becoming SAFE certified requires that application vendors conform with the safe policy framework as specified in the SAFE functional specifications.

SAFE in electronic records. Driven by the desire to cut costs, improve patient outcomes and reap the benefits of electronic business processes, SAFE sponsors are investigating the legal, business and technology requirements associated with making use of electronic means in the creation, transmission and retention of records. Internal differences in the assessment of these requirements may discourage entities from searching for a coherent or common approach, as was described earlier.

One difficulty in finding the, quote, unquote, adequate solution appears to be different sensitivity levels, e-records, like paper records, have in practice. Some e-records represent legal or business assets, such as contracts, intellectual property, privacy data, regulatory files, evidentiary materials or prescriptions.

Those require a high level of electronic reliability and strength. In our experience, electronic prescriptions and related data fall into this category. SAFE provides the necessary infrastructure and controls to support legal and regulatory requirements for archive and record retention. In no way does this standard limit how an application chooses to format or structure its records. Regardless of the standard adopted for e-prescribing, SAFE believes it can support the e-record requirements associated with that.

I have hopefully communicated to you that SAFE is not about pharmaceutical companies or drug development or regulatory compliance. SAFE is a mature set of electronic identity infrastructure standards that can be used to support any type of authentication and signatures amongst different stakeholders within the health care community. SAFE is committed to working with appropriate standards organizations and with the oversight of DEA, DOJ and HHS for creating a secure trust platform for e-prescribing and more broadly e-health records.

Independent of your perception of the relevance of SAFE, I commend your efforts and commitments to advancing the health care infrastructure. Thank you again for the opportunity to participate today.

[Applause.]

MR. CAVERLY: Once again, thank you, panelists, for adding your expertise and information to this process.

We are going to take the next few moments remaining for us in this time slot to entertain questions from HHS and DEA personnel that are here on the stage with us. I would ask those that ask the question to identify themselves. Please use the microphone and those panelists that answer to also utilize the microphone in front of them.

So, I am going to give the first question to our HHS colleagues and if you have some questions to ask the panel.

MS. TRUDEL: This is Karen Trudel from HHS.

Mark, you mentioned as a barrier the fact that pharmacies may not know how to validate an electronic prescription and that there appeared to be a need for some guidance in that area. Could you kind of elaborate on that point a little bit?

MR. GINGRICH: I am not sure. Validating of the electronic script?

MS. TRUDEL: I believe that was in one of your slides, that a pharmacy may receive an electronic prescription and wouldn't really know what to do to go about validating it the same way that they would if they had a paper prescription in their hand.

MR. GINGRICH: What it amounts to, all the information is there as part of the script. If they have a concern that this is not a valid script, they can call back the physician and validate the identity of the physician. If they so choose and if they require a wet signature, they can also fax back the acknowledgement of the prescription. So, I think the mechanics are there --

MS. TRUDEL: Right. So, as part of rolling out any kind of an electronic signature process for controlled substances, there would be the need for some accompanying guidance.

MR. GINGRICH: Right. I think that is what it amounts to. I think right now there are just different ways and different requirements at different state levels. I see a nod of the head here from --

MR. RATLIFF: I am having trouble hearing you. I don't know about the audience. Can you hear the speakers?

If I can just make a few comments. Today as the system is in place, there are, as I was describing, there is a connection and it is a point to point connection between the pharmacy's headquarter systems and in our case, our network. So, there is -- and there is authentication associated with that connectivity. So, there is also the registration process of the physician, et cetera. So, from a technical perspective, there is a high degree of comfort that the prescription is coming from an appropriately registered and authenticated end user.

However, as Mark was describing, this is a new mechanism for receiving prescriptions, right? So, most prescriptions today come in the -- you know, a manual process, a fax process, et cetera. The only thing the pharmacist has in their hand at that point in time is either the written prescription and given the volume of prescriptions they are managing, they are not going to recognize every physician's signatures, et cetera. Prescription pads do get stolen and this is a part of the diversion processes we have today. Then there are other things you can do on the fax end.

So, what we have to do is we have to help make sure and this is a part of what the pharmacies do is to help train the pharmacist and the staffs on managing of electronic prescriptions, in addition to what they are doing today, but also understanding the mechanism for which that prescription arrived to the pharmacy and that it is not, again, just a general e-mail because this is a really important point. It is not like anyone logs on to the Internet, creates an e-mail, makes it look like a prescription and sends it to the pharmacy. That does not happen. I hope that helps.

MR. CAVERLY: Thank you.

DEA?

MR. MAPES: A couple of questions for either Mark or Rick. Does your system allow for office staff other than the doc or the prescriber to send the prescription information to the pharmacy at the direction of the prescriber?

MR. RATLIFF: The ability to do what you just described, Mike, depends upon the actual end user application. So, there are obviously different protocols and there are different state, potentially even federal regulations that mandate how prescriptions are written and transmitted. However, for some prescriptions it is possible for a nurse practitioner to capture that prescription and send it on behalf of the physician. However, in the NCPDP script standard, there is actually a component that allows you to identify the supervisor, if you will, of that individual.

So, if the individual is able to route a prescription as an example for a prescriber, then that prescribing supervisor, if you will, would be attached to that prescription as well. Various state laws and regulations require that to be in place. Not all states do.

MR. MAPES: In kind of a follow-up to that, how would a doctor know if the system were compromised? For example, if the other office staff were allowed to prescribe, not prescribe, but to send the information for the doctor and they had a separate PIN and password to do that and they gave their password to someone else, how would the doctor know that more than he was authorized was being sent to the pharmacy? Is there a way?

MR. RATLIFF: Again, that would depend -- the actual process would depend on the application. Okay? Many of the applications have roles-based security. The role would suggest that, again, for certain types of prescriptions in certain states, you could write the prescription as an individual in that practice, assuming you are using your I.D. and password, you are likely going to be restricted as an individual.

Again, every prescription is captured. So, there are actually some states where prescriptions are being printed at the end of the day and are being reviewed by the practice to ensure that there is not an abnormal number of prescriptions being written or prescriptions written that the physician was not made aware of. So, there are other controls that are put in place. There are a number of situations to help monitor volume of prescriptions written that are outside of just the standard electronic roles-based security processes that are in place.

MR. MAPES: Then the other question has to do with the authorization, the initial identification of those that can prescribe. Is that tied to the credentialing process, for example, the state license or the DEA registration so if they lose their state license or lose their DEA registration, they can no longer prescribe using the electronic system?

MR. RATLIFF: You are going to hear from some of the prescriber/vendors, I believe, tomorrow. I would definitely ask them that question. That would be more relevant to the processes that they utilize and, again, they all use a variety of processes to help ensure from a contracting perspective and authentication perspective that the end user is a licensed practitioner.

From our perspective, we are contracted with the software vendor providing a solution to the physician and we do require, No. 1, that they have contracted appropriately and authenticated the user that they are a licensed prescriber. So, that is No. 1. Then No. 2, they do register that physician in our network, as we described, and we do validate that against the current DEA database to ensure valid DEA numbers and other credentials.

But the actual cutting them off of the network if they have been -- if they are having some type of an issue in a given state, that is typically happening on the physician vendor end.

MR. GINGRICH: I was just going to say, again, we are actually certifying against the same exact vendors. So, it -- just to put an exclamation mark on, I think that is definitely appropriate question to talk to the technology vendors about their processes around credentialing.

MR. POSNACK: This is Steve Posnack. I think we all agree that there are technical solutions out there that can be used. Do you see a time difference in the business processes or work flows associated with prescribing controlled substances versus not controlled?

MR. RATLIFF: What do you mean by time difference?

MR. POSNACK: So, for a normal prescription for a non-controlled substance, a provider would have to go through different authentication or authorization methodologies to prescribe that controlled substance or is -- you know, right now that is happening, you know, on the paper-based side. When they go electronic, is it going to take more time to do so through the system?

MR. RATLIFF: Well, the amount of time that it would take to write a prescription for a controlled substance versus a non-controlled substance, if you do it with systems are they are today, it would be identical, right? However, if you had an incremental level of authentication that is required, it would definitely depend upon what that level of authentication is, whether it is a key fob or whether it is a phone call or whether -- you know, there are a number of ideas that are offered up. Some of those are not only time-related issues for physicians that are constrained from a time standpoint, but the cost and standards, interoperability related.

MR. POSNACK: I mean, I understand that completely. Will there be a difference in the security related to prescribing -- is there going to be one solution for everything after controlled substances go electronic or is there still going to be a difference between prescribing a non-controlled substance and a controlled? Do you see that or do you think that everyone will just go towards the highest level of security?

MR. RATLIFF: Oh, I see. Again, that is kind of dependent upon the direction from the DEA, I guess. The concern is, though, in order to drive adoption and utilization, this has to be a system that is -- we have to be able to provide a system that is very reliable, is very fast and, again, it has got to be secure. But if it is going to require me to write prescriptions for controlled substances differently than I write prescriptions for non-controlled substances, that is one thing. If it is going to cost me more money, that is another thing.

If it is going to create interoperability issues with other things I do in the practice, that is yet another thing. So, if it adds those kinds of complexities, then what will either happen is everyone will try to go to, you know, to the most stringent requirements and deliver solutions in that way so that there is consistency. The problem is we will have costs associated with that. We will introduce new barriers and we will actually decrease the level of adoption and utilization of electronic prescribing, at least in our opinion, in my opinion.

MR. BRUCK: This is Steve Bruck. I just have a comment on that.

My guess, my idea would be that you answer that in the context of the e-prescribing vendors. Going back to your Part A, which would be, as I understood the question, is this going to take longer? Is it going to increase the amount of time it takes a practitioner to write a prescription? I guess, you know, the thing that kind of catches my attention is the fact that some of these vendors are not only providing solutions that work on desk top computers, but they are also providing solutions that work on a hand-held and isn't it interesting to maybe think about a smart card in a hand-held kind of merging into one device.

So, if you agree with that, then you might come to the conclusion that maybe it won't take longer.

MR. BARBER: My name is Linden Barber. I am with the Office of Chief Counsel for DEA. I am not sure if this question is better directed toward the vendor panel tomorrow, but I would like to hear particularly from the three gentlemen that spoke toward the end about the potential for alteration of the prescription information after receipt by the pharmacy detectability with or without relying on audit trails and whether or not that has anything to do with the network systems that you have talked about.

MR. GINGRICH: I guess I will just answer quickly. The audit trail is the key, I guess, in our mind. Being able to maintain that not just at the pharmacy end, but also as Rick mentioned when he talked, being able to tie back the audit trail all the way back to the prescribing end. And having the record all the way back at the physician's prescribing system is definitely a very important part of being able to provide a nonrepudiatable access to the transaction or view of the transaction. So, I think that is --

MR. RATLIFF: Is the question related to the changing of the prescription in the -- once it has made the pharmacy, that --

MR. BARBER: Right. And that is why I caveated it. It may be better asked of the vendors tomorrow, but my question is, it could be electronic record be altered and if altered, after receipt at the pharmacy, what is the method given the current system for detectability of that either by the pharmacist or by state or federal regulators, who have oversight over the electronic prescription.

MR. RATLIFF: Again, the auditing is really critical. But if I am following the question, the key from an audit perspective is to ensure, which I think is part of your question, is it saved correctly at the physician end, as an example and then cannot be changed. Right? And then is it saved in the network and then it cannot be changed and if it is, can that be recognized if we go back through an audit process. I don't know if that is the question or not because once it does arrive to the pharmacy, in today's world, as an example, if the prescription as an example dispensed -- does not have a designation of dispensed as written, then the prescription could actually be changed to generic if the brand was prescribed right. So, there can be a change in the prescription at the pharmacy level and then you could track that back through the network.

MS. DODSON: I think you would be getting an undetected change. So, one where maybe somebody just decided instead of prescribing 30, I will say that the prescription shows 60 and I will pocket the 30. So, that kind of integrity, I think --

MR. RATLIFF: When the prescription actually arrives in the pharmacy, it is stored, right? Then it is displayed to the pharmacist and then the pharmacist can manage that prescription typically within their own guidelines electronically. Some of the restrictions in that to your point are oriented towards those vendors or the chains in these cases, in some cases that write their own software and how they manage the actual storage and presentation and final storage of a prescription as they perceived it.

We can definitely store the prescription in our network. So, how it was received in our system and how it was transmitted and then we -- as we store that, we can actually show, based on certain kinds of technologies, whether it has been -- what we received has been tampered with.

MR. DONFRIED: Let me also comment on that, if I could. The short answer to your question from the SAFE perspective is yes, it is absolutely possible using modern cryptographic techniques to create self-describing stand-alone evidence that on its own, independent of the systems that created or manipulated it and independent of the accessibility of any audit logs or audit files is self-describing, can be successfully verified and validated at any time post the transaction.

From our perspective, that is an absolutely critical element of meeting long term record retention requirements and maintaining legally enforceable evidence over those long periods of time. To give a bit of context there, while the record retention requirements for controlled substances are two years, in the medicine development industry, record retention requirements are life of the compound on the market plus typically a minimum of 20 years.

So, the problem we have had to address at SAFE is how do you create stand-alone, self-describing evidence that is able to maintain its legal veracity and integrity over a period of a hundred years. That is a particular challenging problem, given that we haven't had IT systems for even half that time.

One of the assumptions you have to make is whatever standards you used to describe your data today will likely not be available at some point in the future. So, you also have an 8 track tape problem. If I create evidence that I want to be legally enforceable 20 years from now, it is not a very good assumption to suggest that XML or PDF remain as viable representation mechanisms.

But the short answer to your question is yes, it is absolutely possible. The open source technology I mentioned, USSI, does that today. At the time of signing, using a trusted third party with trusted time and compliance with the NIST specs, it creates notarized self-describing evidence that on its own can provide legal enforceability.

MR. CAVERLY: We could probably address this topic for the rest of the afternoon. However, we have come to the end of our allotted time. So, we are going to take a break for lunch. I have approximately a quarter to 12:00. Let's break for lunch for one hour. We will be back here at a quarter to 1:00 and we will be looking at that time at the practitioner perspective.

Again, panelists, thank you very much.

[Whereupon, at 11:45 a.m., the meeting was recessed, to reconvene at 12:50 p.m., the same day, Tuesday, July 11, 2006.]

AFTERNOON SESSION [12:50 p.m.]

MR. CAVERLY: We have a lot of ground to cover. This afternoon, we have two panels, the practitioner panel, as well as the pharmacy panel. Because of the number of panelists on each and the time limitations within the structure of this meeting, we just ask that the panelists try to stay within their 15 minutes. We don't want to stifle conversation, but neither do we want to take rooms out at the Marriott this evening.

Agenda Item: Practitioner Perspectives Panel

Let me go ahead and introduce then our panelists for the practitioner perspectives. As was mentioned earlier, there are only 11 percent of those prescriptions issued per year, which are controlled substance prescriptions, but 90 percent of practitioners retain a DEA number. So, let me go ahead and introduce those panelists.

Mureen Allen, a senior associate with Informatics and Practice Improvement, the American College of Physicians.

Anita Everett, who is a senior medical advisor for HHS Substance Abuse and Mental Health Services Administration.

John Huffman, who I think is the gentleman who is on his way, is with Holy Cross Pain Management, the American Society of Anesthesiologists.

Robert Tennant is a senior policy advisor, government relations, Medical Group Management Association.

And Alan Zuckerman is on the Council on Clinical Information Technology, the American Academy of Pediatrics, Primary Care Informatics Program Director at Georgetown University.

So, thank you, distinguished panelists. Let's go ahead and begin.

DR. ALLEN: Good afternoon, everyone. My name is Mureen Allen and I am here from the American College of Physicians, here to present the physicians perspective on electronic prescribing of controlled substances.

I would like to take this opportunity to thank the Drug Enforcement Administration's Office of Diversion Control and the Department of Health and Human Services for inviting us to provide comments today. I would like to provide just a short background about the American College of Physicians. We are the largest specialty organization representing over 120,000 physicians of internal medicine and medical students.

As you can see here, 41 percent of our membership are in practices where there are five or less providers and approximately 20 percent are in solo practice. So, we have a very keen interest in health information technology and production because many of our members are in very small practices, where it sometimes can be very difficult for them to adopt.

Recently, in 2005, we conducted a study and we found that 35 percent of our members work in settings where they have electronic health record systems that are used directly for patient care. We also found that that number decreased when you looked at practices where there are five or less providers in the ambulatory setting and only 20 percent of them were using electronic health records.

Now, of those who had computer systems, 90 percent of them were using them to write prescriptions specifically electronically and 13 percent of them were using them to communicate with a pharmacy. Again, these are numbers for those who have systems but when you looked at practices that were smaller then these numbers decreased. However, overall, these numbers are consistent with the national average, which I am told is about 18 percent of practices are using some sort of electronic prescribing system.

So, as you heard this morning, those of you who are here, physicians are very busy writing prescriptions. They are writing 3 billion prescriptions annually and it is estimated that if there is universal adoption of the electronic prescribing systems, we can save approximately $20 billion based upon reduction in adverse drug events and better utilization of medications. Approximately 30 percent of those prescriptions annually also keep pharmacists busy as they have to call physicians to ask questions, to ask for clarifications and to ask for refills.

So, if we adopt electronic prescribing, we know that we are going to get significant benefits. So, again, we will have reduction in illegible handwriting, which most of us physicians suffer from as a chronic condition. We will be able to automate the process of checking for drug allergies and we will be able to improve patient safety and increase efficiency by implementing clinical decision support and alerts in the system.

That can also be accrued as well when you think about controlled substances. So, what are the major concerns with controlled substances? From a physician's perspective, we are concerned about the diversion of those prescriptions. We are also concerned about the potential for abuse, as we all are. But those will determine the kinds of system makes it very, very easy for them. Prescription pads get lost or are stolen. Medications are lost or stolen. Prescriptions themselves can be altered by those who want to and there are people out there who will obtain DEA numbers fraudulently and use them.

So, our concerns with controlled substances are that for us it tends to be a burden when you are thinking about paper systems. We have to have special prescription pads. We have to maintain accurate and detailed records. We have to have a high index of suspicion that someone in front of us wants the prescription because they are abusing medications. But for those physicians who legitimately and routinely prescribe controlled substances for clinic use, they sometimes can be under suspicion and that is a concern for us as well.

So, why would we think about -- prescribing controlled substances, for those patients specifically on chronic controlled substances, this will make it easier for them to be monitored and managed so that they can receive their prescriptions in a timely manner and also be able to fill those prescriptions a lot more quickly.

For physicians, it will be a significant reduction in the paperwork burden to prescribe these medications. It will result in a reduction in the amount of prescriptions that are forged or stolen, less ability for DEA numbers to be stolen and used if it is done as an electronic prescription and more potential for physicians to accurately monitor the use of medications and to ensure compliance with therapy.

Essentially, if we have a closed system for prescribing where the physician writes a prescription electronically and sends it to a pharmacy, we can cut out a whole host of problems with abuse -- and fraud. So, what should an electronic prescriber system look like?

Well, our perspective, we think that the system used to prescribe controlled substances should incorporate the existent technologies and should not involve extensive and expensive -- remember, approximately 40 percent of our physicians are in small offices, where if they have already adopted this technology, asking them to implement greater technology burdens or increased financial burdens will drive down the adoption of this technology.

We think that whatever system you choose, there should be some sort of role-based authentication so the system should be able to query or should know are you a provider, are you allowed to prescribe controlled substances? Do you have a DEA number and if you are allowed to prescribe, at what schedule level?

In addition, there should be some sort of authentication. I am told by the experts today that most systems have adequate methods to authorize and authenticate the -- writers who are writing these prescriptions. However, if there is a need for an additional challenge, then we have told that digital signatures will ensure appropriate authentication. There should be methods to ensure the integrity of the scripts. So, once it is written by the provider, there should be some method to check that this was the prescription that was written and sent. So, we have been told that the prescription and storing copies locally and remotely can ensure this and also maintaining audit trails of who has accessed the prescription, who wrote it and where did it get sent.

Again, there is the issue of nonrepudiation and we are told that the current system does allow for that, but digital signatures are at a higher degree of security. A tricky issue that has been debated and with technology is the whole notion of privacy and security of patient information and that would be something that will have to be discussed, I guess, by those who deal with the legal issues as to what information can be released. We feel that if you use secure socket-layered transmission encryption, VPNs, you can keep that prescription secure so that others can't hack into your system or listen on the system to acquire that patient information.

The other thing that we think the system should do is to provide a fill status or a cancellation status notification to the provider. In fact, the more I think about it, it probably should be a two-way system so if a prescription is written electronically, sent to the pharmacist, then there should be a notification sent back to the provider that this prescription has been filled so that those who would like to get a second prescription, that potential will be reduced by having some sort of two-way notification on both ends.

The other area I would like to bring up for consideration is the notion of state level monitoring. I have worked in my previous life when I was in active practice in a state where we had state monitoring and it made it a lot easier for me when I wrote prescriptions. So, these systems do allow you to check for the potential for doctor shopping. They allow you to determine if there are unusually large amounts of prescriptions that have been prescribed and that the patient has made multiple requests.

If you do consider some sort of electronic prescribing system for controlled substances, I would argue that there is a role to have these systems integrated so those states that are already monitoring can also have a two-way flow of information to determine if there are excessive prescriptions that have been prescribed electronically and detect any sort of potential for diversion or abuse.

So, the key points I would like to make today that I think you should think about is, you know, we support the role of electronic prescribing for all prescriptions. We think that having a system where prescribers use system for one set of prescriptions and another system for another set of prescriptions, for example, the controlled substances is really untenable and would drive down the adoption of technology.

We feel that using the system to prescribe all medications, including controlled substances will allow physicians to accurately more ensure these controlled substances and ensure compliance so that patients who wish to get medications of multiple providers will have notification, will be able to check, will be able to tell me what is going on, especially if it is integrated with the state programs.

If the current system is deemed not to be suitable for the determination of nonrepudiation, we do accept that there is a possibility for the use of digital signatures. If this addition of technology does not result in increased financial and technical burden to physicians who have already adopted a technology.

We also ask that whatever you consider, be consistent with the current Medicare Modernization Act language and the current e-prescribing final rules where there is federal preemption of American state rules for current -- sorry -- state rules for controlled substances so that there is an overarching umbrella that will be in place that will allow prescriptions to prescribe freely electronically, without necessarily going -- contradicting the current state regulations.

We ask that you consider incremental change so to the extent that there are current systems that are already doing electronic prescribing and to the extent that we have been told that they are sufficient, that if you want to add beyond that level, that that be incremental.

We also ask that you consider if you haven't done so already to consider conducting pilots to see how this will impact physicians, especially those physicians who are in small medical offices. I think we all have the same goal. We all want to have a functional health information technology system that delivers quality improvement and patient care. To that end, we ask that you do not raise the bar to technology adoption and consider incremental change.

We also ask that you consider the current system and we are told that is sufficient but recognize that there may be additional needs for addition to the technology -- and that you make that change so it doesn't add a greater technical burden or financial burden to the provider and we also feel that at this stage more study is needed to determine how the technology works for controlled substances.

Thank you for listening to my presentation.

[Applause.]

DR. EVERETT: Thank you. As was mentioned, I am Anita Everett. I am a psychiatrist and I also work as a senior medical advisor within one of the other agencies, but within the HHS family of agencies, the Substance Abuse and Mental Health Services Administration or SAMHSA.

So, I come to you in two capacities. One is as an individual who works as a bureaucrat in the Federal Government. I won't say I am a fed because I am actually technically under contract, which enables me one day a week just to work as a community mental health or community psychiatrist in a clinical setting. So, I am an actual clinician, who works in the federal bureaucracy, as it were.

I want to thank you very much to the Drug Enforcement Agency, as well as my friends at the Center for Medicare and Medicaid Services for inviting me to come and talk with you today.

I thought I would present a bit of information from the latest SAMHSA National Survey on Drug Use and Health that relates to prescription drug abuses, as well as a few ideas from the perspective of a clinician. So, prescription drug abuse is on the rise. I think we are all aware of that generally. It has been covered in a lot of things in the media.

Our most recent -- SAMHSA is the federal agency that administers the survey that is called the National Survey on Drug Use and Health, which was formerly known as the Household Survey. It is now called NSDUH. In the most recent results of our survey, 2.4 million persons, age 12 or older, were new initiates of non-medical use of prescription pain relievers. That is almost 1 percent of our entire population that has had non-medical use in some sort of pattern of prescription drug abuse.

So, it is very much on the rise. Over half of these new initiates were females, which might reflect a slightly changing demographics in the style of what we are usually used to thinking of as the typical sort of drug abuse population. Of the medicines or the pain medicines that were used, 48 percent new initiates used Vicodin, LorTab or Lorcet. Thirty-four percent used Darvocet, Darvon or Tylenol; 20 percent Percocet, Percodan or Tylox and 18 percent generic hydrocodone and then from there, lesser amounts. This is also becoming an increasing problem in the teenage population.

A recent study from Columbia revealed that the prescription drug misuse of prescription drug use rose 212 percent between the decade 1992 to 2003. So, it is becoming a problem sort of all over. Law enforcement, as we know, is becoming progressively involved in this, both at the federal level, as well as at the state and local government level. It has become much more prominent in the daily workings of particularly local law enforcement entities.

About half of our states now have prescription monitoring systems and a piece of our agency, the Substance

Abuse Treatment Section of our agency works very closely with these state monitoring systems as they are emerging. I know that will be covered tomorrow in a different panel in a lot more detail.

The proliferation of pain clinics has also become a bit of an issue for us, as we become concerned about national issues with regards to shifts in population and use of prescription drug use. Pain clinics, our information tells us that 10 to 20 percent of those receiving services from pain management clinics go on to develop some sort of problem. This is new information since the pain clinics have proliferated and we will have someone that is going to speak a little bit more about that.

We don't worry so much use in the context of the pain management clinics because we know most of those staff are very well-schooled in the management of these kinds of issues. It is when they leave the pain clinics and go to other care that there is less sophistication in the way that access to medications is worked with. So, that has become an issue for us in a number of our surveys.

So, those are sort of the things from the SAMHSA perspective that I wanted to talk about. I did have a few issues that I wanted to sort of make sure are on the table with regards to the perspective of a clinician. I know this morning there was discussion and presentations of some of the technologies, but I wanted us to think why is it that we can have FedEx, you know, we can have systems that contract by the minute practically, packaging that goes from one little town in rural southern California to Maine, we can know exactly where the package is at any given minute of the time, but we can't know the same kind of information about prescriptions. Actually, of course, we can know that information. We just don't. A good number of our physician workforce doesn't use electronic methods for writing prescriptions, despite a lot of compelling reasons for that, which, of course, is why CMS and DEA are -- why we are here today is to talk a little bit about that.

Physicians are trained to be cautious and American physicians are trained to be highly autonomous. That has become particularly compelling to me as I have worked through my role in the Federal Government with a number of other physicians from different countries. Today at SAMHSA we have a physician working with us from the U.K. system and he is talking about how they are working with electronic prescriptions there. It is a little bit different when you have physicians who are much used to working in a system of care.

We want to integrate our scientific -- we have physicians, American physicians, who want to integrate our scientific understanding of best practice with our individual patient's needs and presentations to tailor the best course of action for every individual patient. We are not a group who adapt well to bureaucracies and bureaucratic rules. It is a negative thing in physician communities to be a bureaucrat. There are resistance to rules and impositions from government. When a person comes in and complains of pain, physicians want to address that problem through a quick diagnosis and treatment.

We also all are aware of the compelling pressures on physician and practice management systems to move patients through systems relatively quickly. So, in order for this to be adopted by physician communities, in addition to being respectful of privacy, which, of course, is a big concern to those of us in the psychiatric community, there have to be systems in place that are user friendly and fast. Of particular interest would be something that enhances patient safety in terms of accuracy, as well as interactions and information about quick access to potential interactions, enhanced patient safety in terms of quantity access and as well as access to medications. As a psychiatrist, we think about who has access to what kinds of medications with regards to overdose potential and danger in that regard.

A final thing that I wanted to comment just a little bit about that I wanted to make sure from the perspective of a physician was on -- was, again on the table in this dialogue as we think about impact on physician communities and the greater good and myself, as well as SAMHSA is very much in favor of the entire move toward electronic prescribing for a number of different reasons that have been and will be talked about. However, we don't want to set up systems that put our practitioners in jeopardy. In preparation for coming today, I reviewed some things in the current media and ran across an article from Campbell County, Tennessee. The sheriff's office in this particular county said that 90 percent of their inmates in the Campbell County Jail are there for using or selling pain pills.

This is not a scientific survey, but 90 percent is a pretty high number. The majority of people selling them have their own prescriptions. On the street, 1 hydrocodone may be as valuable as $10 apiece. One of the inmates in this particular interview stated that addicts will take extreme measures that often land them behind bars. They are willing to break into drugstores. They are willing to rob people. In some cases they are willing to murder for drugs because of their addiction.

So, thinking about the life of the addict and the condition of the addict, we do have to remember, it is a pretty intense physiologic addiction that can change individual's personalities in the way they function. So, what does that background do for physicians, particularly American physicians, who really crave autonomy and want to be on their own and not be told -- not be regulated, so to speak. How can we protect physicians from threats is what I am trying to sort of understand and make sure is on the table. Addicts know about the tradition of autonomy and American physicians and do work to try and exploit this.

A friend of mine from Iraq recently told me of an incident that he was very ethically disturbed by. An individual came into his office one day that had been a patient of his. Actually, he was the mother's physician, but he knew the individual. He also knew him as an addict. He walked into the office with a grenade and said that he was going to pull the pin right there in the office unless this physician wrote him several prescriptions for a hundred each of hydrocodone.

That kind of thing is a little bit dramatic for us now in the States. However, it is not unfeasible that we would have physicians in harm's way, particularly if we arm them with new information and they are now expected to know that three other doctors are writing the same prescriptions, creating mechanisms that will help to protect the physicians so they can comfortably say, no, we can't do that as a very important part of that. But it is my understanding that many of the state programs that do have prescription monitoring haven't been in place long enough to fully address that, at least on a national sort of level.

So, that is something that I think we would want to just consider from that perspective. So, in summary, I have some information -- you know, at SAMHSA, we do monitor and follow on the national level, use of prescription drug -- I have used prescription drugs. It is becoming very much an issue for us and something that we are very concerned about, developing systems that can help us track and monitor and manage that more effectively is something that we are very supportive of.

Thank you very much.

[Applause.]

MR. CAVERLY: Let me just check and see if Dr. Huffman has been able to join us. Okay. In his absence then we will go on to Robert Tennant, senior policy advisor, Medical Group Management Association.

MR. TENNANT: It is a pleasure to be here. I am Rob Tennant with the Medical Group Management Association. MGMA was founded in 1926. It is the nation's principal voice for medical group practice. Our 20,000 members manage and lead 12,000 organizations in which about 242,000 physicians practice medicine. We are very supportive of health information technology in general and we believe that moving the nation's medical practices to electronic prescribing, one that includes controlled substances will greatly improve patient care and significantly streamline administrative processes.

I would like to focus my discussion on four main areas: the current use of paper prescriptions, the clinical and administrative benefits to e-prescribing, discuss some of the security issues that relate to controlled substances and conclude with a few recommendations on how to move ahead. Paper prescriptions are still the most widely used method of prescribing, most typically the method used for prescribing controlled substances. Many clinicians rely on paper prescriptions because they are a simple and fast method.

Issues with deciphering illegible handwriting continued to plague the medical profession, though. In most care settings preventing prescribing errors is dependent on a system of downstream inspection, usually by the dispensing pharmacist. While pharmacists are remarkably good at catching these errors, they make more than 150 million calls to physicians each year to discuss possible errors or otherwise clarify prescriptions. Many errors still continue to slip through the safety net.

In their landmark 2003 study, the value of computerized provider order entry in ambulatory settings, the Center for Information Technology Leadership suggested that more than 8.8 million adverse drug events occur each year in ambulatory care, of which over 3 million are preventable. CITL also estimates that nationwide adoption of electronic prescribing will eliminate nearly 2.1 ADEs per year here in the United States.

This would prevent nearly 1.3 million provider visits, more than 190,000 hospitalizations and more than 136 life threatening ADEs. Of course, medication information conveyed via a paper prescription is not automatically stored. It must be reentered by hand in the pharmacy system and is not recorded efficiently in the clinician's office. Paper itself is more expensive. It is expensive to move and it is expensive to store.

Use of handwritten prescriptions also brings up security issues as paper prescriptions are relatively easy to forge and steal. Of particular concern for controlled substances is altering of the prescription sig. It is all too easy to change one refill to ten with almost no way for the clinician or pharmacist to know.

In addition, physical security of the prescription pads is a constant concern for practices. Unfortunately, many break-ins of practices and clinics, especially in urban areas are done specifically to acquire these pads.

So, let me turn and talk about the benefits of electronic prescribing. Of the many benefits, the most important perhaps is enhanced patient safety. Safety is increased through the legibility and accuracy of the prescription, as compared to handwritten notes, as well. When you incorporate drug formularies, you can check interactions, contraindications at the time that the prescription is written.

No more lost paper scripts that are never filled. One study suggested over one-third of all prescriptions are never filled. That means the patient is not getting the care that the physician ordered. From the administrative perspective, you can also improve quality, efficiency and reduced costs by actively promoting appropriate drug use and providing formulary information in regards to alternatives and co-pays, reduction in the number of phone calls required, provide instant connectivity between providers, pharmacies, health plans and PBMs.

Systems that practices use now are very small and portable. In fact, for many practices, it is their first foray into health information technology. Automated prescription renewals can reduce clinical and administrative time for pharmacists and for physicians and eliminate call-backs due to bad handwriting, generic checking or formulary problems. From a cost saving perspective, e-prescribing allows practices to handle refills faster with estimated reductions of 12 minutes per refill, from 15 minutes using paper to three minutes using e-prescribing and reduced time when e-prescriptions are faxed instead of using the phone, from six minutes per call to less than one minute per fax.

One of the most exciting benefits of e-prescribing comes from its integration with practice with the practice's electronic health record. Robust systems allow physicians to check the medication against other medications that the patient is taking, along with other allergies the patient might have. In addition, these integrated systems allow documentation and storage of all prescriptions and access by all authorized clinicians.

For the health plan, e-prescribing can reduce costs due to accurate prescribing and decreased chances of medical errors, reduced costs due to increased adherence to preferred drug lists, reduced internal administrative costs and, in fact, may serve as an advantage to both subscribers and employers.

Thanks to the Medicare Modernization Act and the HHS final rule, we now have an excellent set of foundation standards for e-prescribing. However, one standard was not included in the first set of foundation standards that should prove to be a very valuable security tool for the e-prescribing of controlled substances. The fill status notification transaction permits pharmacies to send a message to the clinician when the prescription has been filled. This will allow clinicians to monitor the dispensing of controlled substances to guard against security breaches that led to unauthorized fills.

As the paper prescription pad and the clinician's signature must be kept secure, the access to electronic prescribing part of the electronic health record must be kept secure as well. I contend that the combination of the existing HIPAA security and privacy regulations, along with several additional provisions could ensure that controlled substances are e-prescribed safely and securely. We all know that the final security tells covered entities to ensure that the confidentiality, integrity and availability of all EPHI must be protected. We must protect against any reasonably anticipated threats or hazards. We must protect against any reasonably anticipated uses or disclosures and we must ensure compliance by our workforce.

In terms of technical safeguards, covered entities must implement policies and procedures for access control on systems that maintain EPHI. To ensure transmission security of controlled substance, we recommend examining whether two currently addressable specifications should now be required. Integrity controls, security measures to ensure that electronically transmitted PHI is not improperly modified and encryption of e-prescribing data. Data integrity can be ensured through appropriate policies and procedures and data integrity must also contain person or entity authentication, which requires the covered entity to implement procedures that verify that a person or entity seeking access to the EPHI is the one claimed to be doing so.

I want to talk about the digital signatures a little bit. It is obviously a very key implementation feature for e-prescribing. When digital signatures are employed, three features should be implemented -- integrity, nonrepudiation and user authentication. You can also have continuity of signature capability, ability to accept electronic counter signatures, independent verifiability of electronic signature and -- integrity.

Obtaining a digital signature certification using public key infrastructure may prove to be a good approach as well. PKI can certify encrypted data that contains prescription information. Clinicians would be required to guard against unauthorized access to this private key. Once the data is decrypted, the pharmacy would be assured that the prescription has come from the legitimate source. The use of PKI establishes a high level of trust among users.

Any e-prescribing system must have at its core control over access rights. A strong argument can be made that once the prescription leaves the practice, security can be maintained quite easily. The critical issue for practices employing this technology is to secure access to their system. The electronic prescribing application that they use in the practice must have the ability to access the patient's record, handle secondary access roles and -- limit independent prescribing or prescribe with co-sign privileges.

Access to the e-prescribing system is only granted to those that have permission and access to controls such as passwords must be in place. The requirement to protect confidential information is clearly more critical than ever. Augmenting the HIPAA security rule appears to be the best approach to achieving what all stakeholders require, safe, secure and streamlined e-prescribing.

In conclusion, while MGMA is confident that electronic prescribing will improve clinical performance and ease administrative burdens, there are clear roadblocks ahead of us. Revising the HIPAA security rule, developing the fill notification transaction standard, expanding provider education on a -- security measures and instituting pilots, as well as harmonizing the many state laws governing e-prescribing should all be considered.

It is important to remember, though, that health information technology is costly and the majority of this cost is borne by physician practices. We encourage the Federal Government to take into account the cost and burden of e-prescribing when developing rules related to controlled substances. The HIPAA security final rule itself is an excellent model for how regulations could be crafted, allowing considerable flexibility for covered entities in terms of how to comply while ensuring the security would appear to be the best approach.

We appreciate your interest in this important topic and thank you for inviting us to present our views.

[Applause.]

DR. ZUCKERMAN: Good afternoon. I am Alan Zuckerman, representing the American Academy of Pediatrics and I, too, want to express our special thanks to both DEA and to HHS for finally bringing about this extremely important meeting. I have been asking for such a meeting in many settings for many years now for NCVHS hearings, at the AHIC or community meetings and in the history of developing the NHIN and I think this is a landmark meeting that, hopefully, will lead to important progress in this most important area.

The American Academy of Pediatrics represents 60,000 primary care pediatricians, pediatric medical specialists and pediatric surgical specialists, who are dedicated to the health, safety and well-being of infants, children, adolescents and young adults. We submitted a statement on electronic prescribing controlled substances, have a large number of copies of that statement, as well as copies of my slides. So, those of you who are interested can read our full statement and give me more freedom to speak to some of the issues.

AAP cares about EPCS because of the importance of electronic prescribing of controlled substances to children with attention deficit disorder, who are on chronic stimulant medications. This for us is about the prescribing of Ritalin and not Oxycontin. We have a lot of very good longitudinal data. The children who are supposed to be on chronic medications do not do as well in maintaining their medications if they see a pediatrician two or three times a year, than if they see a psychiatrist once a month. The hassles of wet signatures on paper not being able to use fax or phone contacts creates a tremendous fall-off rate in the rate of use of medications and tremendous hardship to families, who are often dealing with multiple children with different problems.

It also affects children on some anti-convulsant medications and other situations where we want to maintain continuity of the prescription medication. We also care very much about electronic prescribing in general and feel that this is going to be an extremely important pathway to improving patient safety and quality. We want to reduce the barriers to the use of health information technology and practice and many of our members are, indeed, in small practice and compared to other specialties have even lower rates of adoption of e-prescribing, perhaps only 15 percent and adoption of electronic health records that is certainly below 20 percent among those caring for children.

Like other professional societies, we have become active in a variety of standards development, other activities, sending representatives to HL-7 and ASTM, participating in certification commission and Health Information Technology Standards Panel that you heard about this morning. I spend about a third of my time in academic pediatric practice across the river at Georgetown, but I am also one of the few physician members of NCPDP, who doesn't actually work full time for a vendor. And I have been a member of the Interoperability Working Group at CCHIT and also the Consumer Empowerment Technical Committee at HITSP.

Just as a quick overview of what the issues are as I see them. There is an urgent need for us to enable electronic prescribing of controlled substances, not just for its own sake, but to drive the general adoption of electronic prescribing for all prescriptions and all medications. In order to get there, we need to have some appreciation of the kinds of security measures and costs that physicians are going to tolerate to get EPCS because it is a tradeoff and they always have a quick and easy fallback to paper and in electronic prescribing, there is a tremendous misalignment of the benefits with the physicians expected to invest and pay the cost, but others achieving the benefits of preventing these adverse reactions.

I will speak somewhat about the attractiveness of the smart cards and PKI technology that you have heard about, but also try to point out some of the unanswered questions and problems in trying to use this on a large scale with physicians in the real world. I want to introduce the notion of comparing provider level PKI with vendor level PKI as a way to gradually move towards introducing these sophisticated security technologies to physicians. I think there has been a tremendous amount of change in PKI technology and much of the demonization of PKI may no longer hold as much truth as it did in the past.

We do have methods now to make DEA registration and the use of PKI much easier than it would have been five years ago. It is important to consider the linkages to the emerging nationwide health information network and see how these two activities can move forward hand in hand and as part of that, we want to present a five year phase road map for gradually moving towards some of the PKI technologies you heard about this morning.

With regard to the urgent need for electronic prescribing for controlled substances, without a doubt the greatest risk of electronic prescribing is that people are not going to use it. As you have heard from the previous speakers and as there is ample published literature, the benefits of electronic prescribing, both in terms of workflow into patients and in patient safety and quality are enormous, especially when it is used in the context of clinical cessation support and in pediatrics there are areas of per body weight dosage calculations and other things, where electronic prescribing has enormous value in identifying more information about medications.

Not having electronic prescribing controlled substances is a hardship to physicians who are already using electronic prescribing and have begun to appreciate its value, but even more importantly, not having electronic prescribing as a barrier, particularly in specialties like pediatrics, psychiatry and anesthesia where there is a higher usage of controlled substances. It is a barrier to getting more physicians to use electronic prescribing for everyone.

Patients are in effect being deprived of important quality and safety benefits that can occur, particularly when decision support and integration to electronic health record is possible. The risks of fraud and abuse are certainly in our opinion much greater in the paper systems today they are in electronic prescribing today. But there is no question that once electronic prescribing is in place, that is going to change over time as incentives become greater.

Two of the two-way transactions that were mentioned before, the prescription fill, which is not in widespread use today is similar to closing the order's loop for lab tests, where when you write a prescription, you want to know if it was filled, just as when you order a test, you want to know if you got the results back. Medication history, ideally would give you a window on whether a patient was getting substances from multiple physicians. However, it is almost an assumption that patients, who are trying to divert controlled substances are not going to be doing so on insurance and are not going to use consistent patient identification. So, we probably won't get medication histories for diversion control, but we will get it to get a deeper appreciation of compliance with chronic medication.

Well, what are physicians willing to do to get electronic prescribing controlled substance. I tried informally to get some data on this and we clearly need some studies because physicians who have been using electronic prescribing for six months or more tell me that they are willing to tolerate additional costs, costs on the order of maybe 50 or 60 dollars every three years because they know how much time it will save. They know how inconvenient things are for them now.

But those physicians who aren't using electronic prescribing, cost is an absolute barrier to adoption. Even when insurance companies are willing to give them a PDA or cell phone, give them a prescribing service completely for free, you have trouble getting physicians to adopt and buy into electronic prescribing. Once they are there, the use picks up. In other countries, where physicians have been given financial incentives, they were able to progress very quickly from 15 percent use to 95 or 99 percent use.

I am told there are fewer than a hundred physicians in the United Kingdom who don't prescribe electronically. It is almost universal in Australia and New Zealand. The United States is really an exception among developed nations, using technology and not adopting electronic prescribing because we have pushed too much of the cost on the physician users.

The situation will change a little bit in May of 2007, when CCHIT begins to require electronic transmission of prescriptions from all certified ambulatory EHRs. Today, most of the prescribing is taking place on stand-alone e-prescribing systems. In the near future, it is going to be coming from electronic health record systems. Physicians simply don't want to have two separate systems, one for controlled substances, one for non-controlled substances.

They are willing to carry smart cards, particularly some of the new U.S.B. devices, but they are not willing to carry a dozen of these things. This is one given to me by my hospital that enables me to view x-rays and lab reports and other things on the web from home. It has room on it for several certificates so it could serve several purposes, but if I had to carry separate devices, it would be a problem for me to find the right one and be willing to use it.

Physicians in general aren't going to tolerate biometrics because of the time delay. There is simply too much pressure. Pediatricians are often seeing patients every 10, 12 or 15 minutes. You can't take two minutes to wait for a secure I.D. token to reset its changing password or to try to get an iris or fingerprint reader to work correctly. Electronic prescribing is very, very high volume and the security risks are not very obvious to the physicians. So, the tolerance for time delays just simply isn't there.

Physicians also get very upset about vendor lock. They don't want to be putting the physician where they are dependent on a single vendor for their smart card, for their readers, for certificates or anything else. We have to have competitive choices to get physicians to buy in. Of course, enrollment and identification must be made as quick and as easy as possible. The DEA has made outstanding progress in their web-based registration renewal, which really makes life easy for physicians and in part because they do such a good job on initial enrollment and checking, credentialing and certification the first time around.

Why do we need smart cards? What do they do for us? Well, as you heard this morning, PKI, this public/private key asymmetric encryption, adds three features to a simple electronic signature like a graphic or a symbol. It provides third party authentication of the signer and that extends also identification. This is a signature that you can read the name on. In my hospital, I have to both sign in a normal signature. Then I have got to print my name and even write in my pager number so they can figure out who actually signed something.

With PKI, you get it automatically. It checks the document or message integrity so that you know that the document in front of you is the one that was signed and hasn't been altered. It does that through calculating a message digest encrypted with the physician's private key and it provides for nonrepudiation, this non-denial of who signed things because one and only one person can carry that smart card and can have access to the private key. There is no way that you can give it away or duplicate it to other people if it is implemented properly.

If you are going to use PKI, there is almost no reason to compromise and take halfway measures. You have got to go all the way and make sure that the nonrepudiation comes with us. With these smart cards, the reason they are so intriguing and they, of course, come in a conventional credit card style that requires external readers, U.S.B. or an AGON(?) SD cards and there are the contactless cards like they use on the metro here, is the key pair is generated on the card. The encryption takes place on the card and that private key never leaves the card and if the card is in any way damaged to try to get data out, it becomes unusable.

This property of non-duplication of a single existing copy is really critical to the non-repudiation, getting physicians to take them seriously. If you are wearing an I.D. badge with the card built into it, you are less likely to lose it and you are more likely to always have it with you. They also can be revoked remotely if they are lost or stolen even by the user themselves and, of course, if there is any revocation of privileges to prescribe, this also can be implemented remotely.

Another fascinating use of PKI is to protect the DEA number. I personally have had office staff borrow my DEA number to feed substance abuse and we are in a constant confrontation with insurance companies about not wanting to release our DEA number without justification. In the normal signature process, use a private key to encrypt the message digest and a public key to read and verify the signature. You can do the reverse for the DEA number. You can encrypt it with the public key that everyone knows and then only the physician with their private key can unencrypt that DEA number and make it part of the controlled substance transaction.

That makes it easier to use the same certificate for both controlled and non-controlled substances and to use it for other authentication signature purposes where the DEA number simply isn't required. So, one payback to physicians of carrying smart cards is that they may finally have serious control over their DEA number and not need to disclose it unnecessarily.

But there are some unanswered questions. No one has really gone about enrolling huge numbers of physicians in a large scale PKI that spans multiple organizations. We do have a limited experience with the SAFE and BioPharma, where there is a lot of incentive when you are doing clinical trials and when there is a lot of reimbursement at stake. But we have never done this for lower end applications. CDC has about 500 of these out there for public health reporting. A few organizations have used it for filing claims, but you have got to remember there are like 800,000 DEA certificates and if we are going to scale something up to hundreds of thousands of people, we need to start slow. We need to prove it can be done on that large of scale.

It is also extremely hard to get physicians to understand what PKI is about and to use it responsibly. I consider it part of the basic science and medicine. I teach it to all my first year medical students. But it is really hard to get the message across and get people to work with it. Some of the PIN-based biometric signatures, other things, have a much greater intuitive notion. The cryptography of PKI and the value of the smart cards that look just like U.S.B. keys, just hasn't gotten through there.

Clearly, we are going to need face to face identification before we issue smart cards and how we are going to do this for hundreds of thousands of people, whether we can use hospital credentialing offices or even send people to motor vehicle authority or what are we going to do? It is simply not something you can do over the Internet sitting at a terminal.

Someone has got to do photo I.D. checks and we have got to make it fast and easy. Clearly, web access, both for enrollment use is going to be important. As we move to more EHRs, we have the problem that many people are using ASPs. Some of them are using the Citrix main frame approach that may or may not be compatible. As HIPAA security rules have been implemented, it is getting harder and harder to install middle ware or other devices on computers where you are.

When I am on call on a weekend, I may take 50 calls from parents and they are in the hospital seeing kids in the nursery or something, I get a call from an asthmatic, right now I can walk up to any hospital terminal. I can e-prescribe refills in. If I can't install the middle ware or there is no smart card reader for my smart card, I won't be able to do that in the future. That is why we may need to reserve the PKI only for controlled substances and why even there, it may take time to develop national standards so it is universally available in hospitals and offices, as well as at home.

Physicians are mobile. They do an awful lot of prescribing on cell phone PDAs and other devices. Physicians also like user friendly technology. That is why the Macintosh and the Palm are so popular and we don't have really good demonstrated solutions that interoperate between Windows and Macintosh, between Windows, mobile pocket PCs and Palm devices. Physicians seems to lose and forget things all the time and it is unclear whether if there is too high a replacement cost, they will report loss promptly or they will simply stop using the technology.

One thing to make the technology easier to get going would be to move the PKI from the provider to the vendor. Basically, when we talk about PKI today -- anyway, the physician presents their smart card to their computer or laptop and that is where the signature action is going to take place that gives you the nonrepudiation.

From there, it is passed on to the EHR and then on to the pharmacy. In an alternate strategy, the smart card would reside right in the EHR or e-prescribing computer and the digital signature would apply only to the message that goes over the Internet to the pharmacy. Actually, people are also using smart cards today for -- authentication of their firewall or network interface, which provides another measure of knowing where the prescription has come from. What this means in practical terms is that if you do provider level PKI, every provider has to have their own smart card, but if it is the vendor level, you only need one smart card for the EHR system in the office or for a central e-prescribing or EHR system.

With provider level, each provider has to do their own DEA registration and PKI enrollment. With a vendor level, the vendors would have to DEA register, but they would enroll just once. For a provider, they need to present their smart card every time they sign a prescription and many of today's systems, like the one that I am using, we actually have a separate password for signing. So, you use one password to log onto the system. You have to remember a second password after you have finished writing your prescription. But in the vendor level system, the smart card stays in the system and as long as it is there, you can sign and send prescriptions on to the pharmacy.

Now, when you do have individual provider PKI, you get the benefits of a nonrepudiation and identification. In a vendor system, the current log-in procedures are unchanged, but if you are in a provider system, if you don't have your smart card with you, you can't write that controlled substance prescription or potentially any prescription at all. In the vendor system, the two factor authentication becomes optional and, in fact, one smart card can serve the needs of many different providers that are sharing services from a single vendor.

Let's look at some other things that can make PKI a little bit easier for physicians to use and accept because today it is almost a given assumption physicians simply won't do this. One trick would be to have physicians enroll only once every three years, the way they do today for their paper, DEA certificates. If you have one fee to cover the PKI enrollment and everyone paid the same fee, then you wouldn't have the incremental fee barrier, although you might require physicians to present a smart card. But the experience of large hospital systems is you almost have to give the smart cards to physicians to get them to buy in.

If you can use one smart card for several different hospitals and DEA registration in multiple states, it is going to make life easier and reduce the cost. And instant web enrollment is another highly attractive feature and it is almost worth the $20 to go out to GeoTrust and purchase an e-mail certificate that links your e-mail to your name just to see how easy this is to do. From a pull down list you select your smart card vendor. You put the smart card preferably with an integrated U.S.B. reader into your computer, sends a message, generates the key pair.

You fill in the certificate request. It goes out. The certificate comes back. It gets installed as soon as you pick up the phone and call the right number based on your e-mail to prove who you are. In just a very quick transaction, you have got a certificate loaded on your smart card and you are ready to go. You don't have to make multiple stops. You don't have to do other things.

The face-to-face identification could take place days or weeks later at an appropriate point with the certificate held in abeyance until identity checking was completed. Having multiple vendors and form factors like the SD cards for cell phone PDAs will be important and also limiting our demands on sophisticated cryptography also influences cost.

Now that RSA is no longer under patent, that is no longer a cost barrier, but if we go from a 1024 bit key to a 2048 bit, if we try to go from the SHA-1 message digest to an SHA-256 or 512, we may kick the price up ten or twenty dollars on each unit. We are dealing with potentially hundreds of thousands. We are going to have to scale our level of cryptography to the level of threat and risk. Of course, self installing web applications are going to be really important.

As Kelly Cronin said this morning, we really can't allow separate systems to develop in parallel for different purposes. If we are going to have a nationwide health information network, electronic prescribing controlled substances has to be part of it and, in effect, digital signature and authentication are going to be a requirement of any network that handles electronic documents. What we have today is kind of a chicken and egg business. Should the DEA with its outstanding credentialing capabilities become the enabler of the NHIN by providing identity and certificates of the NHIN or should the NHIN once developed become the enabler of electronic prescribing.

Today, we have many different vendors and switchers handling things. In the United Kingdom, they developed a separate parallel telecommunications infrastructure for their nationwide health information. We don't know what our NHIN will look like in its final form, but, hopefully, EPCS will be an important part of it and NCVHS has additional hearings on functionality coming up at the end of this month and hopefully will be able to get some of these features into it.

In conclusion, let me share with you some ideas about a road map that might take us to PKI in small steps that might achieve physician buy in, promote electronic prescribing and not subject us to undue risks. We could allow EPCS to begin today using the technology already in place for electronic prescribing, which many of the speakers have said is superior to what goes on with manual paper systems, but this would involve resolving state laws and many other conflicts.

Ross Martin of Pfizer had a wonderful idea at lunch today, where he said why don't we just print paper prescriptions, wet signed in parallel with the EPCS so that we are in compliance with existing laws. Physicians will have the patients carry the wet signed prescription and now we have got a bargaining chip with physicians to buy into PKI because in a few years if and when they convert to a full PKI and smart card, they then could stop printing the second paper copy. So, we get a little bit of the benefits of both worlds and we could get started extremely quickly, but there would still be real benefit to use the electronic prescribing for the controlled substances to get the electronic transmission to the pharmacies.

Within a year, we could probably put in place this vendor level PKI, have our EHR vendors and e-prescribing vendors register with the DEA and start putting smart cards and digital signatures on to the computer level system before things go out to the pharmacy and that gives us a permanent record in the pharmacy with a nonrepudiation signature, at least on behalf of the vendor.

Two years from now, if we make an early start, we could have completed some pilots of what physicians will actually accept and use, particularly in a small office environment. The AAP would be very eager to work with some technology partners and with some universities to get a real world test of PKI and its acceptability. Three years from now, we are going to have an outline of plans for the NHIN and even certification in place and if we start working now, we can harmonize what we do for EPCS with the NHIN so the physicians will have a single infrastructure for identity, not two separate systems growing up in parallel.

Regardless of what happens on the regulatory side, there are going to be physicians who will adopt best practices and who will want to use PKI digital signature and get the nonrepudiation. Four years from now we should have good national standards in place for at least optional use and have some method whereby the signatures are portable and the middle ware in readers are standardized throughout hospitals in this country.

As we learned this morning, one must constantly go back to reassess threats and risks because five years from now whatever we do on an interim basis today is going to change as the new threats arise from experience and level of use. Today, a few early adopters, a few thousand physicians won't create incentive. If we have hundreds of thousands of people doing this in four or five years, that is the time to come down with more definitive regulations once we get electronic prescribing in place.

Thank you very much.

[Applause.]

Again, copies of our statement and slides are up front.

MR. CAVERLY: Let me make one final call for Dr. Huffman.

Okay. Let's go on then to the question and answer portion of this presentation for practitioners. I will throw the first question to HHS again. We have been joined by some additional colleagues. So, as you ask the question, if you would please identify yourself.

MR. KELMAN: Jeff Kelman.

They often give me a dead mike. Jeff Kelman from CMS. By the way, Dr. McClelland sends his regards. They wanted to make sure that I reemphasized the high priority of electronic health and e-prescribing is in our agencies look forward over the next several years.

I have a question for Dr. Everett and Dr. Zuckerman and it was sort of covered, but to try to summarize it, in comparison with the current system, paper prescribing dispensing of controlled substances and of telephone prescribing and dispensing a controlled substances in the community and in institutions, what do you see as the risks or benefits in terms of diversion and abuse going to electronic systems?

DR. ZUCKERMAN: I think one of the most important things is some limitation on the delegation to others, that it becomes so much more difficult to impersonate a physician. Physicians will have to do themselves what might be done by staff in other settings. Of course, another property of PKI is you can use it to countersign somebody else's signature, but I think that the things which I have experienced many years in practice, patients adding zeroes to turn a 10 into a 100, people borrowing DEA numbers, people pretending to be a physician, patients presenting under different names to multiple physicians, even in the same practice and easily being able to leverage additional prescriptions that way.

I have never actually seen a prescription copied and taken to multiple pharmacies, but that is another concern, which can't happen in electronic prescribing because the transmission is instantaneous to a predetermined endpoint.

DR. EVERETT: I would agree. Many types of diversion would be limited by this kind of thing, the stealing of the prescription pads. things like that, breaking into offices would be less likely. The degree of sophistication that would be required to break into systems would make that virtually impossible, it sounds like.

There is still the likelihood -- and I will have to find out from our staff exactly what the numbers are, but there still is the likelihood that prescriptions that are written for an apparently legitimate reason could still be diverted. Doctor shopping might be lesser if we have a system set up so that doctors can see, oh, you have gotten five other prescriptions in the last two weeks from different -- five other physicians. But still the element of you give Gladys White a prescription for a hundred of something with three refills and she, in fact, gives it to her son, who sells it on the street. That kind of diversion will not -- you know, won't be directly addressed by this.

But the whole process may heighten awareness and help the physician community be more aware of these kinds of things and we are looking out for it.

I can find out numbers for you, though, Jeff, on it, of the diversion that happens, what part of it is that side of the thing versus the pre thing. That would be interesting to know.

DR. ALLEN: I would also like to add that as we heard that there are about 50 percent of states are currently monitoring prescriptions and they are monitoring the paper prescriptions. So, if you have an electronic system that integrates, then you can do that on the back end. It can be done automatically and seamlessly so that you can tell if a patient comes and you are getting ready to write a prescription. You can be able to track that down and figure out what is happening. It is all done in the back end automatically and seamlessly and right now where that paper prescription has to go into somebody and I would have to call and find out has this person received his prescription recently. So, that will be done automatically for you if you integrate with that system.

DR. ZUCKERMAN: There is another side to diversion, which somebody who is monitoring programs work on and those are physicians, who write excessive amounts and who collaborate with this and are not unintentional victims.

Of course, that is something where the automated programs very quickly can monitor prescribing patterns of individual physicians and that again has become more common to detect that. So, it is less likely that physicians will renew it if they know someone is watching.

Again, as powerful as any security technology is, it can always be broken. One of the most powerful security technologies is knowing that someone is watching you and that changes the behavior of both physicians and patients.

MR. CAVERLY: Thank you.

DEA.

MS. GALLAGHER: I am Cathy Gallagher with DEA.

I think if I was a physician and I am not, but nonrepudiation would be something very important to me. It is quite often as an investigator we have gone to doctors to say did you write this and that diversion occurs within the office as well. My question would be to Ms. Allen, those offices that are now using e-prescribing, what does the office staff -- what is their role in transmitting?

DR. ALLEN: Typically, most prescriptions are written by the providers and in the instances where you have a mid level provider, for example, a nurse practitioner or a PA writing that prescription, then in some systems there is space for the -- for you to enter, who is a supervising provider so you will be able to track that way. Now, are you asking could a nurse, in fact, turn around and use your PIN and your password and use this to access the system? I guess to some extent that is a possibility, but for the most part I think we have got a lot of rules and regulations in place that prohibit that. That will happen whatever you do. So, even in today's world, you know, a nurse can write the prescription and sign it. There is nothing to stop that from happening unless you have a pharmacist on the other end, who has a high suspicion that this prescription may not have been written by the provider, him or herself.

So, I think that providers for the most part did not allow this to happen, but there are rules and regulations that do not allow this to happen and that will happen if it is paper-based, electronic or however and you have to put in regulations and systems in place to be able to determine whether or not this has happened.

As Dr. Zuckerman said, that there are methods to ensure nonrepudiation, but I think our policy is that, yes, we agree that this is something that should be done, but if it becomes more of a technical burden, more of a financial burden for providers, especially those in small offices, that we are going to find the technology that can help everyone won't be adopted and we will be behind the eight ball. So, it is something that we have to balance. How do we do this, how do we do this effectively and can we do it in such a way that we don't add an additional burden?

MR. TENNANT: Let me just add to that. As Dr. Zuckerman said, there is no way you can prevent something from happening. What you are trying to do is make it as difficult as possible and what I see going forward is EHRs now have the ability to track who has looked at a record. We need to have that same capability in the e-prescribing system, so you can look at say who sort of broke into the system, who left their fingerprints on it. I think we also need to be accelerating this technology in the certification realm. So, the CCHIT, I think, is going to be a very important player here to make sure that the systems that are certified have these capabilities.

DR. ALLEN: I have spoken to physicians who are using e-prescribing and electronic systems and in academic institutions and in smaller institutions and the one thing they tell me is that they have had very few instances where they can document that somebody has access inappropriately and as Dr. Zuckerman pointed out that checking and auditing and letting people know that you are being checked and monitored is a powerful deterrent for people to do things that they shouldn't be doing because you can't catch what is happening in today's system.

MR. KOCOT: My name is Larry Kocot. I am a senior advisor to Dr. McClelland as well.

I had a question for the panelists. You all talked about the benefits of e-prescribing. I think we all recognize the good that will come out of this. Dr. Zuckerman, you specifically made the point that without adoption, there will be no benefits from e-prescribing. That is a very valuable point.

You seemed to say that we should start with conventional technologies and work towards PKI so that we don't burden the system and discourage adoption. I would ask the panelists to just speculate what is your projection for adoption by physicians over the next five to ten years. How fast will that go and if we burden it, what impact will that have?

DR. ZUCKERMAN: I think the strongest determinant will be incentives. We know from experience in other countries that you can go from where we are today to close to a hundred percent adoption within two years if you put some money in the hands of physicians and give them incentives to do it. I think that the adding additional costs, whether it is time cost or dollar cost will only slow that progress.

It takes about six months for most physicians to really begin to break even, switch over and see the enormous benefit of electronic prescribing, particularly if they are doing it in a full context where they have other clinical data to go with it and a full medication history, knowing what other physicians prescribe. My practice, over half the prescriptions my patients come in on were written somewhere else. They started in the hospital, the ER or with a specialist. And, you know, I think we shouldn't be thinking five or ten years. We should be thinking two or three years to make this happen on a close to universal basis.

MR. TENNANT: I think there is a lot of sort of rivers converging here. For example, our survey that we completed with AHRQ showed that only 14.1 percent of ambulatory settings have EHRs. That number is abysmally low. So, if things are happening, I think the CCSIT certification process will be important. I think should CMS release its rule on the stark SAFE harbor, I think that might accelerate especially e-prescribing. I think if it is coming from the hospital, picking up the cost and doing the education, I think that might really accelerate the use, but if controlled substances are not included, then you are trying to convince the physician to have two systems and it is a discouragement I think to move forward. So, I think the quicker we can move forward with a complete process, I think, the better.

DR. ALLEN: I think that one of the things we want to try to do is in addition to giving the incentives is to lower the bars to adoption. I will give you a for example.

A few months ago, I worked on a project where we were looking at e-prescribing and how we were going to implement this in a number of clinics. One of the things that we had to struggle with in terms of -- is how we were going to deal with controlled substances because we knew that we couldn't do this electronically. We know that even if we wanted to print out the script, then we had to issue the paper. So, there was a whole host of areas that we had to cross. What we are trying to say here is that e-prescribing is probably the lowest level that a physician can enter if he does it as a stand-alone system, probably not the best way, but the lowest way is the easiest way.

If we put barriers in place for this simple part of the puzzle, not simple, but the smallest part of the puzzle that they can do, it is going to make it a lot more difficult for that adoption to take place. So, I think the simpler answer is that we need incentives. We need to reduce the barriers and allow them to use this technology to its fullest extent for all prescriptions.

DR. EVERETT: On a very concrete level, I am also trying to think of what you are imaging your physician in an office. It doesn't currently have a system in place, who may be a -- you know, as many physicians are in single offices, what would make that person want to change their system and time and education are a factor with regards to that. It is very easy to write a prescription by hand and the transaction is finished then and there. That can be done electronically, but there is the time involved in doing that. So, I don't -- incentives are involved, but I don't think it is all just financial incentives.

I don't know what kind of training we are talking about, but I am thinking also about initial training and how long it would take to get physicians to do that. They are going to have to stop their practices for a couple of days to learn how to do this. Those kinds of things would be -- could be considered as barriers as well.

DR. ALLEN: Those are barriers. I think that and one of the things I tell physicians who are thinking about adoption of technology is that this is not the equivalent of going out and buying a Dell, any level, that you have to have a -- in place. You have to think about how you are going to do this. As I said, you know, how to do electronic prescribing, but what were we going to do with the controlled substances. Those had to be taken into consideration. But I think the key thing is that once it is adopted, physicians will tell you we should have done this a long time ago, that this is a benefit for us to be able to write that prescription electronically -- sent to the pharmacy and our patients can get that filled.

If we look at the benefit in terms of how do we make this work, I think that is the bottom line.

MR. TENNANT: I think, we all recognize the benefits and the question is, well, if it is so wonderful, why haven't we done it. The simple reason is money. I think should CMS come out with a pay for performance program because there are two ways to think about paying for performance. You can pay for outcomes, which means a lot of pay for work and hassles or you can say we know the system is going to save money if we adopt e-prescribing. So, let's pay for it at the front end, you know, use a modifier and give it a little additional money and if a physician knows they are going to be paid a little bit more, they can build their budgets and all of the sudden they realize that it makes good sense to move forward.

DR. ZUCKERMAN: We have a lot of examples from other parts of the world, other industries. New South Wales, Australia, they gave physicians $1,500 a year and it got going very quickly and then they let the drug companies put ads on the system, something I don't think we would ever want to do in the United States, but over there physicians are more than happy to have the drug ads just like they see in their journals pop up so that they don't have to pay for this computer or this system.

We ought to take a lesson from the lawyers. Lawyers in law school get free access to a whole lot of technology services that make them totally dependent on technologies and once they graduate, they are not willing to go back. If we subsidized electronic prescribing for every medical student and every resident in the United States, it wouldn't take more than two or three years to get all of those new physicians coming out insisting on having at least electronic prescribing and probably moving very quickly to electronic health records.

In fact, the American Academy of Family Physicians wants to require electronic health records within all of their residency training programs within the next few years. This is the way to get it done. Make the new physicians dependent on the technology so they won't go back.

MR. CAVERLY: Thank you. DEA, additional questions? None? HHS, any additional questions?

All right then. Thank you very much, panelists, for adding your opinions and expertise, for your professionalism.

[Applause.]

Let's go ahead and take a break, let's say, until 2:30. It is 2:15 now, 15 minute break.

[Brief recess.]

MR. CAVERLY: We are actually running about five minutes ahead of schedule, which is great.

Agenda Item: Pharmacy Perspectives Panel

As we proceed through this last panel this afternoon, it is the Pharmacy Perspectives Panel, as we had discussed this morning this issue of electronic prescriptions for controlled substances certainly starts at the doctor, but it is the pharmacists that are responsible for filling that prescription and at least under current DEA regulations are the only ones responsible for keeping a record of that dispensing. So, we have gathered some folks here to represent the pharmacy perspective on electronic prescriptions.

We have Paul Baldwin with us, who is the executive director for the Long Term Care Pharmacy Alliance.

Colleen Brennan, director of professional and education affairs, the National Community Pharmacists Association.

Lynne Gilbertson, who is the director of standards development for the National Council of Prescription Drug Programs.

Calvin Knowlton with the American Pharmacists Association.

And Kevin Nicholson, vice president, pharmacy regulatory affairs, National Association of Chain Drug Stores.

So, thank you, folks. Thank you, panelists, for participating in this process with us. I will go ahead and let you get started.

MR. BALDWIN: Thanks very much. My name is Paul Baldwin. I am executive director of the Long Term Care Pharmacy Alliance, and as a trade association exec, it has always been one of my personal objectives to have as few official contacts with the Department of Justice as I could possibly have. Boy, I am relieved that they are smiling.

I will tell you what, I am not a -- you will soon find out some confessions are better made at the beginning rather than to be embarrassed and found out later as you would easily discern from my remarks that I am not a technology maven, although I did manage to talk my wife through hooking up the Internet connection last night on the phone. So, I think I am a little bit better than I thought I was.

But I am really here to talk sort of about the perspectives of long term care pharmacy and how, you know, this issue of electronic prescribing of controlled substances needs to happen in the long term care pharmacy environment. Just to give you some background here, this is an area that is a little bit different from the normal practice setting. First of all, the Long Term Care Pharmacy Alliance is a trade association that represents the leading providers of long term care pharmacy services. So, our members provide pharmacy services to residents of long term care facilities and I think for the purposes of our discussion today, even though the long term care environment is becoming more and more expansive, I think, you know, traditionally when we think of long term care environment, we think of nursing homes and certainly skilled nursing facilities are sort of the thing that most people come to mind and I think for the relevance -- purposes of relevance for our discussion today that maybe we can think about skilled facilities as being the venue in which we will have this discussion.

Our members provide services to just about 60 percent of the residents of the 1.6 million residents of long term care skilled nursing facilities in the United States. The long term care continuum goes anywhere from skilled nursing facilities to nursing facilities to assisted living facilities, group homes. One of the -- we frequently talk about long term care pharmacy in the context of Part D, which frankly has been consuming us all for the past better part of a year and, in fact, some of us for the better part of three years. This is the nice opportunity to sort of break away from the day-to-day concerns of Part D and think about the future. This certainly we think is a considerable part or a serious part of the future of long term care.

The average long term care resident in the skilled facility is 84 years of age, takes roughly nine medications at any given time, including over the counters and PRN medications. They have eight different disease states and over 50 percent have some level of cognitive impairment.

So, we are talking about the oldest and the sickest among us and two-thirds of these residents are dually eligible. They qualify for both Medicaid and Medicare and roughly 70, 75 percent of these folks get their drug benefits under the Part D benefit. Pharmacies in -- one of the distinctive features of long term care pharmacy versus retail pharmacy is the fact that in long term care pharmacies, the patients don't come to us, obviously. We go to the patients. So, that is a distinctive feature and that really sort of puts everything on its head when we talk about how are we going to process transactions, how drug orders are transmitted and how they are dispensed and how they are delivered and how they are delivered to the beneficiaries.

So, just to give you the -- and by the way, I mean, in preparation for this meeting, you know, I took the hard road and actually read through the Controlled Substances Act. Whoa. I am hoping to earn points here for this. I actually read through some relevant sections of the Code of Federal Regulations, Title XXI. So, I even knew that stuff.

MR. BARBER: I am surprised you didn't read it ten years ago.

MR. BALDWIN: Gee, I wish I had.

One of the things, one of the benefits you get of reading the Controlled Substances Act is that you are no longer guessing what they mean by controlled substances. These guys are serious about this word "controlled." As you will see, we talked about the process of ordering and dispensing in long term care facilities how this process works and what areas we think, you know, there are some opportunities to have an ongoing discussion.

In the long term care pharmacy industry or the long term care industry, unlike retail, where the physician generates a prescription, which goes to the pharmacy, in long term care environment, everything happens beginning -- the end of the pipe, the intake part of this whole pipe is the nursing facility. That is where everything happens. We don't work off discrete little slips of paper that have prescription on it with a sig and Rx and the number of dispensed and refills times x with a signature on it. It is off a chart order.

Those chart orders are then transmitted generally via fax to a long term care pharmacy and a long term care pharmacy can serve as few as, you know, 100 to 500 residents or as many as 20,000 residents. One of our members has a fairly large long term care pharmacy up in Annapolis

Junction, Maryland that services over 20,000 nursing home beds in three states. So, a fairly good size enterprise.

When the order comes in, the chart order comes in to the pharmacy, the pharmacy then -- you know, this is sort of a real -- a very important point of contact here. The pharmacy then, you know, whoever intakes that prescription, verifies it and then transfers it to the computer systems for both, you know, quality control, processing and payment information. Then that prescription then gets, you know, checked against the DUR and the other systems we have in place to make sure that the drug is appropriate, that it is not contraindicated or it is not going to cause a drug reaction with a drug currently taken by the beneficiary and once it passes that, then it goes through the process. Ultimately, it ends up in the staging area. Trucks are loaded and the drugs are carried out to the facilities served by that pharmacy.

Again, the delivery rates can be anywhere from a few miles to over a hundred miles and sometimes deliveries take place as few as once to as often as three times a day. Of course, there is all the issue of stat orders where we need to get out drugs at any given time of day between scheduled orders.

So, that is pretty much the process flow and when we get into the issue of controlled substances, you know, Schedule II drugs, those can be ordered, you know, via fax, but, of course, having read the DEA regulations on this and having talked to people who actually do this, you have to, you know, the wet signature. How is that for jargon? Wet signature. Good. I am racking points up here.

You have got to have that signed prescription within seven days according to DEA and I think maybe some states have even tightened that up. But in most pharmacies, now think about this, when you have got a pharmacy that serves 20,000 beds, you know, making sure that you have a hard copy of a controlled -- you know, a Schedule II drug is a full time job for somebody. In some cases it can be a full time job for two people.

So, being able to transfer this whole process to an electronic system in which, you know, the DEA drafts regulations on and it makes it, you know, no longer required for us to get hard copy, has a tremendous opportunity to save money, which is important in our industry, but it also has a very high potential to save on the obvious things we have talked about today, which is medication errors and, you know, dispensing errors, things that happen when we are reduced to trying to read somebody else's writing.

The one critical element that I think I want to -- and we have hard experience with this issue on how regulations are written over the past few years because, you know, unless our industry is attentive to the actions of the Board of Pharmacy or in this case the Drug Enforcement Administration, often the assumption is that the physician is the prescriber or the prescriber is the point of entry of everything. The prescriber is the nexus or the initiation point of everything that happens with an electronic prescription.

One of the examples of where oversight has caused us administrative issues is when, you know, in the past when we have had to deal with boards of pharmacy on audit issues and they say, well, you know, your Medicare -- we need to see the prescriptions for these drugs you have dispensed and charged to Medicaid and we have to say, well, you know, we use chart orders. We don't use prescriptions and the auditors scratch their head and say, gee, I wonder if there is a provision for that in the Board of Pharmacy laws to do that. So, we end up having to sort of scramble around and try to make sure that, you know, those things are legitimate.

Now we have an opportunity here, though, during this process to point out that the beginning point for this whole process of prescribing, whether it is controlled substances or uncontrolled substances, is the nursing facility and not a physician necessarily with the PDA. So, I think that is a critical point that when we talk about, you know, from a regulatory standpoint that we make it clear that the nursing facility here is the genesis and the jumping off point of all the electronic or all the prescribing process.

Now, the reality of life for nursing homes is since we have dragged the nursing homes into it, remember that the nursing homes generally are not DEA registrants. Most, unlike hospitals, which have, you know, DEA license and a prescriber or a pharmacy, a nursing facility is generally not regulated by the DEA. So, you know, how are we going to -- and I think that has some implications when it comes to, you know, what do we require for terms of, you know, transferred, you know, digital signatures and those kind of things.

The other important issue is that when we decide we want to do electronic prescribing in long term care, I think we have to realize that just as, you know, Dr. Zuckerman mentioned in his presentation, that the nursing facilities in this case are going to have to see a tangible benefit, a benefit that is worth investing whatever is required from a technology perspective to be able to get this thing in the loop.

Now, certainly from a regulatory standpoint, as they are subject to federal survey and certification oversight, there is an incentive to make sure that you can do whatever you have to do to improve quality of care and minimize drug prescribing misadventures, but, you know, one of the disturbing things, I think, or one of the things that bears some consideration is that nursing facilities were not among the proposed entities to have some kind of a safe harbor under the start clause, as I understand it.

You know, if you are going to enforce the nursing facility, which, you know, operate on fairly thin margins to invest significant amount of money in technology systems in order to be able to generate prescriptions to a pharmacy, then I think the logical conclusion is that we probably have to provide some sort of a financial incentives or financial resources to be able to do that.

We are in favor -- I mean, as you can see just from my brief comments here, obviously, there is a lot of benefit to be had in the long term care environment for a conversion from a paper dependent system and over to an electronic system. We think not only obviously in money -- you know, I had one pharmacy, a considerable sized pharmacy out in the Midwest tell me that they spent in forms -- this is not all related to prescribing, but in forms alone, in preprinted forms in paper, this fairly substantial pharmacy spent over $17,000 a month just on paper.

Anyway we can reduce that paper and the associated costs of moving that paper from one pile to another has potential to increase the efficiency and increase patient safety and increase effectiveness of what happens in the long term care environment.

So, you know, I am feeling pretty confident now. I think I have gotten through this. There is not a whole lot of looks of skepticism out there. So, before I am tempted to get into the vagaries of PKI and PCPDP and X12, I am going to leave.

[Applause.]

MS. BRENNAN: My name is Colleen Brennan and I am from the National Community Pharmacists Association and I would like to thank the DEA and HHS for inviting us here to really give the community pharmacists' perspective, the independent community pharmacists' perspective. One of my colleagues is also at the table, who will talk a little bit about chain drug store community pharmacy, which has a very similar perspective, but a little bit different. He will talk a little bit later.

So, a little bit about NCPA. We were actually formed in 1898 as the National Association of Retail Druggists. We are currently in our 108th year, which is very exciting for us. We represent the pharmacists, owners, manager and employees of nearly 24,500 independent community pharmacies in the United States. Independents dispense approximately 1.6 billion prescriptions annually, which is

42 percent of the retail prescription market and we really like to say that prescription medicines are our business because 92 percent of our members annual sales are from prescription medicines, which is slightly different than you may find in the chain drug store world.

So, it really is our business. We do a lot of it and I think Ms. Ferritto has mentioned earlier that if 11 percent of the prescriptions yearly are controlled substances, then our folks are filling a lot of those controlled substances. Independent pharmacies offer a wide range of patient services, I think, pertaining to our topic today, hospice and pain management would be the two areas that would mainly impact the controlled substances. You can see 39 and 20 percent respectively of our folks do do hospice and pain management.

Also, I think pertinent today to today's discussion, our folks are very well connected. We do a yearly survey called the NCPA Pfizer Digest and it is kind of a breakdown of all the services and things that our folks do during the year for their patients. You can see that 71 percent of our members utilize the Internet from their pharmacies. So, there are some folks who live in rural areas who may not be so well-connected, but for the most part people are coming along and this is a really tremendous opportunity for them with e-prescribing.

So, NCPA believes tremendously in the value of electronic prescribing not only for regular prescriptions, but also for controlled substances, so much so that in 2001, along with NACDS, we formed a -- partnered with a company called SureScripts and we developed that company, which represents about 55,000 of the independent and chain community pharmacies. The goal is to utilize electronic prescribing to increase patient safety, efficiency, quality of care.

SureScripts enables true electronic connectivity between physicians and pharmacies and I think you heard that earlier today. So, the benefits of electronic prescribing, there are just a lot of them actually. So, what I did was to get ready for this presentation, I spoke with a small population of the folks that we represent, some of our members and did a very informal survey and asked them about the types of things that they value, those that are using the electronic prescribing.

The fact that the physician is able to direct the prescription to a specific pharmacy is very important, especially when you are talking about controlled substances. You are worried about drug diversion and forgeries, et cetera. So, they feel that there is less incidence of drug diversion if you are able to control it in this fashion. Folks feel that the electronic prescribing is more secure than paper and oral prescriptions -- I know we talked about that a little bit earlier this morning with regard to controlled substances and a secure network for tracking the prescription, such as SureScripts and some of the other things that I am sure we will hear about tomorrow from the other vendors, can really be analogous to the track and trace technology that we are looking at for counterfeiting in that the prescription can be tracked from the physician to the pharmacist to the patient and you know if that patient has picked up their prescription in the long run.

So, that also gets into other matters that are near and dear to my heart, like adherence and compliance and persistence. You know, has the patient picked this prescription up and are they taking it?

Electronic prescribing would also provide a more accurate inventory control, possibly an inventory reduction of controlled substances. Folks are always worried about having their stores broken into and burglarized and their controlled substances being taken. So, that could be a positive also. There is an easier tracking of professional competency issues. I think Dr. Zuckerman mentioned that earlier. You can really kind of see, you know, who is out there prescribing what and how often.

Studies are showing a decrease in time for the pharmacist, meaning they are spending less time kind of on all the work it takes to do faxes and phone calls and all that stuff and what that means is they have more time to spend with patients, which again, you know, kind of feeds into our whole pharmacy quality alliance movement, where we want pharmacists to spend more time with their patients on medication therapy management and other issues.

You can also track less therapeutic duplication by using e-prescribing and it does decrease the potential for medication errors due to illegible prescriptions and I think someone also touched on this earlier. You know, the Institute for Safe Medicine Practice has done lots of studies on this and showing that, you know, ways to decrease medication errors are, you know, classically it is illegible handwriting. People don't do the abbreviations correctly, unclear telephone or verbal orders, those types of things.

So, again, e-prescribing would really help to alleviate a lot of those problems and we would see a decrease hopefully in medication errors. So, today, the Pharmacy Perspectives Panel was asked to look at several things, in particular dispensing of controlled substances, electronic prescriptions, maintenance of them and electronic records.

So, I talked to -- again, I polled some of the folks from NCPA, members that are currently using electronic prescribing and ask them -- the first three questions I kind of grouped together. What is your perception of current risks? How do you identify those risks? How does your electronic prescribing system address those risks?

So, just a couple quotes. One member felt that they are faxing prescriptions already. So, why not do electronic e-prescribing. One member utilizes the controlled substance ordering system. They feel that that is very well regulated and obviously is for electronic ordering of Schedule II drugs. It seems to be working well. So, again, the next obvious step would be to be able to e-prescribe controlled substances.

Actually, a great dovetail with Paul's previous presentation is the fact that I have a member who has a very high long term care business, as well as retail business. Her concern is that all of these processes be the same and uniform. So, she is not doing one thing for long term care and one thing for her retail businesses. As long as the security measures are in place, their PIN or password or whatever type of security measure you would like to take, it is probably actually safer than using the oral orders as we talked about or written prescriptions.

Again, her concern was that the physician can direct the controlled substance prescription to a specific pharmacy and make sure that the patient is getting the right drug from the pharmacist that they want them to go to.

Additional modifications. Most people felt that -- the ones that are using electronic prescribing feel that it is already working. It works well with existing systems and it integrates very well into the current pharmacy work flow. They feel that if they are already faxing some prescriptions and that is integrated into the work flow, that it really is not going to be a huge problem to integrate now e-prescribing of controlled substances into the work flow. The software capabilities are there.

They don't feel it should be too burdensome financially, hopefully, was the caveat. Are the risks to prescriptions for controlled substances different? The stakes are always higher with controls. However, the safeguards in the system that exist currently seem to be very safe and everybody I talked to felt that it has got to be safer than paper because it is so easy to forge paper prescriptions nowadays. The technology is quite amazing from what I understand, not having tried it myself.

So, the last couple of questions were how do you ensure the integrity of your prescription records? Do you see any current or future threats? Again, most folks really felt like they do not see a threat to the system. They really feel like that this is something that they are used to doing. They are used to using PINs and passwords on different systems and really feel like it would take a pretty spectacular hacker to get into the system to change a prescription, where, again, you know, as we have talked about before, you can have people adding zeroes to prescriptions and, you know, all kinds of things and making some pretty wonderful photocopies, et cetera.

So, they feel -- the members that I spoke with feel that they don't really see any tremendous threats in the future and they do feel that the PINs and passwords that are used now are very safe. Smart cards open, that works, et cetera. The folks I spoke to were not real familiar with this type of technology. Their concern only was they are open to new ideas, but their concern is always the bottom line because as you know with independent pharmacies, there is a very small bottom -- a very slow or a very small margin for them. So, technology needs to be affordable for them to adopt it.

So, some additional comments, the question was asked about retention of electronic control prescriptions and the pharmacists that I spoke to said that they currently are used to printing out hard copy prescriptions and as we discussed earlier, there are tons of paper flow in the pharmacy on a monthly basis and it would be great to reduce that, you know, that money and put it towards other things like patient care.

However, they are used to printing out a hard copy currently and they don't have a problem continuing to do that if that is what the law provides for. Everybody is very much aware of the electronic prescribing provisions in the Medicare Modernization Act with the goal to improve patient safety, quality of care to patients, be more efficient, including cost savings in the delivery of care without unduly burdening health professionals, physicians, pharmacists, et cetera.

This, again, ties into the whole quality movement with Medicare. If you can make things more efficient in your work flow in the pharmacy, the more time you are going to be able to spend with your patient and you are going to see other things kind of cascade from there that can only be better for the patient.

Potential disadvantages, again, cost to independent pharmacies. No surprise. Someone mentioned state board of pharmacy uniformity. I am not sure whether that would play in or not, but that is always a concern with our folks.

That is it. I would really like to thank DEA and HHS for the opportunity to present this information on behalf of the independent community pharmacists that I represent. They are a tremendous group of people. They want to serve their patients well and efficiently and I think that electronic prescribing offers them a way to continue to do that.

So, I hope that we will be able to implement that and we support your efforts. Thank you.

[Applause.]

MS. GILBERTSON: Hi. My name is Lynne Gilbertson. I am director of standards development with the National Council for Prescription Drug Programs. I am a little bit of a fish out of water on the panel, representing a standards development organization that is American National Standards Institute Accredited.

We create standards based on industry participants coming together, representing all different sectors of the pharmacy industry, pharmacies, prescribers, payers, health plans, vendors, switches, you name it, all come together, put aside their differences most of the time and build standards that the pharmacy industry can use. We have standards that are named in HIPAA and in Medicare Modernization Act. The telecommunications standard and the scripts standard might be two that you are aware of.

A little bit of background and history of efforts that NCPDP members and staff have been involved in over the years, related to digital signature. This is a historical perspective. So, I just wanted to let you know, in 2000 and 2001, we were very involved in American National Standards

Institute, Health Informatics Standards Board, multi-SDO digital signature project. It brought together quite a few of the standards development organizations and we were very active in bringing forward use cases that had to do with trying to build a digital certificate environment that could be used in health care with a pharmacy perspective.

We were one of the only organizations, unfortunately, that proceeded far enough down the path to bring forward some of the use cases and there were a lot of open issues that were found as we delved deeper into this project in ways that we -- the industry, we weren't aware of, was able to fill in some of these gaps. So, to our knowledge, the project was never completed and the paper was never finalized.

Some industry activities. The National Committee on Vital and Health Statistics solicited industry testimony in 2004 and 2005 related to electronic prescribing, the Medicare Modernization Act and the state of the industry. The NCVHS posted a recommendation letter to HHS in March of 2005. Some of the information I will be discussing as we go forward would include some of the recommendations from NCPDP and the industry. These were submitted to NCVHS in 2004 and then to the DEA as part of our response in 2006.

Some of the industry concerns that were cited during the NCVHS testimony, there was a lack of health care experience and unknown costs involved in supporting the premise they were looking for, which was the PKI and the digital certification security that they were charged to take a look at. They spent a lot of time talking with the industry, trying to pull health care experience in these areas, trying to pull even other experience to see if it could be used as the basis for the health care industry. A lot of gaps were seen. There are things that were started, pilots or theories or things like that, but nothing they could really put their arms around.

They had testimony on the different biometric pilots that were going on and there were concerns expressed by most of the testifiers as to the usability of the biometrics in the health care environment. There were very limited pilot studies that were done in health care and even other industry segments to form the basis for health care so that recommendations were what was proposed to HHS.

Some of the perspectives cited, you have seen some of these as the more knowledgeable industry participants, who are actually doing this every day, have mentioned over the past couple of hours, they are using user registration and verification processes with trusted partners. There is a sign on and authentication processes. There is secure message transmissions going across these wires. There is a lot of auditing processes going on and logging processes.

When it comes right down to it, no matter what the prescription arrives on, it is the pharmacist who is responsible for using his or her professional judgment on whether they should proceed with that prescription. The recommendation from NCVHS and the industry was these were adequate for assuring the appropriate delivery of the prescriber's intent to the dispensing pharmacy.

Some other industry perspectives was a recommendation for a minimum standard for assuring the secure delivery of prescriptions for basic processes for all prescriptions, including the controlled substances. Testifiers noted that there are laws and regulations for fraudulent behavior. The message going across the wire, the transaction packet, does not create fraudulent behavior. It by itself cannot actively do anything. It is the human beings involved that can create the fraudulent behaviors.

There was an electronic signature discussion during testimony, which was very interesting because what we found as listening to the testimony is there are lots of terms thrown around and used interchangeably. One of the first things that was brought forward is a kind of a 101 on what is an electronic signature. This is from the e-sign act, which NCPDP and its members did support, which is -- it is an electronic sound symbol, data string or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. It can be my name. It can be a scribble I make. It can be a password. It can be whatever is determined to be my identifier as my electronic signature.

This diagram you have seen in a couple of presentations today. I can't take credit for it. A wonderful member created it and it was vetted through the membership process, but it does show the different touch points that go on in the e-prescribing security and the infrastructure that goes on. All these different places where authentication takes place, where security is taking place and, hopefully when the testimony comes out, this will be attached in there so you can take a look at it. You see that there is quite a bit of robust touch points going on, as well as all the auditing procedures that take place. It is important to note that obviously some of these do not take place when we are talking about paper prescriptions.

They are going on in the electronic world. Some of this came out of the world that a lot of the industry experts were in, which is the pharmacy claims processing, some out of the credit card world processing. So, there has been experience based on how this flow goes from the prescriber through their networks that they build with trust and into the pharmacy and back. Of course, it goes both directions, from the prescriber to the pharmacy, sending new prescriptions, but also remember the refills going back from the pharmacy to the prescriber asking for renewals or -- those are very important to the pharmacy industry perspective because think of how many prescriptions you have renewals of or refills of compared to how many new.

This last slide is new. I encourage you to take a look when you get a chance in the testimony. This represents input from our long term care pharmacy arena and basically the big point is the note at the bottom, that the security and authentication touch points are the same as used in the non-long term care model, which is the diagram before.

This is a different business flow because as we discussed earlier, long term care does have a different business flow of the electronic prescribing environment, but they use the same security authentication infrastructure. If any of you are aware of the MMA e-prescribing pilots that are going on through AHRQ and CMS, long term care pilot is underway. It is, the first reports, extremely successful. The different entities are I think somebody said tickled pink with what they are seeing as far as work flow changes and it is also based on the infrastructure that they are currently using today and the same as in the non-long term care model. So, it is important not to hold the long term care environment to a different set of standards that may not work or that may negatively impact that environment when it is not proving any benefit to them.

So, that is the newest picture. I would like to thank you for your time.

[Applause.]

DR. KNOWLTON: Well, good afternoon, again. I, too, would like to thank everyone for the opportunity to present the pharmacists perspective on electronic prescribing of controlled substances.

My name is Calvin Knowlton. I am president and CEO of a company called Excelerex. Excelerex provides pain management support services for hospice patients and also is involved in two of the CMS demonstration projects, EMHS demonstration projects. But today I am here as past president of and on behalf of the American Pharmacists Association. Now, the difference is that we have got a lot of busyness at this table, but I think I can help you with it a little bit.

We have folks that represent owners of long term care pharmacies. Then we have folks that represent owners of independent pharmacies and then we have folks that represent owners of chain pharmacies. The American Pharmacists Association founded in 1852 represents 57,000 to 60,000 community pharmacists. So, we actually are the national professional society for pharmacists and many of our members also belong to the other groups, too. So, that is kind of what we are about.

We provide care, our pharmacists do, in all practice settings, of course. Community pharmacies, chain pharmacies, hospitals, long term care facilities, managed care organizations, hospice settings and the military.

Let me first convey the strong support of APHA for the agency's efforts to allow this discussion for e-prescribing of controlled substances. We are very encouraged that the Department has called this meeting and efforts are moving forward with the establishment of an e-prescribing system. APHA was involved, American Pharmacists Association was involved in the DEA's early efforts several years ago to create the public key information based system for e-prescribing. We believe we must take lessons from that -- that were learned from that and move forward without reinventing the process.

So, my comments today will address three basic areas, the benefits of e-prescribing, strategic considerations for controlled substances prescriptions and implementation recommendations. E-prescribing has the potential to substantially benefit the health care system and if developed and implemented as has been discussed today, e-prescribing may create additional efficiencies in the delivery of health care. Now, you have to question that after the article that came out in the electronic version of Health Affairs today about what this really saves.

But we believe it will have some efficiency move to it. It also will provide improved access to patient medical records. That is a key, improved information about drug utilization history, drug interactions, insurance information. therapeutically appropriate alternatives, risk stratification, all sorts of things that are involved when you go electronically. By making this same information available ubiquitously to the party, the stakeholders, e-prescribing may facilitate a lot more collaboration than we have now. This may decrease the time for -- that is needed for phone calls, back and forth between prescribers and physicians and pharmacists and insurance plans.

The other benefits, it has the potential to provide for a safer medication delivery system and that is really the key. For example, the electronic transmission of prescriptions may reduce medication errors through a decrease in the number of illegible handwritten prescriptions. E-prescribing may also reduce the number of prescription forgeries. Forgery of a prescription is a relatively simple task in the current paper-based environment and anybody who is practicing, particularly in our situation with hospice, it is there.

An individual is more able today to acquire the full profile of prescribers. They are able to acquire the DEA number of the prescriber. They are able to prepare a paper prescription and all that is much easier than with electronic activity. E-prescribing will also have a tremendous impact on record keeping controls and will facilitate and enhance enforcement. E-prescribing will reduce opportunities for errors by creating an electronic record and allowing for digitally recorded interactions between the pharmacist and the prescriber. This would reduce the administrative burden inherent in the current recordkeeping requirements from CSA.

You know, when they were talking about recordkeeping, about two people doing records, we service about -- almost half of the hospice patients in the United States, about 75,000 a day. We have probably 35 people to just collect these records, chasing down paper prescriptions. It will provide tighter control when it is electronic. DEA can come in and say I want to see this document, I want to see this zip code, I want to see this drug and it is all available.

Most important, it is going to provide reduced time for patients to access necessary medications and I will tell you that if you are familiar with hospice at all, there is about 170,000 people a day on hospice in the United States and 80 percent of them are in their own home. The hospice workers go to them. Their median length of stay is about 21 1/2 days right now. So, the 75,000, for example, that we service will be a different 75,000 this time next month.

The trajectory of death is phenomenal and predictable and their need for -- over half of these people are post-cancer patients. So, they are in pain crisis most of the time. Their need for quick access is so impeded right now with the current system because the current system was -- you know, evolved way before we all thought about hospice and, you know, so it is really time to change it. This would drastically help the access and the time to care and the time to palliation for the hospice patients particularly.

It is important also to note the degree of benefit to the health care system will largely depend on how the e-prescribing program is designed and implemented, as well as the number of providers who decide to embrace the system and other folks have talked about that, the adoption issue. The adoption will depend on our ability to develop this as a cost effective user friendly system that doesn't create administrative burdens for pharmacists who are prescribers.

The strategic considerations for the controlled substance prescription is to create a usable and practical system that allows for e-prescribing of controlled substances. It is significant to do that, but it is very doable, but while we work to ensure -- while we are doing this, we work to ensure that the drug distribution system for controlled drugs limits opportunities for abuse, misuse and diversion and, you know, what we haven't talked about today and just to plant something in your ear from the DEA, one of the things we see is much, much more of an issue with diversion is not the upfront prescribing and who is doing what. It is the back end, that nothing happens to the drugs when the people pass away.

So, there are 3,000 people dying a day; 1,500 of them that are on pain medicines in hospice alone and there is no control at all, you know, for where a hospice should be -- which is totally funded by the government should say, you know, we paid for that stuff. Let's make sure you are destroying it. Different states have different regs. Most have none. So, there is a lot of stuff out there that is diverted just on the back end and not on the front end.

Now, you have tried -- the DEA has tried to mitigate a lot of these risks by placing rigorous requirements on the distribution of controlled substances and under the CSA Schedule II controlled substances are only dispensed upon receipt of a written prescription, except as was noted in rare cases of emergencies. In emergencies, oral authorization is permitted between the pharmacist and the prescriber, but the prescription must still be written, reduced to writing and delivered to the pharmacist within seven days. That is different with Schedule III, IVs and Vs, where they can be written or they can be oral and they have to be reduced to writing by the pharmacist.

All controlled substances must be initialed by the pharmacist of record and stored appropriately. We would like to move toward e-prescribing of controlled substances and it would appear that the DEA would have to issue new or modified existing regulations to clarify several terms and requirements. Under an e-prescribing system, a quote, written prescription would include prescriptions transmitted electronically and a quote signed position in accordance with the e-sign law, which treats electronic signatures as an equivalent to written signatures, would include prescriptions electronically signed by the prescriber. If the agency moves in this direction, we encourage the DEA to also clarify through regulations that electronically transmitted prescriptions are not subject to the seven day rule, which frankly dissuades prescribers from using C2s -- it is just one more task -- and has no transparent benefit that I have ever seen.

We suggest language whereby pharmacists can initial and annotate prescriptions electronically and that e-prescriptions can be stored electronically as long as they are readily retrievable. But we realize that authorizing regulations to allow e-prescribing may not be enough. We need to ensure that an e-prescribing system is secure and limits opportunities for forging or altering prescriptions. The systems must allow for pharmacists to determine whether the prescriber and the prescription is legitimate. We understand the DEA has concerns about an electronic systems ability to provide appropriate security and controls. At the APHA, we also believe an electronic system will enhance security and controls and not diminish it.

But before we expend time determining how to construct a system that would incorporate these types of controls, we should look at how pharmacists evaluate prescriptions in the current paper-based system. I am sorry some of this is redundant to the other speakers. It is not like the synoptic gospels, where one started and we looked at each other. You know, we kind of all did our own thing here and we can't -- but we have kind of coalesced, it seems like.

Pharmacists have an active role in helping prevent diversion and abuse. Pharmacists evaluate each prescription, using their professional judgment, dispensing procedures controls and common sense. Pharmacists know the prescribers in their community. They recognize the prescriber's signature and know or can access the prescriber's DEA registration number. Pharmacists also know their patients and when a questionable prescription is received, they question the prescription and contact the prescriber for verification or clarification.

The same principles can apply to e-prescribing. A couple of recommendations. Our first recommendation, creating an e-prescribing system for controlled substances does not require the adoption of an entirely new system. Technology -- and I think the last speaker had slides to that effect -- technology already exists that allows for the safe transmission of sensitive information. Electronic technology for e-prescribing is already in use. There are e-prescribing programs currently offered by vendors and electronic prescription routing companies. These technologies in use today must be secure and they are all HIPAA compliant, providing for transmission security, integrity of the information, transmitted access control and authentication.

You know, in our setting with community pharmacists, a lot of what we see, too, is not folks that are in academic medical centers or in the VA, but we see people out in the real world and they are using Blackberries and they are communicating with PDAs on things like that and that is what we need to make sure that we keep to the fore as we are thinking about this. How can we have this implemented in a way that we will have uptake with what they are using now.

The second implementation recommendation that we would have is that it is important that all electronic prescriptions be held to the same standard. This has been said before also. While the risk for drug abuse or diversion or misuse may be greater with controlled substances, all electronic prescriptions should be transmitted in a secure environment. This means that we need one seamless integrated system for e-prescribing of both controlled and non-scheduled drugs. We should base this system on the e-prescribing standards that are being established by HHS and CMS using NCPDP script standard version 5.0.

The third recommendation, we recommend the use of the National Provider Identification, the NPI, as the provider identification for e-prescribing. The NPI is the preferred identifier because it is the identifier that the vast majority of health care professionals and payers must use by 2007 to comply with HIPAA. Use of the NPI would also allow pharmacists to participate in secure two-way electronic conversation with prescribers. Pharmacists could use the NPI to identify themselves in communications with prescribers, allowing both providers to know that the communication is between two health care professionals.

We have that type of communication capability now, just in the companies that are starting to do risk stratification for medication-related problems to show, you know, this person is on the ten drugs and what is the risk of a medication-related problem with those drugs. It would be nice to be able to go back and forth, not just with prescriptions, with that type of information.

The NPI should be the standard provider identifier for any e-prescribing system, but it could be supplemented by the provider's DEA number when it controls substances requested. This is another way to think about it.

Finally, the APHA encourages the agencies to implement an e-prescribing program for controlled substances as quickly as possible. As we discussed earlier, there are many benefits to an e-prescribing system. Because of these benefits, the agencies in the health care community have been working toward this goal for many years and now we believe is the time to make it reality.

So, to conclude, the American Pharmacists Association strongly supports efforts to implement e-prescribing for controlled substances and we do recognize the challenges. An e-prescribing program must be carefully crafted to facilitate pharmacists ability to provide quality and efficient patient care. It must be responsive to the needs of the health care providers. It must be cost effective. It must not create operational difficulties or new opportunities for error, diversion or abuse.

Diversion and abuse concerns about controlled substances are valid. However, we believe heightened security and controls can be achieved through existing technology and the adoption of one seamless integrated system. We firmly believe that an integrated e-prescribing system will enhance patient safety and will facilitate appropriate access to palliative medications.

Again, thanks for the opportunity to participate today.

[Applause.]

MR. NICHOLSON: Good afternoon. I am Kevin Nicholson, vice president of pharmacy regulatory affairs for the National Association of Chain Drug Stores. NACDS has been involved in e-prescribing or the EPCS project since back in 2002, when we were talking about mandatory PKI requirements. So, I want to thank DEA and HHS for revisiting this issue and providing industry the opportunity to share our views on how electronic prescribing systems can meet the requirements, meet DEA's requirements, under the controlled substances act.

For those of you not familiar with NACDS, we represent the nation's leading retail chain pharmacies and suppliers, helping them better meet the changing needs of patients and consumers. NACDS members operate more than 35,000 pharmacies, employ approximately 108,000 pharmacists and fill more than 2.3 billion prescriptions annually and have sales of over $700 billion.

As you heard earlier today, from SureScripts and from Colleen, NACDS partnered with NCPA back in 2001 to create SureScripts to improve the quality, safety and efficiency of the overall electronic prescribing process. As you heard earlier today from SureScripts, they are the largest network to link electronic communications between pharmacies and physicians, allowing the exchange of electronic prescription information. Today, SureScripts has signed agreements and tested and certified software of pharmacies and pharmacy technology vendors representing more than 90 percent of the U.S. retail pharmacies.

Chain pharmacies are very much interested in receiving prescriptions electronically, including prescriptions for controlled substances. More importantly, however, it is imperative that the prescriptions that we receive are confidential, that they are authentic, they have not been altered and that parties to the transaction cannot deny convincingly that they have participated in that transaction.

Being the last speaker on the last panel today, probably a lot of what I am saying is redundant to what other speakers have said today. So, I will to the extent I can, I will try to make my remarks as unique as possible, to keep you folks awake, not that what I am saying is not interesting. However, as far as the benefits of electronic prescribing, I think, you know, we have talked a lot about the benefits of electronic prescribing and I am not going to address specifically the benefits in my comments right now. I think the benefits are well-established and I am really going to focus more on meeting the needs of DEA under the controlled substances act.

Now, it has been stated that only PKI can ensure that electronic prescription transmission can remain secure and so that the prescription remains confidential, authentic, unaltered and that the prescription information cannot be repudiated. We disagree with this. First and foremost we believe that the electronic prescribing systems and technology already in place provide a much less risk and greater security than the prescribing processes than the non-electronic prescribing processes, such as paper and oral prescriptions.

It is well-known that written prescriptions are completely unsecured when they leave the prescriber. Forgeries and unauthorized modifications are existing problems. Oral prescriptions are also subject to forgery. They may be telephoned into pharmacies pretty much by anybody who knows the prescriber's DEA number. I agree with Lynne's testimony that -- with NCPDP's testimony that current business practices for authenticating electronic prescriptions, such as user registration and verification processes provided by trusted partners, user sign on authentication requirements, secure message transmission and auditing systems provide adequate security for electronic prescriptions, including those for controlled substances.

In addition, there could be addition monitoring or auditing processes that could be put in place to provide additional security if that is deemed necessary. As I stated, pharmacies need assurances that the prescriptions that we receive by any mechanism are confidential, authentic and have not been altered.

Ideally, the prescription delivery process would provide for these assurances. For oral and written prescriptions, greater security requirements for controlled substances are commensurate with the greater need for greater security due to the fact that that these controlled substances are more likely to be diverted. However, for electronic prescriptions, the need for privacy security and safety are equally important for both controlled and non-controlled substances.

For example, all electronic prescribing systems must comply with HIPAA and state specific privacy and security requirements because this is sensitive, protected health information. These privacy and security requirements already in place ensure that only authorized individuals may access protected health information that comprises the prescription. The provisions that protect privacy and security will also protect against anyone attempting to access electronic prescribing information for diversion purposes.

Electronic prescribing systems could not exist without these protections from intrusion, whether they be for controlled or non-controlled substances. Additionally, as I stated earlier, pharmacies must be assured that the prescriptions we receive cannot be repudiated by the prescriber. When the pharmacy fills a prescription, they need to know that the prescriber did in fact sign that prescription, that the prescriber can't go back and say, oh, no, that is not my prescription. I didn't write that. I didn't write it for that drug, that strength, that dose, those directions.

Again, systems are already in place, such as we mentioned earlier, the use of registration and verification of processes. These are sign on authentication requirements and network auditing and monitoring procedures. These will assure that a prescriber cannot repudiate electronically transmitted prescriptions.

Finally, pharmacists will still rely on their professional judgment before filling a prescription, whether it is provided to them electronically or by paper or by call in from the prescriber's office. Pharmacists are familiar with practitioner's prescribing patterns and if a particular prescription seems questionable, a pharmacist may still contact the prescriber to verify that prescription's authenticity and validity.

So, as I reach the end of my prepared comments, we believe that current electronic prescribing systems meet DEA's requirements for controlled substance prescriptions. The systems in place have been designed to protect sensitive patient health information from unauthorized access. These systems comply with federal HIPAA and state specific privacy and security requirements.

Unauthorized individuals may not access these electronic prescribing systems. This is true for privacy and security protection, as well as for diversion prevention. Moreover, current electronic prescribing systems provide much more protection from diversion than the current system of paper and oral prescription. Also in closing, I would like to address Dr. Ross Martin, One of the earlier speakers mentioned that Ross had come up with an idea that it would be -- perhaps it would be a good idea to facilitate electronic prescribing, electronic prescriptions for controlled substances if the prescription was written and signed with a wet signature, in addition to being transmitted to the pharmacy.

I just want to -- with all due respect, I want to say that probably won't work for pharmacies because it would be very difficult for the pharmacy to have to match up electronic prescription that came in with the wet written -- match up with the written prescription with the wet signature. So, I just want to mention that we don't believe that would work in the pharmacy environment.

But thank you and thank you everybody.

[Applause.]

MR. CAVERLY: Once again, my thanks to the panelists for their participation and sharing their views and the information that they have been able to share with us. We are going to throw this again to questions to our panelists from the DEA and HHS representatives. Why don't we throw the first question to the DEA side this time to kind of shake things up a little. We will see if they are awake.

First question for DEA.

MS. GALLAGHER: I will jump in here. This might be stupid question but it will help me understand the issue. I forget which panelist talked about the pharmacy being able to talk back to the doctor on refills and if there was a question on a prescription, how would the process work getting it back to the physician's office is my question and who responds back? Is it a staff member or what is the process in -- I am assuming this is going on in today's practice. I just would like to be educated.

DR. KNOWLTON: I think that was me, Knowlton.

Well, in our own practice, we do that already. So, it is two Blackberries right now. It is not for controlled substances, though. But we go back and forth.

MS. GALLAGHER: It is not a trick question. Just by e-mail?

DR. KNOWLTON: Yes, just like you -- but it is secured. It is behind the firewall and secure. So, you can -- you know, there are certain ways you can do that, where you can share patient information. You can't do it through regular e-mail, obviously, but you can do it when it is set up appropriately.

MS. GALLAGHER: Is it the physician talking back to you, not a staff member?

DR. KNOWLTON: No, it is actually the physician that has the Blackberry and then our pharmacist, going back and forth.

MS. GALLAGHER: Thank you.

MR. CAVERLY: HHS, questions? I am sorry. We have a follow-up.

MS. GILBERTSON: What I was referring to is in the script transactions there are a number of different business functions that can be done. The new prescription, which is the doctor's office sending a new prescription to the pharmacy, there are refill requests and responses where the pharmacy can send refill requests to the doctor's system. The doctor may have a designated agent performing some of those functions. They may have different protocols and that is probably better to discuss with the vendors or the -- I guess we have got vendors tomorrow -- of exactly what kind of protocols they might use. There is also the ability on for example a new prescription for the pharmacist to ask for a change because they have noticed something about the prescription.

You know, anything that you might pick up a phone and call somebody for. We also mentioned the fill status notification, which is this prescription has been dispensed, has been partially dispensed or was never dispensed to help with compliance and tracking of patient use of their prescriptions and then there are some other transactions as well.

DR. KNOWLTON: If you are here tomorrow, Russ from Gold Standard is going to be here and they have got a thousand, 2,000 of these in physician's hands down in Florida where they are doing this exact thing right now.

That would be a good one to hear.

MR. CAVERLY: All right. HHS?

MS. TRUDEL: In the event that a pharmacy were asked by the DEA to provide information about controlled substances, could you compare and contrast the types of information that you feel would be available to you with an e-prescribing capability over and above what you would have available if you were just handling the controlled substance prescriptions on paper? I am interested in things like audit walks or whatever. How would that change your landscape?

DR. KNOWLTON: In our practice, we are paperless, except for the C2 thing, but we also have it through optical characters, so it is actually already recorded anyway. But when DEA comes in and we are one of the largest users of these types of substances in the United States and when the DEA comes in, which they do a lot, they can go right to the computer, frankly, and pull up whatever they want instantaneously by physician, by nurse, by hospice, by patient, by drug, by zip code. It is all on a data cube. It is all real time. So, it really does facilitate -- I mean, I know they miss going through the paper things, the file, you know.

MR. CAVERLY: DEA, further questions?

MR. BARBER: I am Linden Barber with the chief counsel's office.

I wish we maybe could have some of the earlier panels ask questions of this panel because I don't know that I can do justice to this, but I heard one of the panelists talk about moving toward one standard, NCPDP, Script 5-0. Did I say that correctly? I think I heard that.

How do you envision this working if the National Health Information System were to go to a wide variety of applications, you can put your prescription on a smart card and the patient takes that to the pharmacy of their choice versus sending it over your VPN or however the networks are currently working? Do you envision the signature technology that you have advocated being sufficient to still provide nonrepudiation, record integrity and is this something that could move beyond the members that you currently have in your associations without requiring them to be part of the network that several of you have been involved in helping to establish so that there is competition in the electronic health information arena? Those are -- I am not being very articulate. It is a very broad question, but maybe you can help provide some insight on those things.

MS. GILBERTSON: Just as a follow-up back to you, are you thinking in terms of whether a doctor writes a prescription on a pad and hands it to the patient or whether it is dropped into a thumb drive, what difference there might be?

MR. BARBER: I guess my question is everyone believes in the benefit of electronic prescribing and it would be great if we could move toward that to reduce errors and a wide variety of other things. But my question is are the systems that you are envisioning, that you are talking about, the ones currently in place, I believe, at least a couple of panelists are involved with SureScripts. What if a doctor doesn't want to send it over the network? They want to put it on -- and, you know, ten years from now we have moved to a system where the patient has a smart card with their health care record on their smart card and the prescription can be directly loaded to a hard token that the patient then takes to pharmacy of choice, not something that they have to tell the doctor ahead of time. This is the pharmacy I want you to send my script to.

Will your system work as far as the signature technology still providing nonrepudiation, record integrity and in light of the fact that several of you are involved in SureScripts and you are looking at advocating one standard, is there a possibility that the type of technology you are advocating can be used across a broad spectrum of other networks that don't tie a physician or other practitioner into one particular network?

MS. GILBERTSON: From a standards perspective now

-- I think the other panelists can address usage, but from a purely standards perspective, you could envision that somehow that physician has to drop a transaction onto that smart card. The patient goes to their pharmacy of choice. They read whatever accessibility they have on the smart card, which might be that prescription request. It has got the user name and the passwords and all the things that are on that electronic transaction that could have been across a wire but it is contained in a packet of data sitting on that thumb drive. The same controls would be accessed. Do I know who this is? Do I recognize the prescriber? Do I recognize through the environment?

Now, you might -- you are shifting the control because things that the networks in between do as part of trusted environments might have to be shifted down to the pharmacy for that kind of control. So, there would have to be some real discussion on that because the trusted network is one of the infrastructures of why these people are connected to each other. Otherwise now you are putting all the trusted controls that the networks are providing onto each end of the user. So, that may make it more difficult for the user systems themselves.

DR. KNOWLTON: This is why you guys get the big bucks to make these regulations. That is a tough one.

You know, people write a prescription. They mail it. The brother drops it off. The sister drops it off. The friend, whomever. You know, they get there all sorts of ways now. I think that is exactly what you said, what we would want to see continue, not to be pushed into just one way of doing something, but have some options as technology evolves, you know, that we could -- that this could fit into.

When we said one standard, what we were more referring to was, you know, one thing for all prescriptions, you know, for control, non-control. So, we don't have systems that are different, that we could use one system and it would work everything. But I agree with you. I think variety is what we would need to go.

MS. BRENNAN: From our perspective or from my own perspective, I am not a technology expert whatsoever. My guess would be -- and you would have to check with the vendors, you know. My own perspective would be that the technology is going to grow and as there is competition in the market, you know, things will change. I think that as Calvin just said the consistent -- we want some consistency of the way things are done and then the technology, I think, will advance beyond what we can even think of today.

MR. BARBER: If I may with a follow-up, the -- I am trying to think about the practitioner who is writing the prescription. If you are in the SureScripts network and you are enrolled by one of their practitioner vendors, you would have your PIN and password if it is a smart card, whatever it is that you authenticate to the system, that practitioner then cannot use that to prescribe over any other network at this point, can he? Or --

MR. NICHOLSON: I think we would have to ask SureScripts, maybe during the open mike they can -- if there is someone still here from SureScripts they can address that.

MS. GILBERTSON: I mean, the networks connect to each other. SureScripts talk to each other all the time, sharing, so that you can get multiple ways for multiple transactions. But your first entry point is into your trusted network and you don't want 50 different trusted network entry points if you can help it. It is just suicide for the vendors and for the practitioners.

DR. KNOWLTON: But, you know, I think to complicate it more, since you are asking these kinds of questions, it is not far away when it is going to be voice recognition, too. So, we have to -- when we are writing the standards, I think there are other -- if you digitally recorded a call that is coming in, right, that should be sufficient, as long as I can recognize the voice, electronics can recognize the voice, you know. So, as you think -- I think we have to think about where this stuff is going. These handout things may just be a temporary thing for all we know as voice recognition comes on and stuff. We get back to talking to each other.

MR. RATLIFF: Do you want a SureScripts answer to the question?

MR. BARBER: I am not in charge. So, I don't want to ask questions of the audience necessarily.

MR. CAVERLY: Without taking too much time away from it, if you want to address that point?

MR. RATLIFF: The specific point about the question of registering a physician and then them having access to multiple networks, the same principle would hold for other networks and there are physicians that write prescriptions and send through our network to pharmacies connected to our network, but those same physicians might send the prescription to a pharmacy connected to another network and it is possible. They would have to be registered in a very similar fashion to what they are now or could be identified uniquely, et cetera. The vendor applications which we will hear from tomorrow, help manage that at least at the end user level and then the connectivity --

MR. BARBER: Thank you. That helps. I guess my thought and perhaps this is a question that I will put out for the open mike time to hear from practitioners as well as some of the folks that spoke this morning on technology and will speak tomorrow.

One of the concerns that I thought I heard from the practitioner panel is multiple passwords, multiple registrations doesn't work. We want one thing that is applicable across every potential avenue by which I can e-prescribe and if we are looking at specific networks and you are going to need multiple registration that seems -- my question is is that an inhibitor to adoption on the practitioner side of things. It sounds like if you are a pharmacy and you have got your network hooked up, then you are fine as a pharmacy, but practitioners, do you want that type of system where you are plugged into only one network, with that registration need multiple registrations.

So, I will just leave that as an open question if anyone cares to address that during open mike time.

MS. GILBERTSON: Well and there is some precedents to that in the credit card world and in the pharmacy claims processing world with entities that choose to use one network over another for business reasons. But the mechanism of talking to that network or the next network if they decide to move to a competitor is the same and that one needs to be important. It is one set of rules that govern that. So, if I want to take my business from this network to this network, I am still going to send the same kind of information that I send today. I may reregister. I may have to go through certification processes, but once I am up, I am sending the same stuff I would have sent yesterday. That is the precedent that has been used in other aspects of, like I said, credit card and in pharmacy claims processing.

MR. CAVERLY: HHS.

MR. KOCOT: We have heard a couple of comment thieves from the practitioner panels. I just want to kind of go over -- first, it seems like all the practitioners agree that is far better to go e-prescribing for controlled for controlled and non-controlled now as it gives more protection than current paper systems, even with the -- even without a PKI technology. In addition to end to end security, I mean, we haven't even talked about the fraud abuse detection abilities that, for example, credit card networks have and so forth. There are a lot of applications that law enforcement could use to detect fraud instantaneously as opposed to after the fact.

I heard Dr. Zuckerman say that we should phase in PKI and really seems to be a divide here because NACDS perception is that we don't need PKI, that the DEA's concerns with confidentiality, integrity, nonrepudiation, authentication can be met with current technologies.

Dr. Zuckerman made an interesting recommendation that we move forward now with current systems and then implement a phase-in of PKI or if there is a better technology or something else that would satisfy the DEA's concerns, we should start that now and get into that process and evaluate as we go. I am wondering if NACDS has the same perspective and other panelists have the same perspective except leave in whatever that technology is, PKI or whatever to add in if law enforcement feels like they need even further security or further protections.

Can the panelists comment on that?

MR. NICHOLSON: Let me just address it a little bit that we believe that -- as you said, we believe that the current systems are adequate, but we feel also that if there is a thought that additional protections, additional security is required, additional functionality is required, we would support additional monitoring or auditing procedures to the current system.

MS. BRENNAN: I would say from the NCPA perspective we just need to get going, if we can start somewhere and as the process evolves and other standards need to be added in or monitored, et cetera, that is a good thing.

DR. BALLOW: And I would agree. You know, things in our environment are a little bit simpler in that just remember that, you know, the pipe that goes from the nursing facility goes to the pharmacy. It doesn't go to a thousand different pharmacies, we hope. I think, you know, what we are looking for here is a system that works, that is secure, that accomplishes you know the objectives we have established I think, the desirable outcomes for electronic prescribing whether it is for controlled substances or for non-controlled substances. You know, to have the investments that are required but certainly not require any more than that.

MR. CAVERLY: Additional questions from DEA?

MS. FERRITTO: I am not sure if you all are the right persons to address this, but if a person -- if a pharmacist were to receive a prescription electronically today, using the current systems, how would they be able to know whether that prescription was altered after it was written and if an investigator were to come into your pharmacy today, how would they know that a record that they were looking at that was created or received by you 18 months ago was, in fact, what you received?

MS. BRENNAN: Good question. Again, I am not a technology expert, but one of the pharmacists that I spoke with yesterday talked very confidently about the process of tracking the prescriptions through what he called routing numbers and being able to track and I.D. apparently from, you know, beginning to end and that you would be able to see if there was an interference there. Again, probably a vendor question, but his confidence level was very high that you would be able to tell if there had been any intervention with the routing.

MR. NICHOLSON: With respect to the transmission of the electronic prescription, how the pharmacist knows that the prescription received is, you know, completely accurate and authentic and valid. I mean, our members use SureScripts as their trusted partner to ensure the validity and accuracy and authenticity of their prescriptions. Again, I would have to defer to them to describe how they ensure that process.

With respect to once the prescription arrives at the pharmacy, how does an inspector know if a prescription has been altered within the pharmacy, an electronic prescription. Now, again, I am not a technology person and I can't speak for any specific chain, any specific pharmacy, but I would -- just from a legal standpoint, pharmacies need to keep records of any changes made to their records. You know, just from a liability point of view, you can't allow pharmacists or technicians or anyone else access to a prescription, allow them to change it and not have that change recorded and by whom that change -- by who made that change.

I think the state boards of pharmacy would require that. They would require some sort of audit process and certainly you would require that for your own legal liability concerns.

But, again, I would have to ask a technology vendor to explain how exactly that happens, the exact process.

MR. CAVERLY: Additional questions from HHS?

MR. KELMAN: I have one last question for my point.

In view of the fact that e-prescribing is real time connectivity, would anybody on the panel like to comment on the potential for use in terms of safety, quality assurance, control substances, medication therapy management, clinical support systems.

DR. KNOWLTON: Most of the medication therapy management systems, the risk stratification systems, the drug systems, the drug interaction systems and all those things are all electronic. So, when you are receiving the prescription electronically, it can actually be pushed through the system ahead of time before real people even look at it and give you a risk stratification of the patient. You know, is this okay or not? That kind of stuff. So that is the other advantage to it. Otherwise you have to key in something, you know, and that is a chance for error. Then you have to run the program. So, when it is electronic, it can get through that much quicker and help identify potential medication problems.

MR. NICHOLSON: With respect to prescription monitoring, what we heard earlier today, that approximately half the states, I think actually more than -- slightly more than half the states have prospective or actually retroactive prescription monitoring programs where prescriptions are reported to a central database, usually 15 days or a month after they have been filled by the pharmacy. I think electronic prescribing system for controlled substances for -- rather than or maybe in addition to monitoring what has been dispensed, you would also have a way to monitor what was prescribed and I think that would definitely be a beneficial way to track both patients and doctors.

DR. KNOWLTON: Just to put a little icing on that, there are three types of drug use review, prospective, concurrent and retrospective. Retrospective is what normally happens, you know, after it has already been done. Concurrent is somebody has already written a prescription and you are looking at it and saying is this okay before I give it to the patient, but prospective, which is what you are talking about, is where you can catch it before it is even, you know, in the system, so to speak.

So, that is what the goal is. The goal really is to move the whole system to prospective medication therapy management, so you are not at risk of going back to clean up a mess later. To do it at point of care so the doc then knows it, so it comes back to the doc and says, oh, okay, gee, I didn't realize. I shouldn't be getting this, instead of somebody calling up later and saying, oh --

MS. GILBERTSON: And you also get some side benefits with fill status so things that a doctor may not have available now, you know, Mrs. Smith, have you taken all your refills of your heart medicine. Oh, yes, doctor. Well, they now are armed with information that says, no, you only had one refill out of the five. Is there a problem we need to discuss. Things like that that make the information a little bit more accessible.

The other is the advent of the medication history, another set of pieces of information that can arm the clinical decision support with much more information than patient recall or, heaven help us, family recall.

MS. BRENNAN: I agree with all of the statements previous and also the whole idea with MTM is to, you know, find out how the patient is doing, what are they taking? Are they taking their medications on time, et cetera? This all dovetails again into our PQA effort where we are looking at patient adherence, compliance, days of possession of drug, et cetera. So, it all will help. The more information the pharmacist has at the point of seeing the patient, the better they are able to advise that patient on the appropriate use of their medication. That is really what we are all after. That is the bottom line.

MR. BALDWIN: One of the things that I think we have to pay some attention to -- and, again, sometimes the real world can be a little bit more complex sometimes than the theoretical, not always, but in this case, you know, one of the questions I think that the DEA and CMS as well need to think about is at what point do you envision the ability for a third party administrator, a third party payer to be able to intervene in this system? I mean, say, you know, well, this is a Schedule III drug and, you know, it is clearly legally prescribed but it may not be covered or it may be subject to some sort of prior authorization mechanism.

It is not clear to me at what level, at what point in the process, you know, a third party payer or whether it is Medicare, Part D benefit, which is privately administered or Medicaid program or some other program has the ability to intervene in the process and redirect or send it back or somehow intervene prior to its being dispensed.

MS. GILBERTSON: I think part of it is -- one of the speakers alluded to earlier, this is kind of the tip of the iceberg or once you enable the electronic prescribing functions, there is nowhere to go but up at that point. Some of the information that would make it available, Paul, is the prescriber having information to formulary and benefit information. So, they can make an informed decision before they write the prescription.

They can know about medication history. So, they know if there is contraindications going on, things like that that currently perhaps the pharmacist is the only one performing those functions. As far as prior authorization, there is industry pilots going on dealing with trying to connect the prescribers and the payers together, the health plans, to enable once again the doctor to have more information before they actually prescribe the prescription and so it is more clean when it gets to the pharmacy.

MR. CAVERLY: DEA, any additional questions? HHS? Oh, Linden. Pardon me.

MR. BARBER: Kevin, I wanted to follow-up on one of your comments about the pharmacy keeping track of their changes oftentimes due to state regulations and other things and we realize that the vast majority of the professionals represented by all of the panels are complying with their state and local laws, as well as federal laws, that one of the concerns as a law enforcement agency is those who don't comply. So, I would like to explore with you from the pharmacy side, as well as the rest of the panelists, about record integrity.

Michelle had mentioned what about 18 months down the road when we go in and look at it and I have talked to some of the technology panel folks during the breaks to get some information from them from their perspective, but I would like to hear from you when the pharmacy regulatory board goes in to look at records or DEA goes into look at records, how can we -- what assurance is there that that record we are looking at is the same record that the doctor sent and I am particularly thinking about the current requirement with Schedule IIs because if we are going to have one system for all prescriptions, controlled and non-controlled, then it has to be sufficient for Schedule IIs, which is the highly sought after, highly abusable of the controlled substance pharmaceuticals.

Currently, the original prescription, although certainly subject to forgery also is subject to scientific analysis for evidentiary purposes and as the lawyer on the panel, evidence means a lot to me. I would like for you to talk about that and your other colleagues on the panel.

MR. NICHOLSON: Again, I can't describe exactly how it -- you know, the technology behind how it actually happens, but then there are -- I think what we also should recognize that there are instances when the pharmacist, you know, needs to change the record because of change in therapy, because perhaps the dose is wrong, the directions are wrong. There are allowances under DEA regs to change certain information on a Schedule II. So, I think the system is in place to track and audit those changes would also apply for any change that was made to that record.

It has been a number of years since I practiced pharmacy, but back in the nineties what I know that as a pharmacist I could not make a change to a record in the computer system without, you know, typing in my password to access the system and then also, you know, recording that I made that change.

So, again, I can't explain, you know, the technology behind it, but I know that there has to be systems in place to make sure that any change, whether valid or otherwise is recorded and that there is a way to track that change.

MR. BARBER: And I realize again, that may be better directed to some of the folks who might want to speak during the open mike session from earlier panels. I see a few smiles out there.

MR. NICHOLSON: Also, I think there kind of is -- there is a kind of need to also realize that there are two different -- these are like two different questions because there is one question of, well, how do you know when it gets -- that when you receive it on one hand and then the second question -- the second part of that is what you are asking now is how do you know that once you have received it nothing changes at that point. And, again, you know, I don't know the technology behind it, but there are assurances to make sure that every change is recorded and that there is accountability for those changes.

MR. CAVERLY: Additional comments or questions from HHS? We do have one follow-up question over here.

MS. FERRITTO: I wanted to make sure no one else wanted to respond to that, but, again, this may not be a question for all of you, but a lot of you have spoken to audit trails and I wanted to get an understanding of -- because I am not a technology expert either -- whether DEA would look to the pharmacy for these audit trails or whether DEA would be looking to the pharmacies software vendor for these audit trails.

MR. NICHOLSON: I think it depends on who is managing the system for the pharmacy, whether it is -- whether the pharmacy is managing it themselves or whether they have a vendor who does it for them. That is specifically the audit within the pharmacy. If you are talking about for the electronic prescription, then that would be one of the intermediaries, like SureScripts or XO.

MS. GILBERTSON: And you have the current business processes today. I mean, when DEA goes into audit a pharmacy today, you have those steps and processes that are already in place. So, this is some of the same processes. It just came in via -- you know, rather than paper, it came in on -- or a phone call, it came in via an electronic tube.

The other thing is during the NCVHS testimony, I remember one of the presenters discussed about how you can actually track through the entire system from the prescriber system through the network they used, the different steps in the network and then in the pharmacy system so you could actually track that entire transaction at each of those steps for audit purposes, which is something you wouldn't have in the paper or oral environment today.

MR. CAVERLY: Let me offer one more time in fairness, HHS, any additional comments? All right.

Thank you very much. Let's discharge the panelists with our thanks for sharing their views and experience. Thank you very much.

[Applause.]

We have come to the end of our testimony today or the end of our panelists sharing information with us, but as part of this information collection process we wanted to have an open microphone at the end of each day. So, in order to give some structure to this, what I am going to do is I am going to take this first microphone and then we will kind of work around the room and work backward up the aisle.

Agenda Item: Open Microphone

So, I guess the first shall be last and the last shall be first. I would ask in fairness to the other commenters, that you just please keep your comments reasonably brief and if you would identify yourself as well, please.

Yes, sir. Go ahead.

MR. MAJKOWSKI: Ken Majkowski. Just for clarification, a majority of the technology vendors who are connected to us to get eligibility and formulary medication histories and are also connected to SureScripts or ERS or MedoVast(?).

When a physician and a patient choose where they want their prescription to go, the technology vendor has the logic to make sure that the appropriate network is used. Without different passwords, without any different process. So that if it goes to a chain drug store that SureScripts services, it will go through the SureScripts network. If it is a prescription that might go through a mail order pharmacy that the payer or PBM has because the patient has chosen to send their prescription to the mail order pharmacy, then it will go through RxHub to the mail order pharmacy. The physician sees nothing different, doesn't really know that this is all happening in the background, has no change in process. Multiple networks can be utilized by that physician depending on how that prescription needs to be routed.

So, there is no issue there. One other just quick comment and I think several presenters made the point that there is an increase in abuse of prescription drugs. I think it is important to realize that the increase in the abuse and the abuse itself is not all related to the process of prescribing. I heard Dr. Everett talk about the increased use of Schedule IIs by teenagers. I don't think teenagers are breaking into the prescription process and writing prescriptions and stealing prescription pads. I think teenagers are probably using leftover drugs from their parents and their families and maybe hospice patients, as was broad up earlier.

There is more to the increase in use of illicit drugs or Schedule II drugs than the process, that is involved in the actual process. Whether those prescriptions are written, oral or electronic, it doesn't change that part of the problem.

MR. CAVERLY: Thank you.

Let's go to the microphone further up the aisle. Is there someone there? We are in one line. Let's go to the other side then, please.

MR. GRAY: My name is Steve Gray. I am with

Kaiser Permanente. We have physicians, hospitals, pharmacies, all types of facilities. We have a lot of experience with getting the message of electronic prescribing. The first thing I want to mention is electronic prescribing it is very important to move forward quickly with this because it is in many ways -- to the whole use of the electronic health record and probably one of the best uses of the electronic health record and the biggest benefits overall of the health care quality come from the physician support that can be built in to the electronic prescribing process.

You can have that and generate a paper prescription from all the other health information because that would solve a lot of the problems with legibility and so forth. But having said that, I want to go back to the last question asked by the DEA representative. California has recognized electronic prescribing for many years and they decided because of the changes in technology, not to go down the path of writing the specific technology requirements into the regulations of the statute. Instead what they did is they hold the pharmacy responsible for keeping all of the information because it is the pharmacy that is the registrant with the board of pharmacy and the DEA and it doesn't matter who processes their prescriptions or which system you are using now if you hold the pharmacy responsible.

They have a simple statute that basically says that if you are going to receive an electronic prescription and maintain it only electronically, then you must keep everything as it came to you electronically and you must keep a complete record of all changes that are made with complete identification of who made the changes and if it was not a pharmacist who made the changes, a record of which pharmacist authorized those changes. That is written right into the statute and that has served them well.

Obviously, that doesn't work for the full substance prescription because the DEA regulations don't allow it, but it works for the other types of prescriptions. Moreover, the regulations now for and the way that they are implemented in the regulations for HIPAA require that under the security system, you have complete audit trails and audit trails that include not only for changes that were made but for access, for read only access for the record. So, all of the systems now if they haven't already done it are rapidly moving in the direction of keeping complete detailed audit trails right down to literally the subsecond identification of when that access or that change was made. This is another piece of information the electronic prescribing provides now that the DEA wouldn't have. You will actually have a record of date and time as to when that prescription was transmitted, when it was received and so forth.

Now you have a record of when it was sent, but you don't have a record that showed that, gee, this prescription was -- five prescriptions were transmitted from the same prescriber for the same patient to five different pharmacies all within ten minutes. That might be very interesting information to have, which you don't have now. It might be that those prescriptions were not picked up for five different days or five weeks.

So, electronic prescribing of controlled substances are going to provide you with a lot of enforcement information and potential even now, even without PKI and the other things.

My next comment relates to the PKI. We completely agree with the idea that we should move forward with existing technologies right now. There are some perhaps regulatory requirements that you could consider regarding -- and we are talking about audit reports and audit capability that might be required as part of the regulation and would make sense. We have found in our organization it is very helpful to have regular reports back to the people that administer the certification for prescribers because if they are reading the reports and they see somebody that is prescribing, they never certified it. That is very helpful to them. So, those types of reports are completely logical in order to secure security of the system and so forth.

Lastly, I want to make a couple of comments that it is very important to realize that even though that a practitioner panel appeared, it consisted primarily of physicians. There are many more practitioners prescribers that are not physicians that need to be brought into the discussion, including some who are pharmacists. And they have a unique perspective because they have the advantage of seeing through the careers both sides, both ends and even the middle of the process.

So, we have pharmacists that are prescribers. We also have a lot of pharmacists out there who are not prescribers, but they affect prescribing and that is one of the reasons that those of you that have heard me speak at these meetings for the last five or six years have talked about we still need to maintain the ability in some circumstances to have agents of the prescribers able to enter the electronic prescribing process.

An example, clinical pharmacists responsible for review of the patient's medication regimen in a long term care facility, finding something that needs to change. They contact the physician possibly by cell phone and they said, hey there is a change that needs to be made. The physician says, oh, my gosh, you are right. Would you go ahead and take care of that for me? Well, today, that pharmacist could pick up the phone, could call in a prescription, could -- for everything but a Schedule II and take care of that, but it would be far better for that pharmacist to be able to get -- electronic prescriptions with all the decision support, the clearing, the screening and the other advantages that we talked about.

So, there needs to be the ability for some non-pharmacist -- excuse me -- some non-subscribers to act as the agents of the prescriber if you are going to get the full benefits out of the electronic prescribing concepts. And also it is not realistic -- we have learned that 80 percent of our prescriptions in Northern California are electronically prescribed. Why not a hundred percent? Often it is simply because the patient doesn't know which pharmacy he wants to go to. So, they are electronically prescribed but they have to generate a paper prescription to take it somewhere.

There is another process California law allows for an interim data storage device for the description to be deposited in the database with a particular operator of a pharmacies for example and then they can go to the pharmacy of their choice and say there is a prescription waiting for you in the database. I didn't know which pharmacy I was going to be able to get to before it closed. That process is quite common, very handy and encourages electronic prescribing and hopefully eventually we will get to the rest of that hundred percent.

Thank you very much.

MR. CAVERLY: Thank you.

Sir.

DR. MARTIN: Thank you. I am the apparently notorious Dr. Ross Martin who made some comments during lunch. I am the director of health care informatics at Pfizer. My purpose of being here with my Pfizer hat on is that as one of the founding organizations that supported the creation of -- we really do believe that strong PKI is ultimately where we want to go, not just for controlled substances but for the entire -- system and really not just for the health care system but for everything that we do that requires nonrepudiation authentication and we -- in as much as possible we want one system to do that, one methodology for doing that and especially health care. Because DEA has particular requirements that are like the other -- regulated health care research, very high level of authenticity required. We see a common interest here in doing this in a common way.

So, that is my Pfizer hat. I am going to take that hat off and talk about this other issue. I am on the board HITSP board and Board of NCPDP. I am an informatician by training. I am also a father and the husband of a 23 year cancer survivor and also on a daily basis, I take a controlled substance because I have ADD.

So, on a lot of levels I have been thinking about this. I live in the standards world. This is where I spend time. My comments about how we could get beyond this one point of not having to jump immediately to full PKI is where these comments came from. So, let me explain a little bit about my thinking and these may be completely half-baked or they may be a stroke of brilliance in a moment. I have a lot of ideas. So, eventually I strike on something.

So, the suggestion is that we do this in an incremental basis because it is going to take us a long time to get everybody comfortable with the notion of strong asymmetric authentication. Until we get there, because the DEA does have this requirement about the wet signature, the notion that somebody did sign this. My suggestion is that we allow the e-prescribing process to happen fully, that a prescriber could use it for any substance, be it controlled or non-controlled.

The only step that would be different for the controlled substance is that they would be required to print out an electronic printout of that prescription so it is always written out. All they have to do is sign it with a wet signature and then have the patient deliver that to the pharmacy. Now, that prescription would also say on it this prescription cannot be filled without the accompanying electronic prescription. That is actually the signature filling. The electronic prescription is the one that you are using.

The electronic prescription would similarly say you can't fill this without this paper thing along with it. Now, that is the first incremental step. That is the step that still fills fulfills all your requirements. Now, I personally agree with Kevin that the electronic prescribing system as it is exists is better than what our current paper system is for controlled substances. I think it provides more veracity than what we have.

However, I understand that we may not be able to convince the DEA that they should just forget about true nonrepudiation, which I don't think that e-prescribing today can do personally without PKI But let's say that -- I would be very happy if you would just say, okay, anybody sees an e-prescribing into these systems with these fundamental -- using a password kind of level of veracity. Okay. That is all right. I don't think you will do that. So, I am suggesting that we go to a paper system or a paper copy to go along with it. So, you get all the benefits of the e-prescription, safety checks and also you get this -- I don't know how a hacker -- now maybe somebody would be smart enough to hack into the system and have five prescriptions sent to five different pharmacies at once, but then you have to be able to also get five different printed prescriptions with a wet signature on them sent out and they have to be both of those things and they have to be able to do it in a way that it couldn't be audited and noticed.

I think you -- by doing it in this way you limit the ability of people to have it in all ways. The only caveat I would suggest to that is that you would allow -- the kiting of paper prescriptions meaning that at the time of prescribing one real issue with controlled substances is that as we know you have to do it every month. You can only prescribe one month's worth of this drug. You can't do six months. At least in Maryland you can't do it and in Connecticut you couldn't do it.

So, the doctor is forced to write a new prescription every month and that is a real problem. You could do it electronically and say, okay, I am going to print out these six months prescriptions. I am going to electronically send the prescription once a month so that it is dated and, yes, the doctor still thinks this patient should get this, but the patient is not going to have to go back.

The next increment would be all those same things, but require full notification. That closes the loop. It provides an incredible amount of veracity because the -- they can say wait a minute. This does not jibe with what I thought I was doing. Maybe somebody in my office is doing something. Maybe somebody is doing something inappropriate at the pharmacy level.

The next increment could be same as above now, but now introduce PKI to the system and say that anybody can use PKI. If they do that, they can drop the paper trail. They can completely do it without paper and that is good enough. That would give doctors an actual incentive to move away from paper completely and go to PKI and strong authentication.

Then the next increment could be -- actually requiring electronic prescribing and then finally requiring e-prescribing with PKI for all controlled substances and then after that the -- require an -- with PKI for all prescribing. By doing that in incremental levels, I am not trying to put timelines on those increments, but saying that would be the basic process there. We can actually have the DEA become the hero of all this because once -- this is the solution to so many issues within health care, including the research side, including pay for performance, how do you provide that level of veracity for all of that. This is going to be the key to unlock all of that.

When I was prescribing, it was very hard for me knowing that I was taking care of my Medicaid patients, for example, and poverty is not an indicator that I am a substance abuser. It is not a proof that I am a substance abuser, but there is this level of trust issue without a very safe system where I can have confidence that when I write a prescription, that it is not being used improperly. Having electronic prescribing in the middle of this, as we have suggested can really do a lot to reinforce that and also give me confidence that I am not going to -- nobody is going to be looking over my shoulder thinking that I am supporting some abuse of practice or abusing myself.

With apologies to Dr. King -- I will paraphrase his famous words. I have a dream that someday we will judge people not on the color of their skin but in the content of their key palm.

MR. CAVERLY: Thank you.

Yes, ma'am.

MS. HANDEL: [Inaudible.]

MR. CAVERLY: Thank you.

Yes, sir.

MR. RATLIFF: Rick Ratliff with SureScripts.

I wanted to address the auditing issue and make sure that we bring that to some level of closure. I would ask you to make sure you question the panel tomorrow on this issue. But from a SureScripts perspective, we do this today. So, we do auditing in a variety of ways and for a variety of reasons. First of all, it needs to be clear that everyone of our contracts with a physician vendor or with a pharmacy gives us auditing capabilities. So, we have the ability to look at prescriptions as they are created in the physician's office with whatever system they choose to use through our network to the pharmacy. We certify that way as well, just so you know. The systems have to create a well-formatted NCPDP script message as we have discussed today. That has to be sent through the network, received by our system and then received and displayed appropriately on the pharmacy end. So, that is the way we actually certify the physician/vendor solutions.

So, the ability to look at messages and track a given prescription end to end is already in place. Now, the question is on the physician end as a prescription is created and saved, which all physician solutions give the ability for you to view that particular prescription or the prescription history if you will for a given patient, is that potentially tampered with at some point in the future? That is one thing.

The other thing is we do receive the prescription. It can come in different kinds of protocols if you will and what we do is we might translate from one protocol to the other. If we do that, we save the prescription as we receive it and that is archived. We save the prescription as we send it out to the pharmacy. That is also archived and then as you just heard from Walgreen's, you understand what they do now.

So, what you can do in an auditing situation is you can look to see if what was written, at least, was sent in to our network and then on to the pharmacy. If it was altered at the front end, then that is the opportunity for PKI and nonrepudiation, to be honest with you. So then we have the secure activity into our network to ensure that we have the archival functionality to ensure that what is saved anyway is not tampered with at any point in the future from a technology standpoint.

So, you can look at the PKI in a different way, I think, and we can talk about that if that is of interest. But I guess the key point is is we can do the auditing today. If someone was to come to us, we could actually provide the information at least within the network and we have the relationships on the ends where we can actually go in and recreate the prescription if you will. It is time stamped all the way. So, the prescription is time stamped as it goes from the physician vendor to our network and then out of our network to the pharmacy network and has provided a unique transaction I.D. So, there are those kinds of things in place.

The other thing to give -- not to help Ross out too much, but there is one interesting thing that is going on that hasn't been discussed today. It is a little different than putting the prescription into a mailbox, as the gentleman from Kaiser was describing, which is kind of what kind of functionality is or putting it on a key fob. There is some work going on with Adobe to look at a PDF-H kind of standard. So, a health care kind of standard for bar coding.

So, one of the keys as we discussed today are the standards. So, however you represent the prescription -- script format, whether you put it in the mailbox, whether you send it electronically to the pharmacy, whether you put it on a key fob or potentially if you put it -- whether you put it on to the bar code. So, the bar code is actually the NCPDP script message.

If the prescription was sent electronically to the pharmacy and a prescription was printed with the bar code and you had the same contents that were sent out in that bar code. There is a potential that you can streamline some of the efficiency back in the pharmacy by using the bar code to actually retrieve the prescription that is coming electronically, if that makes sense. So, it is a thought. It is just something that is being looked at. It is still not in place.

A couple of other things. One is the NPI was referenced earlier today. I think it is real important to make sure everyone understands that the NPI is something we are all looking at very closely but for prescription routing you need to go from the physician's location to the pharmacy and it has got to go to a specific location. For refill requests it has got to go from the pharmacy to the specific location for the physician. So, the NPI have to be location specific and if it is not, it won't work for transaction routing. So, we have got to be careful if we think about the use of the NPI.

The last thing is the fill message has been mentioned as well. We have just deployed on a pilot basis with our community pharmacy partners the ability to deliver medication history to the point of care. So, if I write a prescription for a controlled substance that goes to the pharmacy, it is dispensed at the pharmacy and let's it is Walgreen's. Then tomorrow that physician goes to review or the next visit, however you want to do this, goes to review that patient's medication history. They will be able to tell that that patient picked up that medication. If that patient happened to go to another physician and another pharmacy to try to get the same medication in a short period of time, that would be visible to that physician or actually the other physician if they are using this service.

So, there is not only the ability to transmit the prescription, so what was prescribed electronically, there is also an ability to provide or match to that the data from the pharmacies as the prescription are filled or dispensed in the pharmacies. You will hear some of this from some of the physicians with us tomorrow.

That is it.

MR. CAVERLY: Thank you.

Yes, sir.

DR. ZUCKERMAN: Alan Zuckerman, pediatrician representing American Academy of Pediatrics.

I just wanted to follow up on what Lynne Gilbertson pointed out about the need to sometimes clarify terms. There are three things I would like to review in part for the record. The first is the difference between a smart card and a thumb drive. These two gadgets here look awfully alike, but this U.S.B. smart card has a storage capacity of 32 kilobytes. There are some that are a little bit larger and the thumb drive next to it has the capacity of 256 megabytes. That is a 8,000 fold difference. What is different is both these things cost about the same amount of money, about 40 or 50 dollars. It is on the smart card they put real computer. It has a CPU chip and it has an operating system and it operates completely independently.

That is why when I go into a metro station with my fare card, which is a compact -- smart card, I can trust it to carry cash on it and to pay my metro fares. So, these are really two completely different animals.

The thumb drive, the U.S.B. disk, simply carries data. The smart card can carry a little bit of data but it is pretty precious storage. So, it is normally used just for authentication certificates, but it can do cryptographic processing that is needed for the signature and a consequence of that that we need to review our definition of the difference between a digital signature and secure message transmission. A digital signature is the property of a document that can be stored on paper with a bar code. It can be stored on a thumb drive or even on a smart card.

But what that digital signature consists of and the way it is used to audit that no changes are made is you go through the message, compute a message digest. Then you encrypt that message digest with the signer's private key. That becomes a signature -- when you go back and check the signature you recompute the message digest and you decrypt the signature value using the public key that is widely known and you compare the two and if the two match, they are perfect. If anyone alters the document, you can't just recompute the message digest and turn it into a signature value unless you know the private key and if that private key never leaves the computer on the smart card, there is no way to make -- but even at that point, you are not finished verifying the signature because you have to go through the additional step of checking the digital signature on the certificate and -- the public key -- there are dates of validity and just like a credit card, you have the -- list. You can go out on the Internet and see if that card might have been invalidated -- or lost their privileges or licensure and right to prescribe on a date when that was valid.

That brings us then to the notion of three different methods for checking whether a prescription has been altered 18 months after the fact. One approach, which is a difficult expensive one is to put digital signatures on that document and when a prescription carries a digital signature, it doesn't have to be sent immediately. It can be carried by the patient on a phone drive, on paper to a pharmacy of their choice and the pharmacy can validate that signature in time.

The other approach is the audit approach and this is a very valid and equally effective approach. Basically there you compare the message of the -- that may exist within the network and the log at the receiving end. And you look for a match. If what passed through the network or what was sent from the physician's office matches the pharmacy, you know that no changes were made.

The third and final method, which is by far and away the most dominant method is essentially blind trust in the integrity of the software in the vendor's system. This is the way things work in most electronic health record systems. It is the way things are working on our pharmacy system. Basically the vendor builds an application and says when I close the record, you can't go back and enter any inputs in the database. But it is essentially blind trust. The danger is that once you hit the signed button, the files in the database is changed but there is nothing in there to verify it.

We have the signature calculation that is -- we simply trust the -- that the design of the system -- you make a change, it is going to be filed on the transaction log and those logs are going to be saved in a way that we can trust the vendor pretty much to do it. One more thing we ought to remember is in NCPDP, there is -- exchange transactions. So, if you do have to alter the prescription of the pharmacy, what we can do in an electronic world, it is not done very often today, is send the prescription back to the physician and have the physician approve the changes and have it come back to the pharmacy. For that to happen, the physician has to be available, connected and essentially if we started using PKI, prescriptions have to be completely resigned because any change to the document -- at the receiving end completely invalidates the signature from the sender.

We do have an electronic strategy for it, but it is going to take us a few years until we get people trained and ready to use it.

MR. CAVERLY: Thank you.

Yes, sir.

MR. KAZZAZ: [Inaudible.]

MR. CAVERLY: Thank you.

Yes, sir.

MR. SCHUETH: [Inaudible.]

MR. CAVERLY: Thank you.

Yes, sir.

MR. SILVERMAN: [Inaudible.]

MR. CAVERLY: Thank you. You may approach.

Yes, sir.

MR. MACAULAY: [Inaudible.]

MR. CAVERLY: Thank you.

Yes, ma'am.

MS. SPIRO: Good afternoon. My name is Shelly Spiro and I am here representing several organizations, including -- I am also a board member of the American Society of Consultant Pharmacists. I am a co-chair of the Long Term Care Workgroup for NCPDP.

I have over 20 years of experience in long term care pharmacy. I was a long term care pharmacy manager. I also ran part of the home health care infusion pharmacy and hospice pharmacy, been very, very involved in the aspects of what takes place in long term care e-prescribing pilot. Like Lynne said, we had a lot of cheers as that first prescription actually came through electronically. From what I can tell you from experience, this is the most important thing that can happen to long term care is to really allow electronic prescribing to take place and specifically controlled substances.

Currently right now, it is hampering us as a consultant pharmacist and as a managing pharmacist of a long term care operation, I can tell you that the paperwork is horrible when it comes to controlled substances, especially in long term care. The current standards and the current regulations do not meet long term care.

MR. CAVERLY: Thank you.

MR. BUCKMAN: I will be the briefest speaker. I am Peter Buckman. [Inaudible.]

MR. CAVERLY: Thank you.

MS. REED-FOURQUET: [Inaudible.]

MR. CAVERLY: Thank you.

Yes, sir.

MR. WHITTEMORE: [Inaudible.]

MR. CAVERLY: Thank you.

Yes, sir.

MR. MAPES: We started issuing digital certificates October 1st in that program. So far I think there have been about 17,000 digital certificates issued. Those are issued to pharmacists and people working in the pharmacy, not to the pharmacy itself. So, that number doesn't represent 17,000 pharmacies. It may represent six or seven thousand pharmacies. Most of the large chains have not yet started that, but this is mostly the independent pharmacies from what we have seen.

MR. CAVERLY: Thank you.

Yes, ma'am.

MS. DENEMARK: I am Cindy Denemark, EDS, Government Solutions.

I just want to quickly reiterate two points that have been made this afternoon. I am a pharmacist, but I have been in an administrative role for almost 13 years and when I heard that the thought that DEA should consider using both an electronic and a paper prescription for Class II, the shudders just went up and down my spine. Your panelists did testify that the administrative burden of matching up that phoned in and then seven days later prescription was tough. Don't do it. Either do your electronic prescribing for your controlled substances or don't. Either trust what you have. As a dispensing pharmacist I would say that.

The other thing that I wanted to comment is on that medication history being NCPDP 8.1 transaction. I oversee a program and we put controlled substances on limited prior authorization five years ago. When the practitioners called into question why in the world I wasn't allowing the prescription to go through, I would go through claim by claim what was going on, where the other medications went from, which other physicians had wrote prescriptions for, what quantities were over the six month period of time and all I could think of is if they could see what I could see, I would prevent this phone call.

If you don't allow them to use electronic prescribing, they are not going to use the medication history as well. So, put it altogether and let them have that just for the tools.

Thank you.

MR. CAVERLY: Thank you very much to all you hearty souls, who stuck it out with us this afternoon.

On behalf of Health and Human Services and the Drug Enforcement Administration, once again, thank you. We will reconvene at 8:30 tomorrow. We will be looking at the vendors, state and law enforcement panels.

[Whereupon, at 5:30 p.m., the meeting was recessed, to reconvene at 8:30 a.m., the following morning.]