March __, 2005

Michael O. Leavitt
Secretary of Health and Human Services
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Leavitt:

The National Committee on Vital and Health Statistics (NCVHS) has been called upon by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) to develop recommendations for uniform standards to enable electronic prescribing (e-prescribing) in ambulatory care. This letter is the second set of recommendations on e-prescribing and sets forth recommendations relating to electronic signature and other important issues.

The first set of recommendations, sent September 2, 2004, addressed message format standards that provide communication protocols and data content requirements, terminologies to ensure data comparability and interoperability, identifiers for all relevant entities within the e-prescribing process and important related issues for e-prescribing.

Electronic Signature Background

Prescription Writing

Prescription-writing is a critical factor in patient care and patient safety., The National Association of Chain Drug Stores (NACDS) estimated that in 2003, .4 billion new prescriptions were written, with another 2.0 billion refills and renewals processed.[1] The Center for Information Technology Leadership (CITL) estimated that $154 billion was spent on prescription drugs. CITL also estimated that as a result of adverse drug events (ADEs), approximately $2 billion was spent in ADE-related hospitalizations and visits.[2]

Prescription writing requirements are controlled by the U.S. Department of Justice's Drug Enforcement Administration (DEA) and state boards of pharmacy. The DEA has regulatory authority over prescribing and dispensing of controlled substances. Prescribers must be authorized to prescribe controlled substances by the DEA and receive a DEA number for this purpose. Controlled substances are medications that have addiction and abuse potential. They are divided into five schedules: Schedule I substances are illegal and may not be prescribed; they are not applicable to these recommendations. Schedule II substances are highly addictive and their prescriptions must be authorized by the prescriber with a handwritten ("wet")

[1] National Association of Chain Drug Stores, Chain Pharmacy Industry Profile, 2004.
[2] Johnston, et al. The Value of Computerized Provider Order Entry in Ambulatory Settings, Center for Information Technology Leadership, 2003.

signature and the original delivered to a dispenser. Schedule III through V substances are controlled, but may be phoned or faxed to a dispenser. It is estimated that approximately 15 percent of all prescriptions written are for Schedule II – V controlled substances. Approximately 2-3 percent of prescriptions are for Schedule II controlled substances. However, it should be noted that a proportionately higher percentage of controlled substances are prescribed for the elderly and disabled[3] and these are likely to be Medicare Part D patients covered by MMA.

Through state statutes, dispensers have the ultimate authority and responsibility to assess the validity of a prescription. They do so by a variety of means. In the past, dispensers relied upon knowing the prescribers and patients, and they were able to watch for various characteristics of the prescription format and prescribing patterns. Times have changed and now patients get their prescriptions filled from many different sources. Dispensers may no longer have the close relationships with prescribers and patients. Therefore, they must now rely upon other means to validate prescription authenticity and integrity. For example, security measures included in emerging e-prescribing networks as well as access to medication claims history and return receipt processes enhance dispensers' ability to validate the authenticity of prescriptions. These electronic systems can alert dispensers to issues regarding patient safety, drug abuse or fraud and prompt dispensers to check with prescribers or take other actions.

E-Prescribing Networks

Today, most prescriptions are handwritten by prescribers onto paper. Prescribers may fax or phone these to a dispenser, or give them to the patient. The patient may take them to a dispenser or use an online or mail order service. Prescribers may use their computers to send faxes to dispensers either directly or through an e-prescribing network, and still others are sending prescription transactions to dispensers using the NCPDP SCRIPT Standard. Testimony indicated that the vast majority of experience with the NCPDP SCRIPT transactions is over e-prescribing networks.

Testimony to NCVHS indicated that prescriptions sent over e-prescribing networks offer the greatest potential to improve patient safety, enhance quality of care, and reduce costs as called for in the MMA. E-prescribing networks are switching services or value-added networks (VANs) that receive prescriptions from prescribers and route them to the designated dispenser. This routing may also involve reformatting a prescriber's transactions to enable acceptance by the dispenser's system including the translation of NCPDP data elements from older versions to newer versions if necessary. These networks can also provide prescribers and dispensers real-time access to medication history, medical history, and drug information to improve patient safety and make it easier to comply with drug formularies. More advanced e-prescribing networks can provide this information automatically with alerts, warnings or reminders to prescribers and dispensers (these capabilities are also referred to as clinical decision support). Because these e-prescribing networks are able to communicate the prescription directly to the dispenser's computer, they eliminate the need to transcribe prescriptions from paper or fax.

[3] Mike Simko, Walgreens, Testimony Feb. 1, 2005 suggested the percentage may be as high as 30 percent.

Security and Authentication in E-Prescribing Networks

Security is the broad concept of providing administrative, physical, and technical services that safeguard confidentiality, data integrity, and availability. Security services required by HIPAA include access authorization, access control, audit control, data integrity, authentication, and transmission security. HIPAA requires covered entities to conduct a risk analysis to determine the level of technology needed to satisfy these requirements, including whether encryption is necessary. The risk analysis takes into consideration reasonably anticipated threats or hazards to the security and integrity of such information and requires ongoing evaluation to respond to environmental or operational changes affecting security.

E-prescribing networks use a combination of the following security services as a means to secure transmission of electronic prescriptions:

- Credentialing upon enrollment of prescribers and dispensers in a value-added network (i.e., access authorization).
- A minimum of a user ID (i.e., access control) and password (i.e., authentication) for access to e-prescribing software.
- Use of a network-assigned electronic signature process (i.e., integrity and audit control).
- Transmission of the prescription message through a private leased line or through the Internet using a virtual private network (VPN) connection or the Secure Socket Layer (SSL) protocol (i.e., transmission security).

Electronic Signature Process

The electronic signature process used by e-prescribing networks includes: identification of the source system (i.e., prescriber’s e-prescribing system or dispenser’s pharmacy system), date and time stamp, sending system identifier, prescriber’s name, DEA number, internal “sender” ID, name of prescriber’s agent if indicated, destination dispenser name address and phone number, and destination dispenser internal “receiver” ID. Dispensers rely upon the network to verify that the sender and receiver are authorized users of the network, that none of the signature components are missing, and that the message is in the NCPDP standard format and version. See Appendix A for an illustration of Current Security and Authentication Practices in E-Prescribing Networks being used by e-prescribing networks.

The current e-prescribing transaction communication process uses a signature that is consistent with the Electronic Signatures in Global and National Commerce Act (ESIGN) definition of electronic signature that is “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.” NCVHS heard testimony from the Electronic Financial Services Council that ESIGN has been widely adopted in the financial services and other industries. E-prescribing transactions are reportedly permitted in approximately 44 states, either explicitly or by default in omitting any prohibition of this activity.[4] It is important to note that because DEA regulations require a wet signature for Schedule II controlled substances, prescriptions for such substances are either handwritten or printed from an e-prescribing device, signed, and handed to the patient. Therefore, current DEA requirements would exclude the transmission of Schedule II controlled substances over e-prescribing networks.

Use of Digital Signature in E-Prescribing

NCVHS heard testimony regarding the current use of electronic signature (i.e., authentication using one or more of password, token, or biometrics), digital signature (i.e., using encryption), and public key infrastructure (i.e., a framework of policies, protocols, and digital signature technology). (See Glossary of Terms for further reference information.) Testifiers included e-prescribing networks, software developers, providers, and standards development organizations, including ASTM International E31 Committee on Health Informatics that provides guidance on authentication for healthcare documentation.

There are several federal government and other initiatives evaluating the use of digital signatures, especially as they seek to strengthen authentication and provide nonrepudiation for messages transmitted over the “open” Internet.

One initiative was the attempt to include the requirement for a digital signature as the form of electronic signature in the proposed HIPAA security regulations.[5] However, standards for digital signatures were not retained in the final HIPAA security regulations.

Another initiative is the federal E-Authentication Initiative promoted through the Office of Management and Budget (OMB) Authentication Guidance for Federal Agencies (M-04-04). This is based on the National Institute of Standards and Technology (NIST) Electronic Authentication Guideline (SP 800-63). NCVHS sought testimony from OMB and NIST to thoroughly understand the E-Authentication Initiative. The testimony helped NCVHS understand how levels of risk are assessed based on the content of data transmission. However, the methods suggested for mitigating those risks assumed that the data transmission would be over the open Internet rather than via private leased lines or using secure protocols for transmission over the Internet, as currently employed by e-prescribing networks. NCVHS’ analysis of the OMB guidance is provided in Appendix B.

Industry Experience with PKI

Testifiers that currently use PKI in health care are experimenting with it in environments that are relatively limited in scope, and, in general, use only certain aspects of PKI. These testifiers encountered considerable overhead in their implementation of PKI and noted the lack of PKI product interoperability.

[4] Carmen A. Catizone and Eleni Z. Anagnostiadis, National Association of Boards of Pharmacy Testimony December 8, 2004

[5] Security and Electronic Signature Standards; Proposed Rule, Federal Register, Vol. 63, No. 155, Wednesday, August 12, 1998, Section 142.310(b)(2), page 43269.

Testimony from the e-prescribing networks, software developers, and prescription transaction standards developers expressed concerns that requiring use of PKI at this time would:

- Impair the ability of the e-prescribing networks to reformat or update the version of the prescription if necessary before it is sent to the dispenser.
- Create severe performance problems due to the complexity and overhead of managing PKI across disparate entities.
- Impose significant additional costs in an industry which is struggling to establish an adequate business case for e-prescribing.
- Delay the adoption of the use of e-prescribing as a result of the cost and burden to install and maintain a PKI system.
- Not provide significant incremental security protection, as testifiers indicated that there was no evidence that current security methods are inadequate relative to fraud and abuse. In fact, current security methods assist in the ability to detect fraud and abuse through return receipts and availability of prescription claim history across providers.[6]

Electronic Signature Observations and Recommended Actions

Observation 1 (Need for Coordination between HHS, DEA, and State Boards of Pharmacy to Avoid Fragmentation of E-Signature Requirements): E-prescribing offers great value. E-prescribing networks provide end-to-end security through a series of electronic pass-offs that do not entail any human intervention. The result of e-prescribing has been improvements in patient safety through more complete and accurate prescriptions, direct transmission of the prescription to a dispenser where fill status can be monitored, and elimination of the need for the dispenser to transcribe, often illegible, handwritten fax or paper prescriptions. E-prescribing transaction processes can support return receipts sent from dispensers to prescribers that also contribute to identification of potential fraud and abuse, should a prescriber receive receipts for prescriptions not written.

DEA through its statutory authority under the Controlled Substances Act requires that prescriptions written for Schedule II controlled substances be delivered to the dispenser in original form with a wet signature. Prescriptions for Schedule III-V substances may be faxed or communicated orally to a dispenser. The DEA has not made a ruling regarding the security requirements for e-prescribing of controlled substances. Some states, however, have established restrictions on e-prescribing. As a result, e-prescribing networks do not provide services in those states.

E-prescribing networks and software developers expressed strong concern that the DEA may require PKI for prescriptions of Schedule II, or II-V controlled substances. Schedule II-V controlled substances represent only about fifteen percent of all prescriptions. The result of having to deal with two or three different processes would eliminate the marginal business case that now exists for networks and developers to make e-prescribing for controlled substances available.

[6] Richard Brook, ProxyMed, Testimony indicated that over 19 million transactions have been handled without a security incident.

It is clear that the security of e-prescribing networks accomplishes more security than traditional paper, fax, or phone, which are prone to abuse given today's copier, fax, and telephony technology. E-prescribing transactions for non-controlled and Schedule III-V controlled substances currently are conducted in compliance with HIPAA's security regulations and include dispenser validation through callback to prescriber for prescriptions written for Schedule III-V controlled substances. Today's e-prescribing networks use several important security features, including credentialing prescribers and dispensers, trading partner agreements to grant access to the networks, and protocols to secure transmission and provide authenticity and integrity to electronic prescriptions. Testimony indicated that there is no evidence that these security measures have been inadequate to secure electronic prescriptions.

Recommended Action 1.1: HHS, DEA, and state boards of pharmacy should recognize current e-prescribing network compliance with HIPAA security and authentication requirements, along with dispenser validation, as the basis for securing prescriptions over e-prescribing networks. Different requirements may be needed for transmission of electronic prescriptions that do not go through such networks.

Deleted: electronic

Recommended Action 1.2: HHS and DOJ should work together to reconcile different agency mission requirements in a manner that will address DEA needs for adequate security of prescriptions for all controlled substances, without seriously impairing the growth of e-prescribing in support of patient safety as mandated by MMA.

Observation 2 (Need for Research to Address Future Security Risks): Because there may be a greater need to send prescriptions over the open Internet in the future or for enhanced security of prescriptions for Schedule II controlled substances, there may come to be greater demand for improved authentication, message integrity, and nonrepudiation services. Although PKI and other forms of digital signature are available, testimony indicated that currently these technologies are costly and impair interoperability for e-prescribing functions. Therefore, it is important to plan for evaluating the feasibility of PKI or other forms of digital signature for use in e-prescribing as these technologies mature. Reference information regarding electronic signature, digital signature, and PKI are available from ASTM International and ISO.

Recommended Action 2.1: HHS should evaluate emerging technologies such as biometrics, digital signature, and PKI for higher assurance authentication, message integrity, and non-repudiation in a research agenda for e-prescribing and all other aspects of health information technology.

Deleted:

Observations and Recommendations Relative to Progress on Previous Recommendations

Observation 3 (Formulary and Benefit Coverage Message Standard) As noted in the NCVHS recommendation letter of September 2, 2004, NCVHS has monitored the progress of NCPDP as it develops the Formulary and Benefit Coverage Message Standard. NCPDP has reported that a formulary and benefit message standard will be submitted for approval to

NCPDP at its March 2005 work group meetings and, pending the balloting process, the NCPDP board of trustees could approve the standard as early as late spring 2005. The formulary and benefit message standard includes formulary status lists, formulary alternatives lists, benefit coverage lists, benefit copay lists, and a cross-reference file of user-recognizable health plan product name to identifiers used for the formulary, alternative, coverage, and copay lists.

Recommended Action 3.1: NCVHS will continue to monitor the progress of the development of the NCPDP Formulary and Benefit Coverage Message Standard and will report any further recommendations to HHS based upon this progress.

Observation 4 (Medication History Messages from Payer/PBM to Prescriber) As noted in the NCVHS recommendation letter of September 2, 2004, NCVHS has monitored the progress of NCPDP as it develops Medication History Message Standards. NCPDP has reported that a data element request form in support of medication history messaging was submitted to the NCPDP and is currently being balloted. Pending the balloting process, the NCPDP board of trustees could approve the standard as early as late spring 2005.

Recommended Action 4.1: NCVHS will continue to monitor the progress of the development of the NCPDP Medication History Message Standards and will report any further recommendations to HHS based upon this progress.

Observation 5 (NCPDP Fill Status Notification Standard) The industry does not have adequate experience with the NCPDP SCRIPT Fill Status Notification Standard to make it a foundation standard for e-prescribing. NCPDP has developed guidance on implementation and operational matters relative to consistent utilization by prescribers and dispensers for the fill status notification transactions. NCPDP expects that board of trustee approval for this guidance will be provided in April/May 2005.

Recommended Action 5.1: HHS should include the fill status notification function of the NCPDP SCRIPT Standard in the 2006 pilot tests, consistent with NCVHS recommendations of September 2, 2004.

Observation 6 (Structured and Codified SIG) NCPDP is gathering data, defining scope and management, and drafting operating assumptions relative to structured and codified SIGs (patient instructions). It is working with HL7 to draft implementation guides and refine data elements and code sets. NCPDP expects to release a proposed standard for coding and testing a structured and codified SIG in summer 2005.

NCVHS further notes that standard units of measure, identified as a topic for further consideration in its September 2, 2004 letter, is included in the work of NCPDP and HL7 as they define the structured and codified SIG.

Recommended Action 6.1: HHS should include evaluation of structured and codified SIGs in the 2006 pilot tests, consistent with NCVHS recommendations of September 2, 2004.

Observation 7 (Clinical Drug Terminology, Drug Labeling, Drug Listing, and Standard Codes for Orderable Items) NCPCP testified that it requested from NLM examples of RxNorm to NDC mapping. NLM has accepted an invitation to speak on RxNorm during the NCPDP annual conference in March 2005 so that further work may ensue.

NCVHS also heard testimony from NLM that several issues are being addressed, including maintenance of RxNorm outside of the UMLS environment, elimination of code changes and handling obsolete drugs, frequency of updates, and enhancing and stabilizing staff support. A study has been conducted which has determined that the current NCPDP SCRIPT Standard has too short a character-limit field for RxNorm codes and that the ability to handle exceptions must be accommodated. NLM is adding NDC codes as available from FDA, and starting to link brand names (although completing this will depend on availability of information from FDA). NLM is also starting to include consistent names for orderable items associated with medications (such as test strips, oral contraceptive dispensers, etc.) and will start with coverage for such items that are reimbursable under Medicare Part D. NLM expects to start receiving structured product labels (SPL) from the FDA later this year for incorporation into the DailyMed. NLM indicated that the FDA estimates that full implementation of the rule will take seven years to complete.

Recommended Action 7.1: HHS should include in the e-prescribing pilots evaluation of the ability for RxNorm to be translated from the prescriber's system into an NDC at the dispenser's system, consistent with NCVHS recommendations of September 2, 2004.

Recommended Action 7.2: HHS should take immediate steps to accelerate the promulgation and implementation of FDA's Drug Listing rule in order to make the inclusion of RxNorm in the 2006 pilot tests as comprehensive as possible. This is necessary to achieve the patient safety objectives of MMA.

Observation 8 (Prior Authorization Messages) NCPDP reported that an industry task group is drafting flows of the medication prior authorization process and identifying where standards exist and where there are gaps. It has identified that attachments being developed for claims may be leveraged and added to in order to be used for prior authorization. NCPDP will coordinate with HL7 if there is a need to support an attachment booklet for the purpose of medication prior authorization attachments. NCPDP indicates that additional research is taking place on structuring prior authorization messages.

Recommended Action 8.1: HHS should support the standards development organizations (NCPDP, HL7, and ASC X12) in their efforts to incorporate functionality for real-time prior authorization messages for medications in the ASC X12N 278 Health Care Services Review Standard and ASC X12N 275 Claims Attachment Standard.

Observation 9 (Coordination and Interoperability of Prescription Message Standards) HL7 and NCPDP collaboration is actively underway in support of the ability to map the data in HL7 order entry messages generated within a healthcare organization to the data and format required by NCPDP SCRIPT messages when transmitted to an external dispenser (e.g., retail or community pharmacy). The e-prescribing NPRM solicited comments on whether Part D plans should be required to use the standards for e-prescribing transactions within a “closed” enterprise (e.g., staff model HMO). NCVHS, however, believes the issue is broader than simply accommodating e-prescribing transactions within “closed” versus “open” enterprises. NCVHS believes that the coordination of data elements in prescription message standards would enhance adoption of e-prescribing overall.

Recommended Action 9.1: HHS should financially support the acceleration of initial and ongoing maintenance coordination activities between HL7 and NCPDP for electronic medication ordering and prescribing.

Recommended Action 9.2: HHS should permit the use of HL7 order entry messages to pharmacies within the same enterprise. If the message is being transmitted to a dispenser outside of the enterprise, HHS should require that it be converted to NCPDP SCRIPT. This is consistent with NCVHS recommendations of September 2, 2004.

Observations and Recommendations Relative to Privacy of E-Prescribing

Observation 10 (Privacy Issues Relative to E-Prescribing) NCVHS Subcommittee on Privacy and Confidentiality held a hearing on privacy issues related to e-prescribing on November 18, 2004. The Subcommittee heard testimony from industry experts and consumers. In general, witnesses noted that e-prescribing regulations will require patient education regarding their rights, patient access to privacy and security policies, and consumer-friendly communications.

Privacy guidance for e-prescribing is provided through applicable state and federal laws and regulations. For example, it is not clear whether state laws restricting certain electronic health record communications (e.g., related to HIV status) without express consent would be preempted by MMA. Similarly, the federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations require express consent for the use and disclosure of alcohol and drug abuse patient records that are maintained in connection with the performance of any federally assisted alcohol and drug abuse program. Any e-prescribing regulations must consider these other health records laws.

The main privacy issue that needs to be resolved in an e-prescribing regulation is what rights consumers should have to limit access to their prescription records, especially for medications related to sensitive health matters, such as mental health, substance abuse, and HIV/AIDS. The same issue of balancing the privacy interest in consumer control with the interests of health care quality and efficiency is central to the National Health Information Network (NHIN). NCVHS will be holding a series of hearings on privacy and confidentiality under the NHIN beginning in February 2005.

Recommended Action 10.1: HHS should identify and address privacy issues that arise during the 2006 pilots of e-prescribing. Special attention should be placed on issues regarding individuals’ rights to request restrictions on access to their prescription records.

Other Standards and Important Related Issues

In its letter of September 2, 2004, NCVHS identified a number of other message format, terminology, and identifier standards and important related issues associated with e-prescribing for which further recommendations may be addressed.

A directory that would identify prescribers and dispenser that are able to accept e-prescribing transactions was identified. It has been learned that e-prescribing networks are using a standard which is based on NCPDP SCRIPT. The industry is working through NCPDP to bring this forward as a standard. NCVHS does not believe any further action on such a directory is necessary.

NCVHS was apprised of the report on Clinical Decision Support for E-Prescribing, prepared by the Joint Clinical Decision Support Workgroup, authored by Teich et al. The white paper identifies: (1) benefits of clinical decision support, (2) barriers to widespread adoption of clinical decision support, (3) basic and advanced clinical decision support features and elements that might be required over time, (4) structures, standards, and other enablers required for clinical decision support in e-prescribing, and (5) incentives to accelerate adoption of clinical decision support in e-prescribing. NCVHS notes that several of the recommendations in this report complement those included in the NCVHS letter of September 2, 2004, especially with respect to the use of RxNorm to support clinical decision making in e-prescribing.

Several other issues have been covered in this letter. Issues that remain open for potential further deliberation include:

- Codification of allergens, drug interactions, and other adverse reactions to drugs.
- Incorporation of indications for drug therapy into e-prescribing messages.
- Methods for patient identification for e-prescribing.
- Use of the National Health Plan ID for e-prescribing.
- Formulary identifier.
- Exchange of medication history among all participants in the e-prescribing process.
- Exchange of medical history within the e-prescribing process.

.

NCVHS is pleased that its recommendations of September 2, 2004 have been addressed in the e-prescribing NPRM, and wishes to thank you for the opportunity to make these additional recommendations.

Sincerely yours,

Simon P. Cohn, MD, MPH
Chair, National Committee on Vital and Health Statistics

Appendices

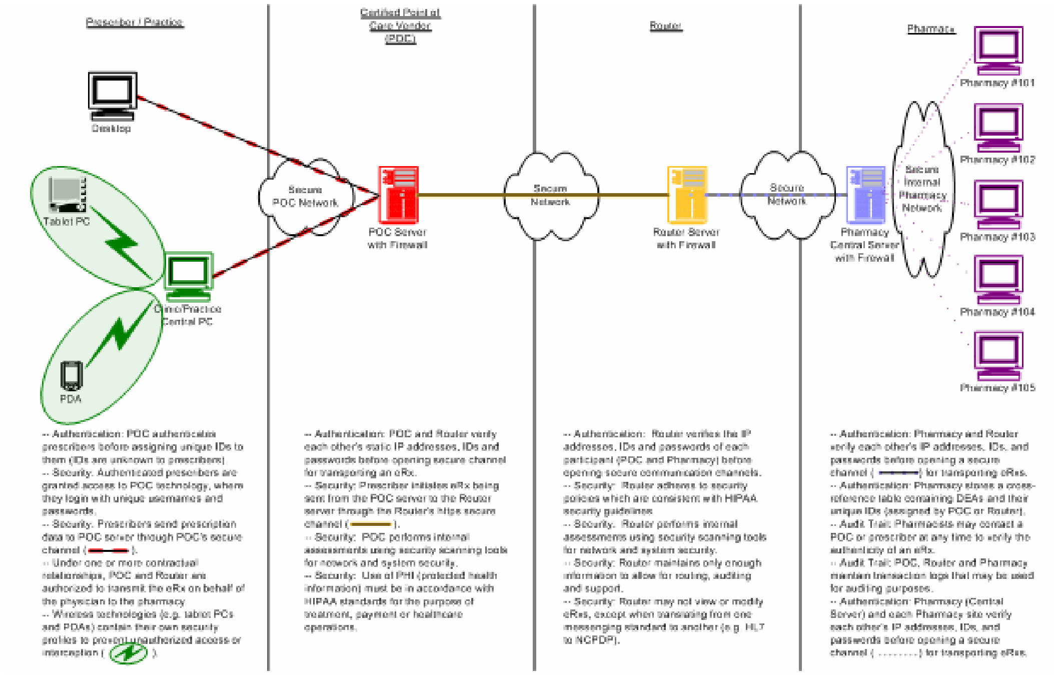
A. Current Security and Authentication Practices in E-Prescribing Networks

B. NCVHS Analysis of E-Authentication Initiative Guidance

C. Glossary of Terms

D. List of Testifiers

Appendix A. Current Security and Authentication Practices in E-Prescribing Networks



-- Authentication: POC authenticates prescribers before assigning unique IDs to them (IDs are unknown to prescribers)
-- Security: Authenticated prescribers are granted access to POC technology, where they login with unique usernames and passwords.
-- Security: Prescribers send prescription data to POC server through POC's secure channel (▬ ▬).
-- Under one or more contractual relationships, POC and Router are authorized to transmit the eRx on behalf of the physician to the pharmacy.
-- Wireless technologies (e.g. tablet PCs and PDAs) contain their own security profiles to prevent unauthorized access or interception (⚡).

-- Authentication: POC and Router verify each other's static IP addresses, IDs and passwords before opening secure channel for transporting an eRx.
-- Security: Prescriber initiates eRx being sent from the POC server to the Router server through the Router's https secure channel (▬▬).
-- Security: POC performs internal assessments using security scanning tools for network and system security.
-- Security: Use of PHI (protected health information) must be in accordance with HIPAA standards for the purpose of treatment, payment or healthcare operations.

-- Authentication: Router verifies the IP addresses, IDs and passwords of each participant (POC and Pharmacy) before opening secure communication channels.
-- Security: Router adheres to security policies which are consistent with HIPAA security guidelines.
-- Security: Router performs internal assessments using security scanning tools for network and system security.
-- Security: Router maintains only enough information to allow for routing, auditing and support.
-- Security: Router may not view or modify eRxs, except when translating from one messenging standard to another (e.g. HL7 to NCPDP).

-- Authentication: Pharmacy and Router verify each other's IP addresses, IDs, and passwords before opening a secure channel (▬ ▬ ▬) for transporting eRxs.
-- Authentication: Pharmacy stores a cross-reference table containing DEAs and their unique IDs (assigned by POC or Router).
-- Audit Trail: Pharmacists may contact a POC or prescriber at any time to verify the authenticity of an eRx.
-- Audit Trail: POC, Router and Pharmacy maintain transaction logs that may be used for auditing purposes.
-- Authentication: Pharmacy (Central Server) and each Pharmacy site verify each other's IP addresses, IDs, and passwords before opening a secure channel (..........) for transporting eRxs.

National Council for Prescription Drug Programs, 2004

Appendix B. NCVHS Analysis of E-Authentication Initiative Guidance

The E-Authentication Initiative is setting the standards for the identity proofing of individuals and businesses, based on risk of online services used, to ensure public trust in the security of information exchanged over the Internet. These standards assume a baseline of the open Internet and provide measures to enhance proof of identity at various risk levels within that construct. The Office of Management and Budget (OMB) Authentication Guidance for Federal Agencies (M-04-04) established four authentication assurance levels, based on NIST's Electronic Authentication Guideline (SP 800-63).[7]

Authentication Assurance Levels
1 = Little or no confidence in asserted identity (e.g., self-identified user/password)
2 = Some confidence in asserted identity (e.g., PIN/password)
3 = High confidence in asserted identity (e.g., digital certificate)
4 = Very high confidence in the asserted identity (e.g., Smart Card)

OMB has also developed assurance level impact profiles for six potential impact categories for authentication errors:

Assurance Level Impact Profiles				
Potential Impact Categories for Authentication Errors	**Authentication Assurance Levels**			
	1	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Based on the guidance provided in the Authentication Assurance Levels and Assurance Level Impact Profiles, if the potential impact for an authentication error in sending a prescription from a prescriber to a dispenser is considered to be "personal safety" (i.e., patient safety), then the OMB would place the risk of authentication error occurring over the open Internet at level 3 or 4, suggesting the need for "high confidence in asserted identity" (using, e.g., digital certificate) or "very high confidence" (using, e.g., a smart card). If the impact is considered as being "unauthorized release of sensitive information" or "civil or criminal violations," the OMB would place the risk of authentication error occurring over the open Internet at level 2 or high, suggesting that there must be at a minimum "some confidence in asserted identity," such as a personal identification number (PIN) or password.

[7] Jeanette Thornton, OMB Testimony to NCVHS, December 8, 2004, E-Signatures: The Federal Perspective

NCVHS testimony described several security measures being used by the current e-prescribing networks to secure the transmission of e-prescribing transactions, including credentialing to be provided access, authentication of both prescribers and dispensers by a minimum of a strong password, trading partner agreements to establish end-to-end security requirements, and use of a private leased line or security protocols establishing a virtual private network (VPN) or other secure channel service for transmission over the Internet. NCVHS believes that consistent application of these best practice security measures would bear no more risk than today's fax or phone prescriptions. In addition to the level of security afforded by these practices, testimony also provided evidence that availability of prescription claims history and acknowledgement of prescription receipt affords greater opportunity to monitor for fraud and abuse, overdosing, and other medical contraindications.

Appendix C. Glossary of Terms

Authentication – NIST SP 800-63 defines authentication as the process of establishing confidence in user identities. HIPAA Security Rule defines authentication as procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Certificate authority (CA) – NIST SP 800-63 defines certification authority as a trusted entity that issues and revokes public key certificates.

Credential – NIST SP 800-63 defines credential as an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. E-prescribing networks providing testimony to NCVHS on December 8, 2004, used the term credentialing to describe a procedure of registering prescribers and dispensers into their systems and validating their DEA status.

Data integrity – NIST SP 800-63 defines data integrity as the property that data has not been altered by an unauthorized entity.

Digital certificate – (a definition for digital certificate is not included in NIST SP 800-63) This was defined by Kepa Zubeldia in testimony to NCVHS on December 8, 2004, as a particular expression of one kind of digital signature.

Digital signature – NIST SP 800-63 defines digital signature as an asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. (Digital signature may be a component of a broader infrastructure called public key infrastructure [PKI].)

Electronic signature – ESIGN defines electronic signature as an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by the person with the intent to sign the record.

Encryption – HIPAA Security Rule defines encryption as the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

ESIGN – Electronic Signatures in Global and National Commerce Act, June 30, 2000; modeled after the Uniform Electronic Transactions Act (**UETA**) proposed by the National Conference of Commissioners on Uniform State Laws, July 1999.

Password – NIST SP 800-63 defines password as a secret that a claimant memorizes and uses to authenticate his or her identity. They are typically character strings.

Personal Identification Number (PIN) – NIST SP 800-63 distinguishes PIN from password as a password consisting only of decimal digits.

Public Key Infrastructure (PKI) – (several references) is an ISO authentication framework that uses public key cryptography and the X.509 standard protocol to enable authentication to happen across different networks and the Internet. The framework includes digital certificates, a certificate authority, registration authorities, policies and procedures, various key management processes, certificate revocation process, nonrepudiation support, time stamping, directory protocols, security measures, and cross-certification communication protocols.

Security – HIPAA Security Rule defines security as measures encompassing all of the administrative, physical, and technical safeguards in an information system.

Token – NIST SP 800-63 defines token as something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.

Appendix D. List of Testifiers