E-Authentication Risk Assessment for

Electronic Prescriptions for Controlled Substances

RIN 1117-AA61, Docket No. DEA-218

I. Introduction

The Office of Management and Budget's E-Authentication Guidance for Federal Agencies (M-04-04) requires agencies to ensure that electronic transactions provide for authentication processes that provide the appropriate level of assurance.[1] Assurance is the degree of confidence in the vetting process used to establish the identity of an individual to whom a credential was issued, the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued, and the degree of confidence that a message when sent is secure. M-04-04 describes four levels of identity assurance for electronic transactions and provides standards to be used to determine the level of risk associated with a transaction and, therefore, the level of assurance needed. OMB established four levels of assurance:

Assurance Level 1: Little or no confidence in the asserted identity's validity.

Assurance Level 2: Some confidence in the asserted identity's validity.

Assurance Level 3: High confidence in the asserted identity's validity.

Assurance Level 4: Very high confidence in the asserted identity's validity.

M-04-04 states that to determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks and identify measures to minimize their

[1] Office of Management and Budget. "E-Authentication Guidance for Federal Agencies" M-04-04. December 16, 2003.

impact. The document states that the risk from an authentication error is a function of two factors: (a) potential harm or impact and (b) the likelihood of such harm or impact. The National Institute of Standards and Technology (NIST) has published Special Publication (SP) 800-63-1, which supplements M-04-04, and provides detailed guidance for actions needed to reach each of the assurance levels.[2]

As defined in M-04-04, authentication focuses on confirming a person's identity, based on the reliability of that person's credential. Authorization focuses on identifying the person's user permissions. NIST SP 800-63-1 defines the process in more detail. NIST SP 800-63-1 defines the steps necessary to reach each assurance level for identity proofing that precedes the issuance of the credential; the use of credential once issued; and the transmission of any document "signed" with the credential. In plain language, an e-authentication risk assessment considers two issues:

- How important is it to know that the person who is issued a credential is, in fact, the person whose identity is associated with the credential.
- How important is it to be certain that the person who uses the credential, once it is issued, is the person to whom it was issued.

This risk assessment addresses the level of assurance needed to allow the use of electronic prescriptions for controlled substances. Section II of the document provides background on the statutory requirements for control of certain drugs and the regulatory program that implements the statutory mandates. Section III discusses the reasons for moving to allow electronic prescriptions for controlled substances. Section IV discusses existing electronic prescription applications. Section V discusses the concerns that DEA has with existing applications that have shaped its decisions on the requirements needed to ensure that electronic prescribing of controlled substances does not become a means

[2] National Institute of Standards and Technology. Special Publication 800-63-1, Draft Electronic Authentication Guideline, December 8, 2008.

for increased diversion and drug abuse. Section VI summarizes the assessment that DEA conducted for the interim final rule.

II. Background

In the United States, controlled substances are regulated under the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 801-971), often referred to as the Controlled Substances Act (CSA).[3] Congress assigned responsibility for enforcement of the Act to the Attorney General, and authorized the Attorney General to promulgate and enforce any rules, regulations, and procedures which he may deem necessary and appropriate for the efficient execution of his functions under the Act (21 U.S.C. 871(b)). Congress also specifically authorized the Attorney General to promulgate rules and regulations relating to the registration and control of the manufacture, distribution, and dispensing of controlled substances (21 U.S.C. 821). The Attorney General has delegated these functions to the Administrator of the Drug Enforcement Administration (DEA) (28 CFR 0.100).

DEA publishes the regulations governing controlled substances in Title 21 of the Code of Federal Regulations (CFR), Parts 1300 to 1316. Consistent with the text and purposes of the CSA, the DEA regulations are designed to prevent the diversion of controlled substances into illicit channels while allowing for the production and distribution of an adequate supply of these substances for legitimate medical, scientific, research, and industrial purposes. The Act and regulations achieve this goal by, among

[3] To be precise, the Comprehensive Drug Abuse Prevention and Control Act includes both the CSA (21 U.S.C. 801-904) and the Controlled Substances Import and Export Act (CSIEA) (21 U.S.C. 951-971). However, for simplicity, the CSA and CSIEA are often collectively referred to as the Controlled Substances Act (CSA).

other things, mandating a "closed system" of distribution of controlled substances, as described below.

Framework of the Controlled Substances Act

In enacting the CSA, Congress sought to control the diversion of pharmaceutical controlled substances into illicit markets by establishing a "closed system" of drug distribution governing the legitimate handlers of controlled substances. H. Rep. No. 91-1444, reprinted in 1970 U.S.C.C.A.N. 4566, 4571-72. Under this closed system, all legitimate manufacturers, distributors, and dispensers of controlled substances must register with DEA and maintain strict accounting for all controlled substance transactions (Id.).

Controlled substances are drugs and other substances that have a potential for abuse and psychological and physical dependence; these include opioids, stimulants, depressants, hallucinogens, anabolic steroids, and drugs that are immediate precursors of these classes of substances. DEA lists controlled substances in 21 CFR part 1308. The substances are divided into five schedules: Schedule I substances have a high potential for abuse and have no currently accepted medical use in treatment in the United States. These substances may only be used for research, chemical analysis, or manufacture of other drugs. Schedule II – V substances have currently accepted medical uses in the United States, but also have potential for abuse and psychological and physical dependence that necessitate control of the substances under the CSA. Virtually all Schedule II-V controlled substances are available only pursuant to a prescription issued by a practitioner licensed by the State and registered with DEA to dispense the

substances. Overall, controlled substances constitute between 11 percent and 12 percent of all prescriptions written in the United States.

Current Requirements for Prescriptions

The CSA requires that, except in limited emergency circumstances, a pharmacist may only dispense a Schedule II controlled substance pursuant to a "written prescription" from a practitioner (21 U.S.C. 829(a)). For Schedule III and IV controlled substances, a pharmacist may dispense the controlled substance pursuant to a written or oral prescription from a practitioner (21 U.S.C. 829(b)). Every written prescription must be signed by the practitioner in the same way the practitioner would sign a check or other legal document, e.g., "John H. Smith" or "J.H. Smith" (21 CFR 1306.05). A prescription for a controlled substance may be issued only by an individual practitioner who is authorized to prescribe controlled substances by the State in which he is licensed to practice and is registered, or exempted from registration, with DEA (21 U.S.C. 822, 823). To be valid, a prescription must be written for a legitimate medical purpose by an individual practitioner acting in the usual course of professional practice; a corresponding responsibility rests with the pharmacist who fills the prescription (21 CFR 1306.04). An order purporting to be a prescription issued not in the usual course of professional treatment is not a prescription within the meaning and intent of the CSA, and the person knowingly filling such a purported prescription, as well as the person issuing it, is subject to the penalties provided for violations of the provisions of law relating to controlled substances.

Longstanding DEA regulations specify that each controlled substance prescription contain certain information, including the practitioner's manual signature (21 CFR

1306.05). This manual signature affixed to the prescription by the practitioner serves as formal attestation by the practitioner that the prescription has been written for a legitimate medical purpose and affirms the practitioner's intent to authorize the dispensing of a controlled substance to the patient under the practitioner's medical supervision. The prescribing practitioner is responsible in case the prescription does not conform in all essential respects to the law and regulations. Further, a corresponding liability rests upon the pharmacist who fills a prescription not prepared in the form prescribed by DEA regulations (21 CFR 1306.05).

A prescription for a controlled substance may be filled only by a pharmacist acting in the usual course of professional practice who is employed in a DEA-registered pharmacy (21 CFR 1306.06). Except under limited circumstances, a pharmacist may dispense a Schedule II controlled substance only upon receipt of the original written prescription manually signed by the practitioner (21 U.S.C. 829, 21 CFR 1306.11). A pharmacist may dispense a Schedule III or IV controlled substance only pursuant to a written and manually signed prescription from an individual practitioner, which is presented directly or transmitted via facsimile to the pharmacist, or an oral prescription, which the pharmacist promptly reduces to writing containing all of the information required to be in a prescription, except the signature of the practitioner (21 U.S.C. 829, 21 CFR 1306.21).

Every prescription for a controlled substance must be initialed and dated by the pharmacist filling the prescription. Under certain circumstances specified in the DEA regulations, pharmacists are required to note specific information regarding dispensing on

the prescription or recorded in a separate document referencing the prescription before the prescription is placed in the pharmacy's prescription records.

The CSA and DEA regulations require the registered pharmacy to maintain records of each dispensing for two years from the date of dispensing of the controlled substance (21 U.S.C. 827(a), 21 CFR 1304.04). However, many States require that these records be maintained for longer periods of time. These records must be made available for inspection and copying by authorized employees of DEA (21 U.S.C. 827(b)). Thus, the nature of this system of records is that the prescribing practitioner creates the prescription, but the dispensing pharmacy retains the record.

The signature requirement for written prescriptions for controlled substances provides DEA with reliable evidence needed to enforce the CSA in administrative, civil, and criminal legal proceedings. In criminal proceedings for violations of the CSA, the Government must prove the violation beyond a reasonable doubt. As the agency responsible for monitoring compliance with the regulatory requirements of the CSA, it is essential that DEA have the ability to determine whether a given prescription for a controlled substance was, in fact, signed by the practitioner whose name appears on the prescription. It is likewise essential that DEA have the ability to determine that a prescription that has been filled by a pharmacy was not altered after it was prepared by the practitioner. Further, because DEA and other law enforcement agencies rely on the records of these prescriptions in the conduct of investigations, they must also know that the prescription has not been altered after receipt by the pharmacy.

The elements of the prescription that identify the practitioner (the practitioner's name, address, DEA registration number, and signature) also serve to enable the

pharmacy to authenticate the prescription. If a pharmacy is unfamiliar with the practitioner, it can use the registration number to verify the identity of the practitioner through publicly available records. Those same records would indicate to the pharmacy whether the practitioner has the authority to prescribe the schedule of the controlled substance in question.

Requiring that the original documents be maintained in paper form serves to support both the accuracy and integrity of each record and, thus, the accuracy and integrity of the system of records as a whole. The availability of the original written and manually signed prescription provides a level of document integrity and provides physical evidence if the record has been altered: alterations of a hard-copy record are usually apparent upon close examination. A forensic examination of a prescription can prove that a practitioner signed it or, equally important, that the practitioner did not sign it. The maintenance of the paper record at a pharmacy also ensures that State and local law enforcement agencies have access to records they need for investigations. In addition, there will be a limited number of pharmacy employees who will have annotated the record and can testify that the prescription is, in fact, the prescription they received and dispensed.

III. Need for an Electronic System

Many parties in the healthcare industry are encouraging the adoption of electronic prescriptions because such prescriptions have the potential to improve patient safety by reducing medical errors that arise from misread or misunderstood prescriptions. They also have the potential to control costs by ensuring that more drugs prescribed are covered by formularies or are generic versions.

In 2003, Congress enacted the Medicare Prescription Drug Improvement and Modernization Act (Pub. L. 108-173) (MMA). Section 1860D-4(e) (codified at 42 U.S.C. 1395w-104(e)) contains the requirement that the electronic transmission of prescriptions and prescription-related information for covered Part D drugs prescribed for Part D eligible individuals comply with final uniform standards adopted by the Secretary of the Department of Health and Human Services (HHS).[4] The standard focuses solely on the format for the transmitted information, not with the process of creating the prescription, the content of the prescription, or the maintenance of the record by the pharmacy.

Providers (including dispensers) maintaining prescription records and electronic transmissions involving protected health information are also subject to the Health Insurance Portability and Accountability Act (HIPAA), which establishes certain protections for personal health information. Health Plans, Health Care Clearinghouses, and covered Health Care Providers that are involved in the transmission of prescriptions must comply with HIPAA standards, which are codified at 45 CFR part 164. Any provider that is party to the creation, transmission, and storage of prescriptions therefore must meet HIPAA's standards to ensure that the information is protected and not revealed to persons who are not authorized to see it. HIPAA does not address issues related to who may create or alter health records.

On February 17, 2009, the President signed the American Recovery and Reinvestment Act of 2009 (Recovery Act) (Pub. L. 111-5, 123 STAT. 115). The Recovery Act authorizes bonus payments for eligible professionals and hospitals

[4] HHS adopted a rule on the transmission standard for electronic prescriptions in November 2005 (70 FR 67593, November 7, 2005) and revised it on June 23, 2006 (71 FR 36023), November 27, 2007 (72 FR 66405); April 7, 2008 (73 FR 18941), and November 19, 2008 (73 FR 69938).

participating in Medicare or Medicaid if they can demonstrate to the Secretary of HHS that they are "meaningful EHR users" as defined by the Act and its implementing regulations. These bonus payments will begin in 2011.

IV. Current State of Electronic Prescription Applications

To understand the risks and DEA's approach it is necessary to understand the current state of electronic prescribing and pharmacy systems. Electronic prescription applications and electronic health record (EHR) applications have been available for a number of years although they are not yet widely used. Electronic prescription applications may be stand-alone applications or they may be incorporated into EHR applications. Either type of application may be installed on a practitioner's computers or may be an Internet-based application, where the practitioner accesses the application through the Internet; for these applications, the application service provider (ASP) retains the records on its servers.

Practitioners obtain electronic prescription and EHR applications from application providers. In the case of at least some ASPs, practitioners may enroll on line. ASPs may ask for DEA registration and State authorization numbers, although they are not required to do so; the degree to which these are verified is at the discretion of the application provider. Similarly, application providers that sell installed applications may or may not determine whether the practitioners have valid State and DEA authorizations. Where a medical practice purchases an application or service, providers may or may not obtain this information for all practitioners in the practice.

Access to an application is usually by means of a user ID and/or a password. At one time, some application service providers indicated that everyone in a practice had the

same password although that is unlikely to be usual practice. The Certification Commission for Healthcare Information Technology (CCHIT) requires that an application have logical access controls and audit trails to gain certification, but there is no requirement that these functions be used. More than half the electronic prescription application providers certified with SureScripts/RxHub (for transmission) are not certified with CCHIT.

Even if there are logical access controls, they may not limit who can perform functions such as approving a prescription or signing it. At medical practices and even more so at hospitals and clinics, many staff members may use the same computers. The person who logged onto the application may not be the person entering prescription information later or the person who transmits the prescription. Some applications have internal audit trail functions, but whether these are active and reviewed is at the practitioner's discretion. In addition, with multiple people using computers, it is unclear that the audit trail can accurately identify who is performing actions. Except for Federal applications that use digital certificates, none of the applications transmit any indication that a prescription was actually signed.

Except in closed healthcare systems (where the practitioners and pharmacy are part of the same organization), electronic prescriptions are transmitted through a series of three to five routers and intermediaries before reaching the pharmacy. The pharmacy application imports that prescription data directly into its database. The pharmacy industry comments on the NPRM indicate that most pharmacy applications have internal audit trail functions to record when records are annotated or altered. Whether these audit

trails are reviewed and retained is at the pharmacy's discretion. There are no standards that apply to pharmacy applications.

V. DEA Issues

DEA supports the adoption of electronic prescriptions for controlled substances in a manner that will minimize the risk of diversion. In the absence of appropriate controls, allowing electronic prescriptions for controlled substances could exacerbate the increasing problem of prescription controlled substance abuse in the United States. The 2008 NSDUH[5] estimated that 6.2 million persons were current users (i.e., in the past 30 days) of psychotherapeutic drugs--pain relievers, anti-anxiety medications, stimulants, and sedatives--taken nonmedically. This represents 2.5 percent of the population aged 12 or older. From 2002 to 2008, there was an increase among young adults aged 18 to 25 in the rate of current non-medical use of prescription pain relievers, from 4.1 percent to 4.6 percent. The survey found that about 52 million people 12 and older had used prescription drugs for non-medical reasons; about 35 million of these had used prescription painkillers non-medically in their lifetime.

The consequences of prescription drug abuse are seen in the data collected by the Substance Abuse and Mental Health Services Administration on emergency room visits. In the latest data, Drug Abuse Warning Network (DAWN), 2006: National Estimates of Drug-Related Emergency Department Visits[6], SAMHSA estimates that, during that one year, approximately 741,000 emergency department visits involved non-medical use of

[5] Substance Abuse and Mental Health Services Administration. (2009). Results from the 2008 National Survey on Drug Use and Health: National Findings (Office of Applied Studies, NSDUH Series H-36, DHHS Publication No. SMA 08-4434). Rockville, MD. http://www.oas.samhsa.gov/nhsda.htm.

[6] Substance Abuse and Mental Health Services Administration, Office of Applied Studies. Drug Abuse Warning Network, 2006: National Estimates of Drug-Related Emergency Department Visits. DAWN Series D-30, DHHS Publication No. (SMA) 08-4339, Rockville, MD, 2007. http://dawninfo.samhsa.gov/.

prescription or over-the-counter drugs or dietary supplements, a 38 percent increase over 2004. Of the 741,000 visits estimated to have occurred in 2006, 195,000 involved benzodiazepines (Schedule IV) and 248,000 involved opioids (Schedule II and III). Overall, controlled substances represented 65 percent of the estimated emergency department visits involving prescription drugs or over-the-counter drugs or dietary supplements. Between 2004 and 2006, the number of visits involving opioids increased 43 percent and the number involving benzodiazepines increased 36 percent. Of all visits involving nonmedical use of pharmaceuticals, about 224,000 resulted in admission to the hospital; about 65,000 of those individuals were admitted to critical care units; 1,574 of the visits ended with the death of the patient. More than half of the visits involved patients 35 and older.

It is essential that the rules governing the electronic prescribing of controlled substances do not inadvertently facilitate diversion and abuse and undermine the ability of DEA, State, and local law enforcement to identify and prosecute those who engage in diversion. In this vein, DEA's primary goals, as they relate to this risk assessment, are to ensure that the nonregistrants do not gain access to electronic prescription applications and generate or alter prescriptions for controlled substances and to ensure that a prescription, once created, cannot be repudiated. As discussed above, the existing electronic prescription applications have the following weaknesses:

- Application providers may or may not determine whether a person subscribing to their service (for ASPs) or purchasing an application is who they claim to be let alone whether they are legally authorized to prescribe medications. There are no legal requirements that they do so.

- In some cases, applications provide access for the practice as a whole so that it is not possible to determine who wrote the prescription because access is not linked to an individual.
- Most of the applications appear to rely on passwords to identify a user to the application. Passwords are often described as the weakest link in security because they are easily guessed or, in healthcare settings, where multiple people use the same computers, easily observed. Where longer, more complex passwords are required by applications as a means to increase their effectiveness, this can actually be counterproductive, as it often causes users to write down their passwords, which weakens overall security.[7]
- With shared computers, there is no assurance that the person who logged onto the application is the same person who is using the computer at a later time. This feature may make internal audit trails, where they exist, of little use because the application will have no way of identifying who is entering data.
- There are, in general, limited standards for security of electronic prescription applications and no requirement that even where security capabilities exist, that they must be used. For example, some applications may be able to set logical access controls to limit who may sign a prescription, but unless those controls are set properly, anyone in a practice might be able to sign a prescription in a practitioner's name. Some applications allow one practitioner (or his agent) to create the prescription and any other practitioner in the practice to sign the prescription.

[7] National Institute of Standards and Technology. Special Publication 800-63-1, Draft Electronic Authentication Guideline, December 8, 2008. Appendix A.

- Except for Federal applications that use digital certificates, none of the applications transmit any indication that a prescription was actually signed.
- In many cases, applications allow a practitioner to indicate that a prescription is ready, then allow other staff to add information to the record before the prescription is transmitted. This feature can be useful in long-term care facilities, but unless the prescription information is secured before other people access it, the integrity of the prescription will always be in question.

At the pharmacy, the pharmacy has no way to verify that the prescription was sent by the practitioner whose name is on the prescription or that if it was, that it was not altered after the practitioner issued it either at the practice or during transmission. The evidence of forgery and alteration that pharmacies use to identify illegitimate paper prescriptions does not exist in an electronic record – not only because electronic prescriptions contain no handwritten signatures, but also because electronic prescriptions are typically created from drop-down menus, which prevent or reduce the likelihood of misspelled drug names, inappropriate dosage forms and units, and other indicators of possible forgery. Although many existing pharmacy applications have audit trail functions, there is no requirement that they be enabled or checked. Record integrity (assurance that a record has not been altered after it was signed) is not an issue for this risk assessment, but it is a central concern for DEA in carrying out its obligation to control against diversion.

The existing processes used for electronic prescriptions for noncontrolled substances, therefore, make it easy for every party to repudiate the prescription. A practitioner can claim that someone outside the practice issued a prescription in his name,

that someone else in the practice used his password to issue a prescription, or that it was altered after he issued it either before it was sent, during transmission, or at the pharmacy. Proving or disproving any of these claims would be very difficult with the existing processes. DEA and other law enforcement agencies might not be able to prove a case against someone issuing illegitimate prescriptions; equally important, practitioners might have trouble proving that they were not responsible for illegitimate prescriptions issued in their name.

When a prescription is transmitted (outside of a closed system), it moves through three to five intermediaries between practitioners and pharmacies. Although prescriptions could be altered, added, or deleted during transmission, DEA is not regulating transmission. Registrants have no control over the string of intermediaries. A practitioner might be able to determine from his application provider which intermediaries it uses to move the prescription from the practitioner to SureScripts/RxHub or a similar service, but neither the practitioner nor the application provider would find it easy to determine which intermediaries serve each of the pharmacies a practitioner's patients may choose. Pharmacies have the problem in reverse; they may know which intermediaries send them prescriptions, but have no way to determine the intermediaries used to route prescriptions from perhaps hundreds of practitioners using different applications to SureScripts/RxHub or a similar service. DEA believes the involvement of intermediaries will not compromise the integrity of electronic prescribing of controlled substances, provided the requirements of the interim final rule are satisfied. Among these requirements is that the prescription record be digitally signed before and after transmission to avoid the need to address the security of intermediaries.

DEA realizes that this approach will not prevent problems during the transmission, but it will at least identify that the problem occurred during transmission and protect practitioners and pharmacies from being held responsible for problems that may arise during transmission that are not attributable to them.

Some commenters on the NPRM claimed that the security practices of intermediaries were sufficient to protect electronic prescriptions. These practices, which are voluntary, do not address the principal threats of diversion, which occur before and after transmission. Maintaining the integrity of the record during transmission is of little value if there is no assurance that a registrant created and transmitted the prescription or that pharmacy staff did not alter it after receipt.

Because regulations do not currently exist permitting the use of electronic prescriptions for controlled substances, there is naturally no evidence of diversion related to electronic prescriptions of these substances. That there is no evidence that other noncontrolled prescription drugs have been diverted through electronic prescriptions is not relevant for several reasons. First, there is a very limited, if any, black market for other prescription medications. Second, there is no reason for law enforcement to investigate diversion of these medications, if it occurs, because such diversion may not be illegal (this would depend on State law). Finally, the number of electronic prescriptions including refill requests, has not been great (4 percent in 2008, according to SureScripts/RxHub).

In contrast, prescription controlled substances have always carried a significant inherent risk of diversion, both because they are addictive and because they can be sold for significantly higher prices than their retail price. The recent studies showing

increasing levels of abuse of these drugs throughout the United States heightens the cause for concern. Accordingly, with controlled substances, there is a considerable incentive for individuals and criminal organizations to exploit any vulnerabilities that exist to obtain these substances illegally.

DEA is obligated under the CSA to ensure that all transactions involving controlled substances are subject to adequate security requirements to minimize the risk of diversion and protect public health and safety. As discussed above, the electronic prescribing applications currently in use for noncontrolled substances do not contain the security features necessary for the level of risk associated with the electronic prescribing of controlled substances. Because of DEA's statutory responsibilities and the magnitude of the harm to the public health and safety that would result if an insufficiently secure system were to cause an increase in diversion of controlled substances, any regulations authorizing the use of electronic prescriptions for controlled substances must contain adequate security measures from the outset. DEA cannot, consistent with its obligations, set the bar lower than it believes necessary with an eye toward increasing the security requirements at some later date should the vulnerabilities be exploited. Regulatory changes take significant time – time during which there could be continuing harm to the public health and safety.

Requirements for Electronic Prescriptions for Controlled Substances

Based on the information presented above, certain requirements related to authentication must exist for any system to be used for the electronic prescribing of controlled substances:

- Only DEA registrants may be granted the authority to sign controlled substance electronic prescriptions. The approach must, to the greatest extent possible, protect against the theft of registrants' identities.
- The method used to authenticate a practitioner to the electronic prescribing system must ensure to the greatest extent possible that the practitioner cannot repudiate the prescription. Authentication methods that can be compromised without the practitioner being aware of the compromise are not acceptable.
- The prescription records must be reliable enough to be used in legal actions (enforcing laws relating to controlled substances) without diminishing the ability to establish the relevant facts and without requiring the calling of excessive numbers of witnesses to verify records.
- The security systems used by any electronic prescription application must, to the greatest extent possible, prevent the possibility of insider creation or alteration of controlled substance prescriptions.

VI. Risk Assessment of Authentication and Authorization of Persons Signing Electronic Controlled Substances Prescriptions

Although DEA has a number of security concerns about electronic prescriptions that are addressed in other parts of its rule regarding electronic prescriptions for controlled substances, this section, which contains the e-authentication risk assessment

for electronic prescriptions for controlled substances, addresses only two issues: whether the identity of the practitioner is confirmed prior to issuing a credential and whether the credential is protected to prevent its use by someone other than the practitioner to whom it was issued. The authentication of the prescribing practitioner is examined within the context of other controls and mitigating factors not necessarily directly related to the authentication of the prescribing practitioner to the electronic prescription application that takes place at the time the practitioner electronically "signs" the prescription.

As previously noted, where a practitioner issues a paper prescription for a controlled substance, the prescription must be written and manually signed. A prescription for a controlled substance may be issued only by an individual practitioner who is both authorized to prescribe controlled substances by the State in which he is practicing and registered with DEA (or exempted from registration) in that State. Only an authorized practitioner may sign a prescription, although an agent of that practitioner may prepare the prescription for signature.

It is critical that DEA and pharmacists that dispense controlled substances be able to identify who wrote a prescription for controlled substances and to determine based on that signature whether the person who signed the prescription is eligible to sign it. As stated previously, a pharmacist who fills a prescription for a controlled substance has a corresponding responsibility and liability to ensure that the prescription was written for a legitimate medical purpose by an authorized practitioner acting in the usual course of professional practice.

All these factors were taken into consideration in the design of all aspects of the interim final rule permitting the electronic prescribing of controlled substances. In

developing the requirements pertaining to the authentication of the identity of persons signing controlled substances prescriptions, DEA has sought, to the extent feasible, to arrive at requirements that can be reconciled with existing electronic prescription applications. DEA considered not only its own obligations under the CSA but also those of the regulated industry.[8]

Initial E-Authentication Analysis of Electronic Prescriptions for Controlled Substances

M-04-04 requires agencies to consider six potential impacts and rate whether failure to ensure authentication would have a low, medium, or high impact on that factor. Before presenting DEA's analysis, a brief recap of DEA's initial analysis (as discussed in the NPRM (specifically, 73 FR 36731-36735, June 27, 2008)) is presented here. The following table summarizes DEA's initial analysis of the six categories, including its evaluation of the level of harm, absent any regulatory controls, that could occur if (1) credentials are issued without confirming the identity of the person to whom it is issued, and (2) the credential can be used by someone other that the person to whom it is issued. The rationale for each of DEA's initial ratings is then discussed in greater detail.

Table 1: Initial Rating of Potential Impacts for Authentication Errors for Electronic Prescriptions for Controlled Substances

Potential Impact	Initial Rating
Inconvenience, Distress, or Damage to Standing or Reputation	Moderate -- At worst, serious short term or limited long-term inconvenience, distress, or damage to the standing or reputation of any party.
Financial Loss	N/A

[8] Because both DEA and the Department of Health and Human Services are involved in addressing electronic prescriptions, they held a joint public meeting on July 11 and 12, 2006, to gather information from the regulated community (practitioners and pharmacies) as well as from the prescription and pharmacy service providers, technical experts, and Federal, State, and local law enforcement. The meeting record is available at http://www.deadiversion.usdoj.gov/ecomm/e_rx/mtgs/july2006/index.html.

Potential Impact	Initial Rating
Harm to Agency Programs or Public Interests	High -- A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of (sic) to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.
Unauthorized release of Sensitive Information	N/A
Personal Safety	High – A risk of serious injury or death.
Civil or Criminal Violations	High – A risk of civil or criminal violations that are of special importance to enforcement programs.

Initial Rating for Potential Impact of Inconvenience, Distress, or Damage to Standing or Reputation

Failure to verify the identity of the person to whom a credential is issued or to limit the ability of others to use a credential once issued could result in the theft of the practitioner's identity and the issuance of illegal prescriptions in the practitioner's name. Until the registrant could satisfy DEA or other law enforcement agencies that he was not responsible for the illegal prescriptions, his DEA registration could be suspended or revoked. Suspension or revocation would mean the registrant could no longer issue controlled substance prescriptions. Such a revocation or suspension could severely limit a practitioner's ability to practice and cause distress and at least temporary damage to the practitioner's reputation and standing. As it generally takes considerable time and effort to resolve issues related to identity theft and issuance of prescriptions in a practitioner's name, DEA initially rated the potential impact as moderate.

Initial Rating for Potential Impact of Financial Loss

Although a practitioner would have to expend some time and effort to address issues related to identity theft or misuse of a credential by someone else, identity theft

and/or credential misuse do not, in and of themselves, affect the practitioner's authority to prescribe controlled substances. DEA has rated the potential impact of financial loss as not applicable.

Initial Rating for Potential Impact of Harm to Agency Programs or Public Interests

DEA is charged with maintaining a closed system of distribution, ensuring that there are adequate supplies of controlled substances to meet the legitimate medical, scientific, and industrial needs of the United States while preventing diversion of those controlled substances to illicit purposes. Current electronic prescribing systems are open systems involving many application providers and several intermediaries in the transmission process. There is more possibility of diversion from this open system than there is from a closed system in which DEA closely monitors the flow of controlled substances.

The current electronic prescription applications and application providers are not required to and, in some cases, do not take any steps to ensure that credentials used for approving prescriptions are issued only to practitioners authorized to prescribe. When issued, credentials usually consist only of user names and passwords, which are easily guessed, observed, or hacked. The current system makes it easy to commit identity theft or to misuse a credential issued to a registrant. The potential exists for widespread and rapid diversion of controlled substances. Such diversion would undermine the effectiveness of the prescription laws and regulations of the United States. This diversion would, by its very nature, harm the public health and safety, as any illicit drug use does. Such diversion would undermine the effectiveness of the entire United States closed system of distribution of controlled substances created by the CSA and would, for the

same reason, be incompatible with the United States' obligations under international drug control treaties. As stated in the CSA, Congress has expressly found that the illegal distribution, possession, and improper use of controlled substances "have a substantial and detrimental effect on the health and general welfare of the American people." (21 U.S.C. 801(2)). Therefore, DEA initially rated the potential impact of harm to agency programs or public interests as high.

Initial Rating of Potential Impact of Unauthorized Release of Sensitive Information

Since this system does not address aspects of the unauthorized release of sensitive information, DEA determined this element was not applicable to the evaluation of the system.

Initial Rating of Potential Impact to Personal Safety

While controlled substances have valuable and necessary legitimate medical purposes, they are controlled because of their potential for abuse and physical or psychological dependence. Their misuse, either intentional or unintentional, could have serious physical consequences to the patient, including the possibility of serious injury or death. Any system that makes it easier for individuals and organized criminals to divert these drugs increases the likelihood that additional people will abuse or misuse these drugs and be harmed by them. Therefore, DEA initially rated the potential impact to personal safety as high.

Initial Rating of Potential Impact of Civil or Criminal Violations

The illicit possession of legitimate (pharmaceutical) controlled substances is a violation of the CSA. The writing of a controlled substance prescription by a person not authorized to do so constitutes illegal dispensing of a controlled substance as doing so is

a violation of 21 U.S.C. 841(a)(1). The person writing an illegitimate prescription could be criminally prosecuted; penalties for such a conviction include imprisonment and/or fines. A practitioner whose identity was stolen to gain a credential or whose credential was used by someone else to issue a prescription for a controlled substance could be subject to legal action in which the practitioner would have to prove that he was not responsible for the prescriptions. Such legal action against the practitioner could include criminal prosecution, civil fine proceedings, and administrative proceedings to revoke the practitioner's DEA registration. Therefore, DEA initially rated the potential impact of civil or criminal violations as high.

Initial Conclusion

Under M-04-04, the overall rating is driven by the highest rating assigned. Therefore, the potential impact of not being able to limit authentication credentials to DEA registrants is rated as high, which implies that without mitigating factors, DEA should impose requirements that meet Assurance Level 4 under NIST SP 800-63-1.

Mitigating Factors

As discussed previously, significant risks are present with electronic prescriptions for controlled substances, particularly if persons not authorized to access the electronic prescription application are able to do so. To mitigate the risks of unauthorized access to the electronic prescription application and to reduce the potential for diversion, DEA developed a number of elements in implementing its regulations. While some of these relate to authentication to the application, others relate to use of the application itself. DEA believes that all of these elements, taken together, reduce the initial ratings for potential harm discussed above.

Separation of duties. DEA's premise for its requirements regarding the access to any electronic prescription application to prescribe controlled substances rests on the principle of separation of duties. The interim final rule requires that practitioners wishing to prescribe controlled substances undergo identity proofing by an independent third-party credential service provider (CSP) or certification authority (CA) that is recognized by a Federal agency as conducting identity proofing at the basic assurance level (Assurance Level 3 for CAs) or greater. The CSP or CA will then issue the credential. This approach removes the electronic prescription application provider from the process of issuing the credential, which limits the ability of individuals at the application provider to steal identities.

Access Control. The possession of a credential by the practitioner, while necessary to legally sign controlled substance prescriptions, is not sufficient to do so. After the practitioner has obtained the credential, a person in the practitioner's office (assuming that the practitioner is in private practice in an office setting) must enter information into the electronic prescription application identifying the practitioner as a DEA registrant, or a person exempted from the requirement of registration, authorized to prescribe controlled substances. A second person in that office, who must be a DEA registrant, must approve the information entered and grant the practitioner access to the electronic prescription application for the purpose of signing controlled substance prescriptions using the practitioner's credential. (Note that a similar system involving separation of duties is being implemented for institutional practitioners, i.e., hospitals and clinics. That system has similar conceptual requirements, but involves different people in the physical processes.)

This separation of duties ensures that even if someone is able to impersonate a practitioner and obtain a credential from an independent third-party CSP or CA, that impersonator will not be able to gain access to the electronic prescription application to sign controlled substance prescriptions unless the impersonator also has the assistance of two persons (one of whom is a DEA registrant) within a practitioner's office. In this way, it will be significantly more difficult for impersonators to gain access to sign controlled substance prescriptions, reducing the possibility of authentication errors and lessening the potential for diversion.

Use of a two-factor authentication protocol. DEA is requiring the use of a two-factor authentication protocol. Two of the following three factors must be present in any authentication protocol used by a practitioner to sign electronic prescriptions for controlled substances:

- Something only the practitioner knows, e.g., a password or response to a challenge question.
- Something the practitioner is, biometric data such as a fingerprint or iris scan.
- Something the practitioner has, a device (e.g., hard token) separate from the computer to which the practitioner is gaining access.

NIST SP 800-63-1 Assurance Level 4 requires a hard token that is separate from the computer to which the person is gaining access, but also imposes more stringent requirements on the cryptographic module and the token. DEA has determined that combining the requirements for FIPS 140-2 Security Level 1 tokens with the requirement that the token be separate from the computer will provide sufficient security to mitigate the risk or misuse. Keeping the token separate from the computer being accessed makes

it much easier for the practitioner to control access to his credential. A person would have to obtain both the token and the second factor to gain access.

Application Requirements. In addition to the requirements discussed above, DEA is also imposing the following requirements on the electronic prescription application that will mitigate the risks:

- The application must have the ability to set logical access controls as discussed above and limit access to indicating that prescriptions are ready for signing and signing prescriptions to DEA registrants or those exempted from registration.
- The application must require the use of the two-factor authentication credential to sign the prescription and digitally sign and archive the record when the two-factor authentication protocol is executed. This step ensures that there is a record of the prescription as signed and allows other people in the practice or facility to add information, (e.g., pharmacy URLs) or review the prescription before transmission.
- The application must not allow a practitioner to sign a prescription if his credential is not linked to the DEA number listed on the prescription.
- The application must undergo a third-party audit to determine whether it complies with the requirements of the interim final rule.

In addition, as part of their approval by the Federal government, CSPs and CAs issuing credentials undergo third-party audits to ensure compliance with Federal government standards.

Final Rating of Potential Impacts

Taking into account the comments that DEA received in response to the NPRM, DEA conducted a second evaluation of the potential impacts of authentication errors for electronic prescriptions for controlled substances. DEA continues to believe that the initial assessments were accurate in all categories. However, consistent with M-04-04, DEA believes that it is appropriate for the agency to accept lower level credentials in view of the mitigating factors discussed above. M-04-04 states, in pertinent part (in Section 2.5):

> Agencies may also decrease reliance on identity credentials through increased risk-mitigation controls. For example, an agency business process rated for Level 3 identity assertion assurance may lower its profile to accept Level 2 credentials by increasing system controls or 'second level authentication' activities.

Following this approach, DEA has concluded that, even though the agency rates overall identity assurance for electronic prescribing of controlled substances at Assurance Level 4, the agency believes that Assurance Level 3 credentials are acceptable in view of the system controls that are mandated by this interim final rule. Specifically, DEA believes that the requirements that the interim final rule imposes for identity proofing, logical access control, the separation of the hard token from the computer being accessed, and the application requirements lower the potential for a non-registrant to steal an identity or gain access to a registrant's credential and issue illegal prescriptions sufficiently to render acceptable an overall Assurance Level of Level 3, as many commenters recommended. With these requirements in place, the potential for diversion through misuse of a credential will be limited, which supports the closed system of

control DEA is mandated to maintain, protect practitioners from misuse of their identity, and protects the public from the harm of drug abuse.

System Design

Based on the analysis above, any authentication system that satisfies the requirements of this interim final rule will satisfy Assurance Level 3. As discussed below, DEA is requiring in-person or remote identity proofing, and two-factor authentication to the electronic prescription application at NIST SP 800-63-1 Assurance Level 3 provided that the token, if used, meets FIPS 140-2 Security Level 1 and is separate from the computer being accessed. Together, these elements will provide the practitioner with the ability to authenticate to the system to sign controlled substances prescriptions electronically.

Identity proofing. Under NIST SP 800-63-1, Assurance Level 3 identity proofing requires in-person checks of photographic identification, but does not require collection of biometrics, and allows remote identity proofing.

Authentication. Each practitioner who is authorized to sign controlled substance prescriptions by the State and DEA must have a unique authentication to access the electronic prescription application. DEA is requiring two-factor authentication that meets the requirements of FIPS 140-2 Security Level 1; the hard token, when used, must be separate from the computer being accessed.

The reason for requiring a hard token is that a practitioner can clearly demonstrate possession and control of it in a way that practitioners cannot ensure control of passwords. Unlike passwords, hard tokens are tangible, physical objects. Their disappearance, loss, or theft should be readily apparent to the practitioner. If a

practitioner was to give the hard token to someone else who then used it to illegally prescribe controlled substances, it would be much more difficult for the practitioner to deny knowledge and intent of the action to give the token away. In contrast, practitioners may not be aware that a password has been compromised.

Electronic prescription applications operate in an open environment and are often part of broader EHRs. Practitioners cannot guarantee the security of the computer systems maintained in medical offices. Due to the nature of medical practice, it is conceivable that many persons, not just the practitioner permitted to prescribe controlled substances, would have access to the computer on which the prescribing application is maintained. With respect to prescribing authority, the CSA is clear — only certain persons are authorized to sign controlled substances prescriptions; it is unlawful for any other person to sign such prescriptions. DEA believes that the identity proofing, access control, and two-factor authentication requirements being established will ensure that only authorized practitioners are permitted to access an electronic prescription application to sign controlled substances prescriptions. At the same time, DEA believes that these requirements will be compatible with existing electronic prescription applications in use today.

As has been discussed previously, it is important to note that the electronic prescribing of controlled substances is voluntary — practitioners may still dispense controlled substances through the use of written prescriptions, regardless of whether they choose to write controlled substances prescriptions electronically. Also, it is important to note that the compromise of an authentication credential through loss, credential invalidation, or other cause, does not invalidate the practitioner's authority to write

controlled substances prescriptions. Practitioners may continue to write controlled substances prescriptions on paper even if their authentication credential has been compromised, so long as the practitioner continues to possess a DEA registration.

Conclusion

DEA believes that the use of NIST SP 800-63-1 Assurance Level 3 identity proofing and two-factor authentication to access electronic prescription applications to sign controlled substances prescriptions will provide security commensurate with the current paper-based prescription system, and will meet statutory obligations of the CSA. Such a system will provide the regulated industry with the benefit of transmitting controlled substances prescriptions electronically, using current electronic prescription applications.