DEPARTMENT OF JUSTICE

Drug Enforcement Administration

21 CFR Parts 1300, 1304, 1306, and 1311

[Docket No. DEA–218P]

RIN 1117–AA61

Electronic Prescriptions for Controlled Substances

AGENCY: Drug Enforcement Administration (DEA), Department of Justice.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: DEA is proposing to revise its regulations to provide practitioners with the option of writing prescriptions for controlled substances electronically. These regulations would also permit pharmacies to receive, dispense, and archive these electronic prescriptions. These proposed regulations would be an addition to, not a replacement of, the existing rules. These regulations provide pharmacies, hospitals, and practitioners with the ability to use modern technology for controlled substance prescriptions while maintaining the closed system of controls on controlled substances dispensing; additionally, the proposed regulations would reduce paperwork for DEA registrants who dispense or prescribe controlled substances and have the potential to reduce prescription forgery. The proposed regulations would also have the potential to reduce the number of prescription errors caused by illegible handwriting and misunderstood oral prescriptions. Moreover, they would help both pharmacies and hospitals to integrate prescription records into other medical records more directly, which would increase efficiency, and would reduce the amount of time patients spend waiting to have their prescriptions filled.

DATES: Written comments must be postmarked, and electronic comments must be sent, on or before September 25, 2008.

ADDRESSES: To ensure proper handling of comments, please reference ''Docket No. DEA–218'' on all written and electronic correspondence. Written comments sent via regular or express mail should be sent to Drug Enforcement Administration, Attention: DEA Federal Register Representative/ODL, 8701 Morrissette Drive, Springfield, VA 22152. Comments may be directly sent to DEA electronically by sending an electronic message to *dea.diversion.policy@usdoj.gov*. Comments may also be sent electronically through *http://www.regulations.gov* using the electronic comment form provided on that site. An electronic copy of this document is also available at the *http://www.regulations.gov* Web site. DEA will accept electronic comments containing MS word, WordPerfect, Adobe PDF, or Excel files only. DEA will not accept any file formats other than those specifically listed here.

FOR FURTHER INFORMATION CONTACT: Mark W. Caverly, Chief, Liaison and Policy Section, Office of Diversion Control, Drug Enforcement Administration, 8701 Morrissette Drive, Springfield, VA 22152, Telephone (202) 307–7297.

SUPPLEMENTARY INFORMATION:

Posting of Public Comments: Please note that all comments received are considered part of the public record and made available for public inspection online at *http://www.regulations.gov* and in the Drug Enforcement Administration's public docket. Such information includes personal identifying information (such as your name, address, etc.) voluntarily submitted by the commenter.

If you want to submit personal identifying information (such as your name, address, etc.) as part of your comment, but do not want it to be posted online or made available in the public docket, you must include the phrase ''PERSONAL IDENTIFYING INFORMATION'' in the first paragraph of your comment. You must also place all the personal identifying information you do not want posted online or made available in the public docket in the first paragraph of your comment and identify what information you want redacted.

If you want to submit confidential business information as part of your comment, but do not want it to be posted online or made available in the public docket, you must include the phrase ''CONFIDENTIAL BUSINESS INFORMATION'' in the first paragraph of your comment. You must also prominently identify confidential business information to be redacted within the comment. If a comment has so much confidential business information that it cannot be effectively redacted, all or part of that comment may not be posted online or made available in the public docket.

Personal identifying information and confidential business information identified and located as set forth above will be redacted and the comment, in redacted form, will be posted online and placed in the Drug Enforcement Administration's public docket file. Please note that the Freedom of Information Act applies to all comments received. If you wish to inspect the agency's public docket file in person by appointment, please see the **FOR FURTHER INFORMATION CONTACT** paragraph.

I. Background

Legal Authority

DEA implements the Comprehensive Drug Abuse Prevention and Control Act of 1970, often referred to as the Controlled Substances Act (CSA) and the Controlled Substances Import and Export Act (21 U.S.C. 801–971), as amended. DEA publishes the implementing regulations for these statutes in Title 21 of the Code of Federal Regulations (CFR), Parts 1300 to 1399. These regulations are designed to ensure an adequate supply of controlled substances for legitimate medical, scientific, research, and industrial purposes, and to deter the diversion of controlled substances to illegal purposes. The CSA mandates that DEA establish a closed system of control for manufacturing, distributing, and dispensing controlled substances. Any person who manufactures, distributes, dispenses, imports, exports, or conducts research or chemical analysis with controlled substances must register with DEA (unless exempt) and comply with the applicable requirements for the activity.

Controlled Substances

Controlled substances are drugs that have a potential for abuse and psychological and physical dependence; these include opiates, 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 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 accepted medical uses and also have potential for abuse and psychological and physical dependence. Virtually all Schedule II–V controlled substances are available only under a prescription written by a practitioner licensed by the State and registered with DEA to dispense the substances. Overall, controlled substances constitute between 10 percent and 11 percent of all prescriptions written in the United States.

History

The CSA and DEA's regulations were originally adopted at a time when most transactions and particularly prescriptions were done on paper. The CSA mandates that some records must be created and kept on forms that DEA provides and that many controlled substance prescriptions must be manually signed. In 1999, in response to requests from the regulated community, DEA began to examine how to revise its regulations to allow the use of electronic systems within the limits imposed by the statute and mindful that the records had to be usable in legal actions. On April 1, 2005, after extensive consultation with the regulated community, DEA published a final rule that allowed the electronic creation, signature, transmission, and retention of records of orders for Schedule I and II controlled substances, orders that prior to that time had to be created on preprinted forms that DEA issued (70 FR 16901, April 1, 2005).

At the same time, DEA began to examine how to revise its rules to allow electronic prescriptions for controlled substances. In addition to complying with the mandates of the CSA, regulations on electronic prescriptions must be consistent with other statutory mandates and Federal regulations. The Electronic Signatures in Global and National Commerce Act of 2000, commonly known as E-Sign, was signed into law on June 30, 2000 (Pub. L. 106–229). It establishes the basic rules for using electronic signatures and records in commerce. E-Sign was enacted to encourage electronic commerce by giving legal effect to electronic signatures and records and to protect consumers. E-Sign provides that, with respect to any transaction in or affecting interstate or foreign commerce, a signature may not be denied legal effect solely because it is in electronic form (15 U.S.C. 7001(a)). However, E-Sign further provides that, where a statute or regulation requires retention of a record, and an electronic record is used to meet such requirement, Federal, State, and local agencies may set performance standards to ensure accuracy, record integrity, and accessibility of records (15 U.S.C. 7004(b)(3)(A)). Such performance standards may be specified in a manner that requires the implementation of a specific technology if such requirement serves an important governmental objective and is substantially related to that objective interest (Id.).

In 2003, Congress enacted the Medicare Prescription Drug, Improvement, and Modernization Act (MMA) (Pub. L. 108–173). 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). One of the considerations in support of this move to electronic prescriptions was the view that using electronic prescriptions in lieu of written or oral prescriptions could reduce medical errors that occur because handwriting is illegible or phoned in prescriptions are misunderstood as a result of similar sounding medication names. Another consideration is that, if prescription records are linked to other medical records, practitioners can be alerted at the time of prescribing to possible interactions with other drugs the patient is taking or allergies a patient might have. Electronic prescribing systems also can link to insurance formulary lists to inform the practitioner prior to prescribing whether a drug is covered by a patient's insurance.

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). The standard focuses on the format for the transmitted information, not with the process of creating the prescription or maintaining the record at the pharmacy. HHS adopted the National Council of Prescription Drug Programs (NCPDP) SCRIPT Standard, Implementation Guide, Version 8.1. The standard specifies fields (name, date, address, etc.) and field lengths for certain transactions including issuing new prescriptions and refills. The rule applies to prescriptions issued to patients under Part D (the prescription drug program for Medicare patients). The rule does not require practitioners or pharmacies to use electronic prescriptions, but rather requires that companies that sponsor Part D coverage establish and maintain an electronic prescription program that meets the standard. The purpose of the standard is to ensure that electronic prescriptions are created and transmitted in a format that can be read by the receiving pharmacy (i.e., that the systems creating, transmitting, and receiving the prescriptions are interoperable).

The rule DEA is hereby proposing has been written to be consistent with the foregoing HHS standard. However, it bears emphasis that the context in which the HHS standard was issued was not specific to controlled substances and therefore not designed to provide safeguards against the diversion of controlled substances. The responsibility for establishing regulatory safeguards against diversion of controlled substances falls upon DEA as the agency charged with administering and enforcing the CSA. Accordingly, while the rule being proposed here by DEA is designed to work in tandem with the HHS standard, its scope is necessarily distinct from the HHS standard.

Prescription records and transmission are also subject to the Health Insurance Portability and Accountability Act (HIPAA), which establishes protection for health information. Any party to the creation, transmission, and storage of prescriptions must meet standards to ensure that the information is protected and not revealed to persons who are not authorized to see it. 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 parts 160, 162, and 164. Because of the wide variety of healthcare providers subject to HIPAA, the requirements are general to allow the providers to adopt protections that are appropriate for their situations. For example, the security steps needed at a one-practitioner office will be very different from those needed at a large hospital system or chain pharmacy system. The DEA rule being issued here is consistent with HIPAA security guidance issued by HHS, as explained later in this document.

Because both DEA and HHS 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*.

Based on the meeting and on the requirements of the CSA and the other applicable provisions of law outlined above, DEA has developed this proposed rule. As the proposed rule illustrates, 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 already increasing problem of prescription controlled substance abuse

in the United States, as discussed further below. It is also essential that the rules governing the electronic prescribing of controlled substances do not undermine the ability of DEA, State, and local law enforcement to identify and prosecute those who engage in diversion.

The remainder of this preamble for the rule is organized as follows:

Section II discusses the framework of pertinent provisions of the CSA and DEA regulations to provide a context for this proposed rule.

Section III describes the current requirements for controlled substance prescriptions.

Section IV discusses the existing electronic prescription and pharmacy systems.

Section V discusses potential vulnerabilities that need to be addressed to prevent electronic prescribing from contributing to the diversion of controlled substances.

Section VI discusses alternatives considered.

Section VII discusses the risk assessment DEA conducted regarding electronic prescriptions for controlled substances.

Section VIII describes the proposed rule and the rationale for the requirements DEA is proposing to impose on prescription and pharmacy systems that create, process, and archive controlled substance prescriptions.

Section IX provides a summary of the proposed rule requirements and their current implementation status.

Section X is a section-by-section analysis of the proposed rule.

Section XI describes a system for the electronic prescribing of controlled substances that DEA is proposing specifically for use by Federal health care agencies (including the United States Army, Navy, Marine Corps, Air Force, Coast Guard, Department of Veterans Affairs, Public Health Service, and Bureau of Prisons). These agencies would be permitted to use either system for controlled substances prescribing and dispensing.

Section XII discusses the incorporation by reference of one standard published by the National Institute of Standards and Technology.

Section XIII presents the required analyses on the economic and other impacts of the proposed rule.

II. Framework of the Pertinent Provisions of the CSA and DEA Regulations

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.)*.

The CSA defines ''dispense'' to include, among other things, the issuance of a prescription by a practitioner as well as the delivery of a controlled substance to a patient by a pharmacy pursuant to a prescription (21 U.S.C. 802(10)). Thus, both practitioners who prescribe controlled substances and pharmacies that fill such prescriptions must obtain a DEA registration (21 U.S.C. 822(a)(2)). The CSA definition of practitioner (21 U.S.C. 802(21)) includes, among others, physicians, dentists, veterinarians, pharmacies, and, where authorized by an appropriate State authority, physician assistants and advance practice nurses.

It is important to reiterate here that DEA registers pharmacies, as opposed to pharmacists. As a rule, pharmacists themselves do not have the authority to independently prescribe controlled substances. Rather, pharmacists rely on the prescription, as written by the individual practitioner, for authority to conduct the dispensing.

Under longstanding Federal law, for a prescription for a controlled substance to be valid, it must be issued for a legitimate medical purpose by a practitioner acting in the usual course of professional practice (*United States* v. *Moore, 423 U.S. 122 (1975)*; 21 CFR 1306.04(a)). As the DEA regulations state: ''The responsibility for the proper prescribing and dispensing of controlled substances is upon the prescribing practitioner, but a corresponding responsibility rests with the pharmacist who fills the prescription.'' (21 CFR 1306.04(a)).

The CSA provides that a controlled substance in Schedule II may only be dispensed by a pharmacy pursuant to a ''written prescription,'' except in emergency situations (21 U.S.C. 829(a)). In contrast, for controlled substances in Schedules III and IV, the CSA provides that a pharmacy may dispense pursuant to a ''written or oral prescription.'' (21 U.S.C. 829(b)). Where an oral prescription is permitted by the CSA, the DEA regulations further provide that a practitioner may transmit to the pharmacy a facsimile of a written prescription in lieu of an oral prescription (21 CFR 1306.21(a)).

Enforcement of the Controlled Substances Act

The Controlled Substances Act is unique among criminal laws in that it stipulates acts pertaining to controlled substances that are permissible. That is, if the CSA does not explicitly permit an action pertaining to a controlled substance, then by its lack of explicit permissibility the act is prohibited. Violations of the Act can be civil or criminal in nature, which may result in administrative, civil, or criminal proceedings. Remedies under the Act can range from modification or revocation of DEA registration, to civil monetary penalties or imprisonment, depending on the nature, scope, and extent of the violation.

Specifically, it is unlawful for any person knowingly or intentionally to manufacture, distribute, or dispense, a controlled substance or to possess a controlled substance with the intent of manufacturing, distributing, or dispensing that controlled substance, except as authorized by the Controlled Substances Act (21 U.S.C. 841(a)(1)).

Further, it is unlawful for any person knowingly or intentionally to possess a controlled substance unless such substance was obtained directly, or pursuant to a valid prescription or order, issued for a legitimate medical purpose, from a practitioner, while acting in the course of the practitioner's professional practice, or except as otherwise authorized by the CSA (21 U.S.C. 844(a)). It is unlawful for any person to knowingly or intentionally acquire or obtain possession of a controlled substance by misrepresentation, fraud, forgery, deception, or subterfuge (21 U.S.C. 843(a)(3)).

It is unlawful for any person knowingly or intentionally to use a DEA registration number that is fictitious, revoked, suspended, expired, or issued to another person in the course of dispensing a controlled substance, or for the purpose of acquiring or obtaining a controlled substance (21 U.S.C. 843(a)(2)).

Beyond these possession and dispensing requirements, it is unlawful for any person to refuse or negligently fail to make, keep, or furnish any record (including any record of dispensing) that is required by the CSA (21 U.S.C. 842(a)(5)). It is also unlawful to furnish any false or fraudulent material information in, or omit any information from, any record required to be made or kept (21 U.S.C. 843(a)(4)(A)).

Within the CSA's system of controls, it is the individual practitioner (e.g., physician, dentist, veterinarian, nurse

practitioner) who issues the prescription authorizing the dispensing of the controlled substance. This prescription must be issued for a legitimate medical purpose and must be issued in the usual course of professional practice. The individual practitioner is responsible for ensuring that the prescription conforms to all legal requirements. The pharmacist, acting under the authority of the DEA-registered pharmacy, has a corresponding responsibility to ensure that the prescription is valid and meets all legal requirements. The DEA-registered pharmacy does not order the dispensing. Rather, the pharmacy, and the dispensing pharmacist, merely rely on the prescription as written by the DEA-registered individual practitioner to conduct the dispensing.

Thus, a prescription is much more than the mere method of transmitting dispensing information from a practitioner to a pharmacy. The prescription serves both as a record of the practitioner's determination of the legitimate medical need for the drug to be dispensed, and as a record of the dispensing, providing the pharmacy with the legal justification and authority to dispense the medication prescribed by the practitioner. The prescription also provides a record of the actual dispensing of the controlled substance to the ultimate user (the patient) and, therefore, is critical to documenting that controlled substances held by a pharmacy have been dispensed legally. The maintenance by pharmacies of complete and accurate prescription records is an essential part of the overall CSA regulatory scheme established by Congress, wherein all those within the legitimate distribution chain must strictly account for all controlled substances on hand, as well as those received, sold, delivered, or otherwise disposed of (21 U.S.C. 827). The CSA recordkeeping requirements for prescriptions are somewhat unusual in that the practitioner is not required to maintain a record of prescriptions written; instead, the record is held only by the pharmacy.

Abuse of Controlled Substances

The level of control mandated by Congress for controlled substances far exceeds that for other prescription drugs commensurate with the facts that controlled substances can cause physical and psychological dependence and have historically been abused. Several studies of drug abuse patterns indicate that nonmedical use of prescription controlled substances (those in Schedules II through V) is an increasing problem even as the use of certain Schedule I substances appears to have declined somewhat in recent years.

The National Survey on Drug Use and Health (NSDUH) (formerly the National Household Survey on Drug Abuse) is an annual survey of the civilian, non-institutionalized, population of the United States aged 12 or older. The survey is conducted by the Office of Applied Studies, Substance Abuse and Mental Health Services Administration, of the Department of Health and Human Services. Findings from the 2006 NSDUH were released in September 2007 and are the latest year for which information is currently available.

The 2006 NSDUH [1] estimated that 20.4 million Americans were classified with substance dependence or abuse (8.3 percent of the total population aged 12 or older). Further, the 2006 NSDUH estimated that 6.7 million persons were current users, i.e., past 30 days, of psychotherapeutic drugs—pain relievers, anti-anxiety medications, stimulants, and sedatives—taken nonmedically. This represents 2.8 percent of the population aged 12 or older. Specifically, the NSDUH estimated that 5.2 million persons used pain relievers, 1.8 million used tranquilizers, 1.2 million used stimulants, and 0.4 million used sedatives. Except for tranquilizers, these estimates are increases from the corresponding estimates for 2005.

According to the NSDUH, more than 20 percent of persons age 12 or older have used psychotherapeutic drugs nonmedically in their lifetime. Overall, 33 million Americans are estimated to have used prescription pain killers for nonmedical reasons in their lifetime. Specific pain relievers with statistically significant increases in lifetime use for 18 to 25 year olds between 2003 and 2006 were the Schedule III controlled substances Vicodin®, Lortab®, or Lorcet® (from 15.0 percent to 18 percent); Schedule III controlled substances containing hydrocodone (from 16.3 percent to 19.2 percent); the Schedule II controlled substance OxyContin® (from 3.6 percent to 5.1 percent); and the Schedule II controlled substances containing oxycodone (from 8.9 percent to 10.8 percent).

Results of a separate study of seventh through twelfth grade students were released April 21, 2005, by the Partnership for a Drug-Free America. The Partnership Attitude Tracking Study [2] tracks consumers' exposure to and attitudes about drugs. The study focuses on perceived risk and social attitudes. For the first time in its seventeen-year history, the study found that teenagers are more likely to have abused a prescription pain medication to get high than they are to have experimented with a variety of illicit drugs including Ecstasy, cocaine, crack and LSD. In 2004, the study reported that nearly one in five teenagers, 18 percent, or 4.3 million teenagers nationally, indicated they have used the Schedule III controlled substance Vicodin® without a prescription. Approximately ten percent of teens, or 2.3 million teens nationally, reported using the Schedule II controlled substance OxyContin® without a prescription. Further, the study reported that ten percent, or 2.3 million teenagers nationally, reported having used prescription stimulants, Ritalin® and/or Adderall®, without a prescription. The 2005 survey indicated that 50 percent of the teenagers surveyed indicated that prescription drugs are widely available; a third indicated that they were easy to purchase over the Internet.

The 2006 National Institute of Drug Abuse survey of drug use by teens in the eighth, tenth, and twelfth grades, Monitoring the Future: National Results on Adolescent Drug Use [3], found that past-year nonmedical use of Vicodin® (Schedule III) remained high among all three grades, with nearly one in ten high school seniors using it in the past year. Despite a drop from 2005 to 2006 in past-year abuse of OxyContin® among twelfth graders (from 5.5 percent to 4.3 percent), there has been no such decline among the eighth and tenth grade students, and the rate of use among the youngest students has increased significantly since it was included in the survey in 2002.

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), 2005: National Estimates of Drug-Related Emergency Department Visits,[4] SAMHSA estimates that about

[1] Substance Abuse and Mental Health Services Administration. (2007). *Results From the 2006 National Survey on Drug Use and Health: National Findings* (Office of Applied Studies, NSDUH Series H–32, DHHS Publication No. SMA 07–4293). Rockville, MD. *http://www.oas.samhsa.gov/nhsda.htm.*

[2] Partnership for a Drug-Free America; Partnership Attitude Tracking study, 2005; *http://www.drugfree.org/Portal/DrugIssue/Research/.*

[3] Johnston, L. D., O'Malley, P. M., Bachman, J. G., and Schulenberg, J. E. (2007). *Monitoring the Future national results on adolescent drug use: Overview of key findings, 2006.* (NIH Publication No. 07–6202). Bethesda, MD: National Institute on Drug Abuse; *http://www.monitoringthefuture.org/pubs.html.*

[4] Substance Abuse and Mental Health Services Administration, Office of Applied Studies. *Drug*

Continued

599,000 emergency department visits involved nonmedical use of prescription or over-the-counter drugs or dietary supplements, a 21 percent increase over 2004. Of the 599,000 visits, 172,000 involved benzodiazepines (Schedule IV) and 196,000 involved opiates (Schedule II and III). Overall, controlled substances represented 66 percent of the estimated emergency department visits. Between 2004 and 2005, the number of visits involving opiates increased 24 percent and the number involving benzodiazepines increased 19 percent. About a third (200,000) of all visits involving nonmedical use of pharmaceuticals resulted in admission to the hospital; about 66,000 of those individuals were admitted to critical care units; 1,365 of the visits ended with the death of the patient. More than half of the visits involved patients 35 and older.

Means by Which Controlled Substances Are Diverted

Understanding the means by which controlled substances are diverted is critical to determining appropriate regulatory controls. Diversion of prescription controlled substances can occur in a number of ways, including, but not limited to, the following:

- Prescription pads are stolen from practitioners' offices by patients, staff, or others and illegitimate prescriptions are written.
- Legitimate prescriptions are altered to obtain additional amounts of legitimately prescribed controlled substances.
- Drug-seeking patients may falsify symptoms and/or obtain multiple prescriptions from different practitioners for their own use or for resale. In some cases, organized groups visit practitioners with fake symptoms to obtain prescriptions, which are filled and resold. Some patients resell their legitimately obtained drugs to earn extra money.
- Prescription pads containing legitimate practitioner information (e.g., name, address, DEA registration number) are printed with a different call back number that is answered by an accomplice to verify the prescription.
- Computers and scanning or copying equipment are used to create prescriptions for nonexistent practitioners or to copy legitimate practitioners' prescriptions.
- Pharmacies and other locations where controlled substances are stored are robbed or burglarized.

Diversion from within the practitioner's practice or pharmacy may also occur, such as in the following situations:

- Prescriptions are written for other than a legitimate medical purpose. Some practitioners knowingly write prescriptions for nonmedical purposes. Criminal organizations commonly referred to as ''rogue Internet pharmacies'' often employ practitioners to issue prescriptions based on online questionnaires from patients with whom the practitioner has no legitimate medical relationship.
- Controlled substances are stolen from a pharmacy by pharmacy personnel. Legitimately dispensed prescriptions may be altered to make the thefts less detectable.
- Legitimate prescriptions may be stolen from legitimate patients. The stolen legitimate prescriptions may be filled by persons addicted to or abusing controlled substances.

Given these common methods of diversion, as well as the alarmingly increasing extent of prescription controlled substance abuse in the United States, many of those at the DEA/HHS public meeting in 2006, particularly representatives of Federal and state law enforcement and regulatory agencies, emphasized that any system allowing the electronic prescribing of controlled substances must have sufficient safeguards to prevent contributing further to the diversion problem in this country. Indeed, this is true regardless of the means used to divert controlled substances in the paper-based system, because electronic prescribing of controlled substances could, if not properly implemented, present another means of diversion in addition to those listed above. However, with proper controls, the risk of diversion can actually be reduced through the use of electronic prescriptions. Among the essential elements of such a system are ensuring that only DEA registrants electronically sign and authorize controlled substance prescriptions and that the prescription record cannot be altered without the alteration being detectable. A system that fails to provide verification of the signer's identity and authority to issue controlled substance prescriptions, and/or fails to ensure that alteration of the record is detectable, would create new routes of diversion that could be even harder to prevent and detect.

III. Current Requirements for Prescriptions for Controlled Substances

As noted above, 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 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 Controlled Substances Act, 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). The manual signature affixed to the controlled substance 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 authority to prescribe the controlled substance in question. 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 may be filled only by a pharmacist acting in the usual course of professional practice who is

---

Abuse Warning Network, 2005: National Estimates of Drug-Related Emergency Department Visits. DAWN Series D–29, DHHS Publication No. (SMA) 07–4256, Rockville, MD, 2007; *http://dawninfo.samhsa.gov/pubs/edpubs/default.asp.*

employed in a 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 must be initialed and dated by the pharmacist filling the prescription (21 CFR 1304.22(c)). Under many circumstances, pharmacists are required to note certain 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.

DEA requires 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(b), 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)). This system of records is unique in 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 relies on the records of these prescriptions in the conduct of investigations, DEA 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.

IV. Existing Electronic Prescription Systems

At present, there are more than 110 service providers that offer systems to generate electronic prescriptions and approximately 20 that handle the receipt of prescriptions at pharmacies.[5] The electronic capabilities of practitioners' offices and pharmacies and the systems used are considerably different. Both types of systems, however, can be classified in the same ways. Systems may be stand-alone software that only handle prescriptions or integrated into larger management systems. In general, pharmacy systems are part of larger pharmacy management systems. Most electronic prescription systems are now integrated into larger electronic health records (EHR) systems; existing stand-alone systems may be integrated into EHR systems in the future.[6] [7]

Systems may also be installed on a practice or pharmacy computers or may be operated by application service providers (ASPs). In the ASP model, the program is retained on the ASP servers and the user accesses the system using leased lines or over the Internet. The ASP retains the records generated. Many pharmacy systems are installed at the pharmacy, but larger chains often operate like an ASP, holding the records on a central server that any pharmacy in the chain may access. Many practitioner stand-alone electronic prescription systems are ASPs. Because practitioners want to be able to access the system when they are out of the office, access is usually over the Internet. Practitioners log on to the system using the same kinds of identification mechanisms as other online business sites (passwords, user IDs).

Pharmacy Systems. Almost all pharmacies have computerized prescription records, which are integrated into overall pharmacy management systems that process insurance claims and billings. When a pharmacy receives a prescription on paper or by phone, the pharmacist or technician keys the information on the prescription into the system; if the patient has had other prescriptions filled at that pharmacy, the patient's personal identifying information is already in the system and does not have to be rekeyed.

Many pharmacy systems have been reprogrammed to be able to capture the data from electronic prescriptions directly. Although many pharmacies have the ability to accept electronic prescriptions, few such prescriptions are sent currently. Many of the ''electronic prescriptions'' generated are in fact transmitted to the pharmacy as faxes or simply printed out and given to

[5] Estimates are based on the number of systems certified by SureScripts plus the number of electronic medical record systems certified by the Certification Commission for Health Information Technology.

[6] National Alliance on Health Information Technology, ''Report to the office of the National Coordinator on Health Information Technology on Defining Key Health Information Technology Terms'', April 28, 2008. *http://www.nahit.org/cms/images/docs/hittermsfinalreport_051508.pdf.*

[7] The National Alliance for Health Information Technology has defined the terms ''electronic Medical record (EMR),'' ''electronic health record (EHR),'' and ''personal health record (PHR).'' Both EMRs and EHRs are defined to be maintained by practitioners, whereas a PHR is defined to be maintained by the individual patient. The main distinction between an EMR and an EHR is the EHR's ability to exchange information interoperably. DEA's use of the term EHR in this rule relates to those records maintained by practitioners, as opposed to a PHR maintained by an individual patient, regardless of how those records are maintained.

the patient. Renewals are more likely to be handled electronically than original prescriptions. Nonetheless, the capability to accept electronic prescriptions is widespread in the pharmacy sector.

Practitioner Electronic Prescription Systems. Electronic prescription systems for practitioners have existed for a number of years, but are still not widely used. A Centers for Disease Control and Prevention (CDC) study of electronic medical record (EMR) system use in 2006 found that about 12 percent of physicians have the ability to send prescriptions electronically using their EMR system.[8] The number of those systems that are used or that generate true electronic prescriptions is unclear. A Rand Health study of 58 electronic prescribing systems found that only 58 percent allowed electronic transmission of the prescriptions (as a data file), while almost all produced printed prescriptions and most could generate faxes.[9] The CDC study indicated that the electronic prescribing function is one of the less used functions of EMRs.

As noted above, many electronic prescription systems are Web-based ASPs. The ASP maintains the records, which reduces the initial cost to the practice by limiting the investment in hardware and connections. The ASP enrolls a practice, issues keys or sets up other authentication mechanisms, which allow the practitioner to log onto the system from any location. Most ASP systems and some installed systems can be accessed using PDAs and other handheld devices. Because many office staff may need to access the systems, many service providers also set different levels of authority so that only practitioners may sign prescriptions; the ability to support varying access levels is a requirement for EHR certification for systems certified by the Certification Commission for Healthcare Information Technology (CCHIT). Over the long term, it is generally assumed that stand-alone electronic prescription systems will be integrated into or replaced by electronic health record (EHR) systems. In this way, data on prescriptions will be automatically added to a patient's records. This shift to EHRs is occurring rapidly. Of the 119 systems certified by SureScripts or CCHIT at the end of 2007, 103 were EHRs. DEA welcomes comments on the protections currently implemented in the systems referenced above to protect against noncontrolled substance prescription forgery, fraud, and other related crimes, and what risk-mitigating controls are in place.

DEA also seeks comment as to whether up-to-date information or statistics are available regarding physicians' ability to send noncontrolled substance prescriptions electronically using their EHR systems and usage of such system functionality. When providing comments regarding this or any other request in this NPRM, commenters should clearly cite the source of the information, the origin of the data, the methodology or analytical techniques used to derive the information, and the limitations of the information, so that DEA may determine the quality, objectivity, utility, and integrity of any data or information provided.

Intermediaries. With so many electronic prescription systems and pharmacy systems, the issue of interoperability is critical. Electronic prescriptions will be of limited value to pharmacies if their systems cannot read the prescription and translate the data directly into their databases. To deal with this issue, the National Council for Prescription Drug Programs (NCPDP) has established a standard format for prescriptions, NCPDP SCRIPT standard in XML (current version is 10, but version 8.1 is the standard that Medicare specifies). Despite the standard, interoperability problems are likely to continue as both practitioner and pharmacy systems may be using different platforms and different versions of SCRIPT. At present, the interoperability problem is solved by using intermediaries that reformat the prescription so that the receiving pharmacy will be able to process it electronically.

Electronic prescriptions are transmitted through not one, but a series of intermediaries. The first recipient, once the prescription is signed, may be the ASP or an aggregator that the electronic prescription system uses. This recipient assigns a trace number to the electronic prescription that becomes part of the prescription record. The ASP or aggregator generally will transmit it to SureScripts or a similar intermediary. SureScripts is a service established by the pharmacy industry to reformat the prescriptions so the receiving pharmacy's system can process them without rekeying the information. SureScripts certifies both pharmacy and practitioner service providers, to ensure that the data it receives will be translatable into other formats. SureScripts may transmit the reformatted electronic prescription directly to a pharmacy, the central server of a chain pharmacy, or the ASP pharmacy management system, which then routes the prescription to the pharmacy for ultimate dispensing. DEA welcomes comments on the protections currently implemented by intermediaries to protect against noncontrolled substance prescription forgery, fraud, and other related crimes, and what risk-mitigating controls are in place. DEA also welcomes comments regarding the current standards and practices used by network intermediaries to route noncontrolled substance electronic prescriptions and whether such networks allow or provide the capability to ''open'' an electronic prescription that is en route.

Hospitals. A final complexity to the electronic prescription network arises from practitioners who serve on the staff of hospitals. Two technical issues exist with any electronic prescriptions these practitioners may write. First, hospital electronic record systems are written in computer languages other than SCRIPT, often HL7. If a staff practitioner writes an electronic prescription for a patient to fill at a pharmacy outside of the hospital, the intermediaries or pharmacies have to be able to translate the electronic prescriptions from HL7 to their own computer system language. Second, staff practitioners are not required to register with DEA. They are allowed to issue prescriptions under the hospital DEA registration number with a hospital-assigned extension that identifies the specific person issuing the prescription. DEA does not dictate the format of the extension. In at least some cases, pharmacy computer systems have not been able to handle the extensions.

V. Potential Vulnerabilities That Need To Be Addressed To Prevent Electronic Prescribing From Contributing to the Diversion of Controlled Substances

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

Although DEA also supports electronic prescribing, the Administration faces some challenges as it moves into an electronic world. A recent study conducted for HHS by the

[8] Centers for Disease Control and Prevention, ''Electronic Medical Record Use by Office-Based Physicians and Their Practices: United States 2006.'' *Advance Data from Vital and Health Statistics*, Number 393, October 26, 2007.

[9] Wang, C. Jason *et al.*, ''Functional Characteristics of Commercial Ambulatory Electronic Prescribing Systems: A Field Study,'' *Journal of the American Medical Informatics Association*, 2005; 12:346–356.

American Health Information Management Association [10] noted that ''e-prescribing presents a new vulnerability because of the increased velocity of authenticated automated transactions.'' Unless an electronic prescription system is properly designed, DEA's ability to prevent diversion and take legal action against those who violate the CSA could be seriously undermined.

As discussed above, with the paper-based system, the paper records provide DEA and other law enforcement agencies with documents that can be used in legal actions to prove that a practitioner has issued prescriptions for other than legitimate medical purposes, that others have forged prescriptions, or that pharmacy records or inventories are inconsistent with prescriptions received. The necessity for presenting prescriptions to pharmacies and picking up the drugs also limits the scope of diversion when it occurs. In contrast, electronic prescriptions can be easy to create, transmit, and alter, often without leaving a trail that links the person forging or altering a prescription to the record. Not only practice and pharmacy staff, but also staff at any of the systems involved in creating, transmitting, and processing prescriptions could generate or alter prescriptions. With the Internet and mail order pharmacies, those bent on diversion gain the ability to send prescriptions to a large number of pharmacies with a few keystrokes.

DEA's concerns with the existing electronic prescription system are the following:

- Service providers do not always determine whether the people enrolling are legally permitted to issue prescriptions, let alone controlled substance prescriptions. Some service providers appear to enroll practices over the Internet; some require submission of copies of the person's DEA registration and State license. Such procedures provide no assurance that authority to issue controlled substance electronic prescriptions will not be granted to people who are not DEA registrants. The DEA registrant list, including DEA registration numbers, is publicly available. The DEA number also appears on each controlled substance prescription and in many cases is preprinted on prescription pads so that any patient receiving a prescription for any drug, regardless of whether it is a controlled substance, will have access to the number. State license information is readily accessible from online State databases. Office staff may have access to the originals to copy. Copies of registration and license certificates would be easy to generate and submit. Present service provider procedures do not protect a practitioner from someone inside or outside the practitioner's practice setting up an account and creating fraudulent prescriptions in the practitioner's name. Moreover, current system designs could also allow a practitioner to repudiate prescriptions written for the purpose of diversion.
- Some systems may not limit who within a medical practice can ''sign'' prescriptions. Many staff at practices may have legitimate needs to access the system; only some have a legal right to sign prescriptions. Unless systems limit the ''signing'' function to practitioners with a legal right to issue prescriptions and provide unique identifiers that make it possible to determine who signed the prescription, taking enforcement action against practitioners who issue illegal prescriptions will be impossible because DEA will not be able to prove beyond a reasonable doubt who signed the prescription. This problem is exacerbated because ''signing'' in an electronic prescription system is a function that is usually nothing more than a keystroke that indicates that the prescription is complete; there is no ''signature'' applied to the prescription. In some cases, there may not be a ''signing'' function, but simply a command to transmit. (The SCRIPT standard does not currently provide a field for an electronic signature or an indication that the prescription has been signed.)
- Access to systems is usually by means of easily shared or stolen information (passwords, user IDs). As William Winsley, Executive Director of the Ohio Board of Pharmacy testified at the DEA/HHS July 2006 public meeting, ''Passwords are useless as a means of computer security in a healthcare setting.'' Too many people are in the vicinity of computers in practice offices to be certain that a password has not been compromised. If passwords or PINs are the only means of authentication for an electronic prescription system, law enforcement agencies will not be able to prove beyond a reasonable doubt who signed an electronic prescription. Practitioners will be able to repudiate prescriptions by saying that someone must have used their passwords.
- Once created and signed, electronic prescriptions pass through several intermediaries, all of which may open the record. Although this process is usually handled without individuals accessing the record, there is no guarantee that they could not do so. Most identity theft occurs not from people hacking into systems, but rather from insiders who know how to manipulate the system. Paul Donfried of SAFE BioPharma [11] and Strategic Identity Group noted at the July 2006, DEA/HHS public meeting: ''It generally is not the cryptography or the firewalls or the audit logs or the data centers that people attack. It is whatever the weak link in the chain is, which normally is the human beings who are responsible for keeping the stuff running and operating correctly.''
- The processing of the prescriptions by multiple parties could mean that law enforcement would have to prove that none of the parties altered the document. This requirement could substantially increase the cost of bringing cases against registrants who are diverting controlled substances as well as burden the service providers and intermediaries, which would have to produce audit trail records and experts to testify.
- The records of the prescriptions are often held by the service providers and intermediaries, not the pharmacies. With paper records, DEA and other law enforcement agencies have the right to inspect and remove records from pharmacies. With electronic records held by service providers and others, DEA and other agencies would have to subpoena records from the third parties—nonregistrants over whom law enforcement may have limited jurisdiction. Although this is a lesser problem for DEA, it could pose a substantial barrier to State and local law enforcement, which would be in the position of having to find other agencies willing to serve subpoenas on service providers who were located in other States.
- Records of electronic prescriptions at pharmacies and at intermediaries may be stored as strings of data, not as easily read text. These records must be able to be downloaded into a format that is easily read and manipulated by law enforcement.

DEA is convinced that its concerns can be addressed without creating insurmountable barriers to electronic prescribing. DEA's requirements in developing this proposed rule are the following:

- The approach must meet DEA's statutory mandates. Only DEA registrants may be granted the authority

[10] American Health Information Management Association, ''*Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities,*'' [September 2005] p. 45.

[11] SAFE BioPharma is an organization ''that created and manages the SAFE digital identity and signature standard for the pharmaceutical and healthcare industries.''

to sign controlled substance electronic prescriptions.

- 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.
- Electronic prescriptions must include all information required for paper controlled substance prescriptions.
- The prescription records must be reliable enough to be used in legal actions without having to substantially expand the number of witnesses that need to be called to verify records.
- The pharmacy system must allow annotation of the records as required for paper prescriptions and must indicate who made each annotation.
- The security systems used by any of the service providers must, to the greatest extent possible, prevent the possibility of insider creation or alteration of controlled substance prescriptions.

In addition, DEA wishes to adopt an approach that is flexible enough that future changes in technologies will not make the system obsolete or lock registrants into more expensive systems. DEA notes that its requirements do not relate to most of the functions of electronic prescribing systems. Other than requiring that the electronic prescription contain the basic information that any controlled substance prescription must contain (and that most prescriptions contain), DEA is not concerned about the format or transmission standards, or any of the added functions (formulary checks, clinical support, medication histories) available in electronic prescribing systems.

Further, as DEA notes throughout this document, the electronic prescribing of controlled substances is in addition to, not a replacement of, existing requirements for written and oral prescriptions for controlled substances. This proposed rule would provide a new option to prescribing practitioners and pharmacies. It does not change existing regulatory requirements for written and oral prescriptions for controlled substances. Prescribing practitioners will still be able to write, and manually sign, prescriptions for Schedule II, III, IV, and V controlled substances, and pharmacies will still be able to dispense controlled substances based on those written prescriptions and archive those records of dispensing.

VI. Alternatives Considered

In developing this rule, DEA considered a range of alternatives, from imposing virtually no requirements on existing systems to requiring systems using public key infrastructure. This section discusses the options considered and why DEA rejected some of them.

Allowing the use of any existing electronic prescription system without additional security. DEA considered whether to permit electronic prescribing of controlled substances using existing systems without any additional requirements. This would be the alternative most supported by service providers of existing electronic prescribing systems, as it would require no system modifications and would allow for the electronic prescribing of controlled substances as soon as a Final Rule permitting this activity became effective. Some have suggested that DEA permit the use of any existing system; if that system is used for diversion, DEA could then tighten its regulations later.

In discussing this alternative, and to understand why DEA rejected it, it first must be noted that any electronic prescribing systems currently being utilized are generally limited to noncontrolled substances as DEA regulations currently do not allow for the electronic prescribing of controlled substances.[12] Thus, any systems currently in place were not specifically tailored to the unique concerns relating to controlled substances—most notably the heightened need to prevent diversion of controlled substances as compared to noncontrolled substances. It is also important to understand the following regarding the current systems used to create, transmit, and process electronic prescriptions.

As discussed above, there are more than 100 vendors marketing systems to practitioners and about 20 marketing systems to pharmacies. These vendors range from start-ups with revenues of less than $1 million to a few very large corporations. There are at present no requirements for how these systems enroll practitioners, no requirements that they verify that the person enrolling is who he claims to be or is eligible to sign prescriptions. Some systems offer enrollment over the Internet. There are no requirements that prescriptions be signed only by someone authorized under State law to do so.

Some systems set access controls; others appear to grant general access to everyone in the office; in these systems, the prescription cannot be linked to a single practitioner. Many, perhaps most, of these systems allow access to prescription signing using nothing more than a password or a password/user ID, forms of identification that are easily compromised, especially in a healthcare setting where multiple staff use the same computers. Prescriptions could be created by anyone and signed by anyone. Some systems appear to rely on the good intentions of the practitioners' staff, a reliance that the high degree of insider medical identity theft and insider prescription forgery renders naïve at best.

There are no standards governing the security of the transmission of electronic prescribing systems currently being utilized. Therefore, while some of the intermediaries that handle prescriptions between the practitioner and pharmacy might have voluntarily implemented effective security measures, they are not legally obligated to do so and—in the absence of binding regulatory requirements—there is no way to ensure that they or others who might enter the market will have effective measures in the future. The intermediaries (up to five per transmission) are not required to keep records or audit trails although the best of them do. As ever, the weakest link can undermine the entire system. At the pharmacy, there are no requirements for audit trails or system security. Some pharmacy systems have good security practices, but others might not. Records could be created or altered without leaving a trace.

The existing system, in short, relies on the hope that vendors will employ good security practices; a few vendors may meet these, but others for simplicity or for economic reasons may choose to ignore them. The widespread reliance on simple passwords stored on computers available to any staff member undermines any claim of reasonable security controls. The existing voluntary certification bodies may help, but for transmission they only look at whether the system can interoperate with them. There is, in any case, no requirement that practitioners or pharmacies use only certified vendors; given the high costs of some certified systems, it would be surprising if some practitioners did not elect less expensive, uncertified solutions. Overall, the existing system provides no legal requirements for identity proofing, assurance of nonrepudiation, ability to authenticate the record, and record integrity. It exposes DEA registrants to the threat of

[12] DEA has granted an exception to its regulations to allow the United States Department of Veterans Affairs to conduct a pilot program involving the electronic prescribing of controlled substances using a system based on public key infrastructure (PKI) technology. PKI-based systems are discussed in greater detail later in this document.

identity theft, insider criminal activity, service provider or intermediary staff criminal activity, and potential criminal penalties for the actions of others that they will find hard to disprove. It creates a new high-speed route for widespread prescription forgery and diversion, which results in drug abuse and deaths. The idea that DEA should wait until this occurs before attempting to impose security requirements cannot be reconciled with the agency'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. Such an idea also fails to properly take into consideration the length of time required to change regulations.

For this alternative, the only way for the pharmacy, dispensing pharmacist, and DEA to ensure that the prescription a pharmacy received was, in fact, issued by the practitioner whose name and DEA registration number are on the prescription would be to require the pharmacy to call the practitioner and confirm each prescription. For DEA to allow a controlled substance prescription to be dispensed without this check would be to abdicate its statutorily mandated responsibilities. Although this alternative would impose the fewest burdens on service providers, it would be hugely expensive for practitioners and pharmacies, requiring up to 300 million callbacks a year. DEA has estimated the costs of this alternative, but DEA does not consider that the costs could be justified or that practitioners or pharmacies would adopt this alternative given the increased burden that it would represent.

Public Key Infrastructure. DEA considered proposing that all electronic controlled substance prescriptions be digitally signed using a digital certificate issued by a recognized Certification Authority. Under this approach, the prescription as signed and the digital signature would be sent to the pharmacy, which would be required to validate the prescription to ensure that it had not been altered after signature. This alternative would provide DEA and other law enforcement agencies with the best forensic evidence, and it would provide practitioners and pharmacies with the best protection against identity theft and forgeries, reducing their legal exposure. However, DEA has been advised that existing systems which follow the standards adopted by the Secretary of HHS pursuant to the MMA for electronic transmission of prescriptions and prescription-related information for covered Part D drugs prescribed for Part D eligible individuals are incompatible with the requirement of digitally signed prescriptions. Electronic prescriptions are processed through intermediaries that may reformat the prescriptions to ensure that the receiving pharmacy can capture the data; the reformatting makes validation of the record impossible. In addition, the intermediaries have expressed concern about incorporating the digital signature, which is usually at least 128 bits, within the current SCRIPT standard. Consequently, DEA does not consider this option to be a viable mandatory approach.

DEA considered and is proposing two options:

Electronically signed prescriptions with security controls. Under this alternative, practitioners would be required to undergo in-person identity proofing and submit documentation of that to a service provider. The identity proofing would be conducted by a DEA-registered hospital, a State licensing board, or State or local law enforcement agency. The service provider would be required to check the validity of the DEA registration and State license before issuing an authentication protocol to be used to sign controlled substance prescriptions. The authentication protocol would have to be two-factor, with one factor stored on a hard token (e.g., a PDA, a multifactor one-time-use password token, a thumb drive, a smart card). DEA would also impose certain system requirements related to the prescription elements and their presentation; most existing systems may already meet these requirements. The prescription would have to be transmitted immediately upon being signed and the service provider would have to digitally sign and archive the record before transmitting the plain text prescription to the intermediaries. The pharmacy would have to digitally sign and archive the prescription as received. The pharmacy system would need an internal audit trail to record any attempts to alter a record and conduct internal checks for such attempts. Both the electronic prescription service provider and the pharmacy system provider would need to obtain annual third-party audits for security and processing integrity. The service provider would have to generate a monthly log, which practitioners would be required to check for obvious anomalies. The rationale for each of the requirements is presented under the discussion of the proposed rule below.

Modified digitally signed prescriptions. Due to the current use of digital signatures by Federal health care systems, and the added security afforded by such signatures, DEA is proposing to allow practitioners that prescribe controlled substances at Federal health care facilities (e.g., Department of Veterans Affairs, Department of Defense) the additional option of using digital certificates, issued by such Federal agencies, to sign controlled substance prescriptions issued in the course of their official duties within those facilities. These Federal agencies would need to determine that the practitioner is authorized and registered, or exempted from the requirement of registration, to prescribe controlled substances. The private key would be required to be stored on a hard token. Federal agencies will already be meeting this requirement in issuing Personal Identification Verification (PIV) cards under Federal Information Processing Standard 201. Most of the system requirements would be the same as in the previous option except that the Federal agency could elect to allow the practitioner to digitally sign and archive the prescription once the DEA-required elements are complete and transmit later when other information has been added (e.g., retail pharmacy URL). The Federal agency would not have to digitally sign the record as transmitted. The pharmacy requirements would be the same. The digital signature would not be transmitted to the pharmacy; the pharmacy would not have to validate the record. However, if a Federal agency wished to include the digital signature as part of the transmission, DEA is permitting this alternative. In that case, the pharmacy would be required to validate the digital signature, but would not be required to digitally sign the prescription as received. Because a Certification Authority would issue the digital certificate and because record integrity is more assured with a digital signature, DEA would not require a check of a monthly log or third-party audits for security. The rationale for each of the requirements is presented under the discussion of the proposed rule below.

VII. Risk Assessment of Electronic Prescriptions for Controlled Substances

On December 16, 2003, the Office of Management and Budget (OMB) issued guidance to Federal agencies on e-authentication (M–04–04) that directed agencies to conduct e-authentication risk assessments to determine the level of authentication needed. It should be noted that M–04–04 was primarily intended to provide guidance to Federal agencies that utilize services through

the Internet, not private sector entities that do so. However, M–04–04 states: ''Private-sector organizations and state, local, and tribal governments whose electronic processes require varying levels of assurance may consider the use of these standards where appropriate.'' With this understanding, the document provides a useful illustration of how to identify and analyze the risks associated with the authentication process.

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. OMB established four levels of assurance:

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

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

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

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 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 document then specifies six categories of harm that might result from an authentication error:

- Inconvenience, Distress, or Damage to Standing or Reputation
- Financial Loss
- Harm to Agency Programs or Public Interests
- Unauthorized Release of Sensitive Information
- Personal Safety
- Civil or Criminal Violations

With respect to each of these six categories, the agency must assess the potential impact as ''low,'' ''moderate,'' or ''high.'' Table 1 showsOMB's impact criteria for each category of harm.[13]

TABLE 1.—M–04–04 POTENTIAL IMPACTS OF AUTHENTICATION ERRORS

	Low impact	Moderate impact	High impact
Potential Impact of Inconvenience, Distress or Damage to Standing or Reputation.	At worst, limited short-term inconvenience, distress or embarrassment to any party.	At worst, serious short-term or limited long-term inconvenience or damage to the standing or reputation of any party.	Severe or serious long-term inconvenience, distress or damage to the standing or reputation to the party (ordinarily reserved for situations with particularly severe effects or which may affect many individuals).
Potential Impact of Financial Loss	At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.	At worst, a serious unrecoverable financial loss to any party, or a serious agency liability.	Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.
Potential impact of harm to agency programs or public interests.	At worst, a limited adverse effect on organizational operations, assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness; or (ii) minor damage to organizational assets or public interests.	Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.	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.
Potential Impact of unauthorized release of sensitive information.	At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact, as defined in FIPS PUB 199.	At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a moderate impact, as defined in FIPS PUB 199.	At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a high impact, as defined in FIPS PUB 199.
Potential Impact to Personal Safety.	At worst, minor injury not requiring medical treatment.	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.	A risk of serious injury or death.
Potential impact of civil or criminal violations.	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.	A risk of civil or criminal violations that are of special importance to enforcement programs.

The Memorandum then states:

Agencies should then tie the potential impact category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of potential impacts identified. Thus, if five categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a Level 2 authentication. For example, if the misuse of a user's electronic identity/credentials during

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

a medical procedure presents a risk of serious injury or death, map to the risk profile identified under Level 4, even if other consequences are minimal.

Again, with the understanding that M–04–04 was not specifically designed to be used by Federal agencies when issuing regulations governing the general public, the logic and method of analysis employed by M–04–04 nonetheless serves as a useful model for completing DEA's task of determining the appropriate level of authentication for electronic prescribing of controlled substances. (In fact, DEA is unaware of any other Government documents that provide any such particularized guidance for completing this task.) For the proposed rule, the two aspects that are relevant to the e-authentication risk assessment are the identity-proofing and the storage of the authentication protocol or digital certificate. The following table presents the six categories of harm and impact using the three OMB-defined potential impact values to determine an identity authentication assurance level for the electronic prescribing of controlled substances (see Attachment A of the memorandum, ''E-Authentication Guidance for Federal Agencies'').

TABLE 2.—IMPACT OF HARMS OF ELECTRONIC PRESCRIPTIONS FOR CONTROLLED SUBSTANCES

Potential impact of authentication errors	DEA rating, OMB description	Comment
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.	Identity theft, issuing of illegitimate prescriptions in a practitioner's name, or alteration of prescriptions could expose practitioners to legal difficulties and force them to prove that they had not enrolled in an electronic prescription system or issued specific prescriptions.
Financial Loss	N/A	
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.	Not to place such strict requirements on authentication protocols used to sign electronic controlled substances prescriptions would open the electronic prescribing system for controlled substances to rampant diversion—diversion which would be very difficult for DEA to detect because of the breadth of the potential problem. Were the authentication protocol of a practitioner compromised, and were controlled substances prescriptions to be diverted for illicit purposes based on that compromised authentication protocol, such diversion would undermine the effectiveness of 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 closed system of distribution of the United States created by the CSA and supported by international treaty obligations.
Unauthorized release of Sensitive Information.	N/A	
Personal Safety	High—A risk of serious injury or death.	Congress expressly declared in enacting the CSA that the ''improper use of controlled substances [has] a substantial and detrimental effect on the health and general welfare of the American people.'' (21 U.S.C. 801(2)). Diversion and abuse of controlled substances results in a large number of deaths and medical visits each year; facilitating diversion can be expected to increase the level of abuse and harm.

TABLE 2.—IMPACT OF HARMS OF ELECTRONIC PRESCRIPTIONS FOR CONTROLLED SUBSTANCES—Continued

Potential impact of authentication errors	DEA rating, OMB description	Comment
Civil or Criminal Violations	High—A risk of civil or criminal violations that are of special importance to enforcement programs.	Given the framework of the CSA and DEA's core mission to enforce the Act, there is perhaps nothing of greater importance among DEA's administrative responsibilities than ensuring that controlled substances are dispensed only by registered practitioners. 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 distribution of controlled substances and is a violation under 21 U.S.C. 841(a)(1). The person writing an illegitimate prescription could be criminally prosecuted; penalties for such a conviction could include imprisonment and/or fines. Because of the number of persons having access to an electronic prescription between the time it is written and the time it is dispensed, including the practitioner's office staff, intermediaries who process the prescription, and the pharmacy staff, the potential for alteration is great. A practitioner whose prescriptions were altered by someone else—office staff or staff at one of the intermediaries—could be subject to legal action in which the practitioner would have to prove that he was not responsible for the prescriptions to avoid civil or criminal liability. If a pharmacy knowingly dispenses a forged or altered prescription, such dispensing constitutes illegal distribution and is a violation of the CSA. The pharmacy could be subject to administrative, civil, or criminal action under the CSA. A criminal conviction for unlawful dispensing in violation of the CSA is a felony that could, depending on the schedule of the controlled substance involved, and the harm resulting, result in a sentence of a lengthy period of incarceration and substantial fine. Even without a criminal conviction, civil violations of the CSA can result in substantial fines. Criminal or civil violations of the CSA might also result in revocation of the pharmacy's registration to dispense controlled substances.

DEA welcomes comments regarding its assessment of risk for the six categories of harm for the electronic prescribing of controlled substances. Commenters should frame their comments in the context of the impacts of those categories of harm included in OMB M–04–04 and Table 1 above.

OMB provides the following guidance in M–04–04 on applying the risk assessment to assurance levels.

TABLE 3.—MAXIMUM POTENTIAL IMPACTS FOR EACH ASSURANCE LEVEL

	Level 1	Level 2	Level 3	Level 4
Potential Impact of Inconvenience, Distress, or Damage to Standing or Reputation.	Low Impact	Moderate Impact	Moderate Impact	High Impact.
Potential Impact of Financial Loss	Low Impact	Moderate Impact	Moderate Impact	High Impact.
Potential impact of harm to agency programs or public interests.	n/a	Low Impact	Moderate Impact	High Impact.
Potential Impact of unauthorized release of sensitive information.	n/a	Low Impact	Moderate Impact	High Impact.
Potential Impact to Personal Safety	n/a	n/a	Low Impact	Moderate Impact.
Potential impact of civil or criminal violations ...	n/a	Low Impact	Moderate Impact	High Impact.

The table below shows the potential impact as rated by DEA and the assurance level associated with each.

TABLE 4.—POTENTIAL IMPACT AND ASSOCIATED ASSURANCE LEVELS FOR ELECTRONIC PRESCRIPTIONS FOR CONTROLLED SUBSTANCES

Potential impact—DEA rating	Level of assurance
Inconvenience, Distress, or Damage to Standing or Reputation—Moderate.	Level 2.
Financial Loss—N/A	N/A.
Harm to Agency Programs or Public Interests—High.	Level 4.

TABLE 4.—POTENTIAL IMPACT AND ASSOCIATED ASSURANCE LEVELS FOR ELECTRONIC PRESCRIPTIONS FOR CONTROLLED SUBSTANCES—Continued

Potential impact—DEA rating	Level of assurance
Unauthorized release of Sensitive Information—N/A.	Level 1.
Personal Safety—High	Level 4.
Civil or Criminal Violations—High	Level 4.

If any one or more of the potential impact categories for authentication errors is found to be high, M–04–04 directs agencies that the appropriate assurance level must be ''Level 4'' (the highest level). Indeed, DEA notes that M–04–04 specifically lists the following as an example of a situation for which Level 4 is appropriate:

> A Department of Veteran's Affairs pharmacist dispenses a controlled drug. She would need full assurance that a qualified doctor prescribed it. She is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount.[14]

The explanation provided in the above example is no less applicable where the pharmacist is employed by the private sector. Even if such risk is essentially identical for both VA pharmacies and private sector pharmacies, the reasoning of M–04–04 indicates that Level 4 assurance is appropriate in both scenarios.

NIST Special Publication (SP) 800–63, Electronic Authentication Guideline, provides guidance on applying the OMB assurance levels to identity proofing and authentication. Identity proofing is the process of determining whether the person being granted authorization to use a system is, in fact, the person he claims to be. Authentication refers to the method by which the person is then granted access to a computer system (e.g., PINs, passwords, biometrics). NIST SP 800–63 defines the steps needed to conduct identity proofing and establish authentication protocols for each OMB assurance level. DEA has used NIST SP 800–63 as a guideline in developing its proposed requirements.

Assurance Levels—Identity Proofing. Identity proofing is the process of uniquely identifying a person. NIST SP 800–63 specifies a number of requirements for both remote and in-person identity proofing for each assurance level.

DEA believes that in-person identity proofing is critical to the security of the electronic prescribing of controlled substances. Ensuring that only licensed and registered practitioners are granted the authority to sign electronic prescriptions for controlled substances is the first step to maintaining the overall security of the electronic prescribing system for these substances. At present, some service providers appear to allow enrollment over the Internet and only require the applicant to submit a copy of the State license and DEA registration. This type of enrollment increases the potential for identity theft and the creation of fraudulent identities of prescribing practitioners and, subsequently, the potential for issuance of forged prescriptions. DEA welcomes comment regarding the enrollment processes service providers have developed to adequately determine whether the people enrolling in such services are legally permitted to issue noncontrolled substance prescriptions and whether and how such processes prevent noncontrolled substance prescription forgery, fraud, and other related crimes.

In-person identity proofing protects individual prescribing practitioners from identity theft. That is, without in-person identity proofing, it would be very easy for anyone to claim to be an individual prescribing practitioner and gain access to electronic prescribing systems for controlled substances; the most likely documents used to demonstrate identity as a prescribing practitioner—State license and DEA registration—can be easily obtained. Persons who work with prescribing practitioners have ready access to State licenses and DEA registration certificates as those documents are often stored at the prescriber's practice location. A member of the office staff could alter a practitioner's registration certificate or merely submit a copy of a practitioner's State license and DEA registration and begin issuing illegal prescriptions without the practitioner's knowledge. As information regarding State licensure and DEA registration is publicly available, people outside the office could create fraudulent DEA registration certificates and State licenses using legitimate numbers and gain access to the system.

Unlike written prescriptions, once a fraudulent identity has been established, electronic prescribing provides little or no indication of the potential for fraud. With written prescriptions, if a person not knowledgeable of prescription-writing styles and tendencies writes or alters prescriptions, those prescriptions are likely to be noticed by a pharmacist who may scrutinize them further. In fact, if the prescription seems out of the ordinary in any way, e.g., the format is unusual, the paper is different from normal, the signature looks wrong, the directions are not in the usual format, the drug name is misspelled, the abbreviations used are not standard, or the quantity seems high, the pharmacy has a responsibility to contact the prescribing practitioner to verify the prescription before filling the prescription. With electronic prescribing, however, once an identity is established, all electronic prescriptions appear the same. Most information is selected from drop-down menus, and there is little to distinguish an electronic prescription written by a person who is not a legitimate prescribing practitioner from one that is written by an individual granted proper State and DEA authority to prescribe controlled substances.

Based on DEA's decision that in-person identity proofing is critical to the overall security of the electronic prescribing system, DEA examined NIST requirements for in-person identity proofing.

Briefly, at Level 2, in-person identity proofing requires the applicant to possess a government-issued photographic identification that confirms the address of record or nationality. Level 2 requires inspection of the photographic identification, and the recording of the applicant's address or date of birth and the number associated with the government-issued photographic identification. If the identification confirms the address of record then credentials are issued and notice is sent to that address; if the address is not confirmed, then credentials are issued in a manner that confirms the address of record.

At Level 3, in-person identity proofing requires the applicant to possess a government-issued photographic identification. Level 3 requires inspection of the photographic identification and verification, through the issuing government agency or through credit bureaus or similar databases, that the information contained in the identification (e.g., name, address, date of birth) are consistent with the application. The applicant's name, address, and date of birth are recorded. If the identification confirms the address of record then credentials are issued and notice is sent to that address; if the address is not confirmed, then credentials are issued in a manner that confirms the address of record.

At Level 4, two independent forms of photographic identification or accounts must be verified, one of which must be a government-issued photographic identification. Further, a new recording of a biometric of the applicant must be captured. The government-issued photographic identification must be verified with the issuing government agency. For any form of photographic identification, the applicant's name, address, and date of birth are recorded.

[14] Although OMB M–04–04 describes a Department of Veterans Affairs pharmacist needing ''full assurance that a *qualified doctor* prescribed [the controlled substance]'' [emphasis added], DEA recognizes that in addition to physicians, the Department of Veterans Affairs also employs dentists and certain mid-level practitioners who are authorized to prescribe controlled substances.

If the secondary form of identification is a financial account, the financial account number must be verified through record checks sufficient to identify a unique individual. The biometric is recorded to ensure that the applicant cannot repudiate the application. Credentials must be issued in a manner that confirms the address of record.

After careful examination of all levels of in-person identity proofing, DEA determined that none of the NIST levels addressed its unique needs and requirements. DEA does not believe that capturing a biometric at the time of enrollment is necessary, as is required at Level 4. Further, DEA does not believe that verification of identity through use of credit bureaus or other third-party agencies would be feasible or is necessary, as is required at Level 3, given that practitioner's State licenses and DEA registrations are also being examined. DEA believed that such requirements could be intrusive for practitioners, who might not want hospitals, State licensing boards, or law enforcement agencies—the entities DEA is proposing to permit conduct in-person identity proofing—to review sensitive personal information such as address information retained by credit bureaus. Finally, DEA did not believe that the address checks required at Level 2 were useful for the purpose served by the in-person identity proofing DEA believes it must require. DEA notes that address checks generally mean address of residence, because that is the address listed on most forms of government-issued photographic identification, whereas prescribing practitioners will receive information and authentication protocols at their offices, which are the addresses listed on the DEA registration and State licenses.

Therefore, DEA has decided to propose in-person identity proofing consistent with, but not equivalent to, Level 3, as discussed below, but not link that in-person identity proofing to any specific NIST requirements.

DEA could not identify any mitigating factors that would enable it to propose remote identity proofing. Remote identity proofing relies on record checks, which would not prevent identity theft and may be more intrusive than the simple in-person requirements DEA is proposing. Remote identity proofing also relies on mailing credentials to the address of record, which would not prevent a member of the office staff from applying for access to the electronic prescribing system for controlled substances and intercepting the confirmation. The electronic world allows for far easier identity theft and can make it more difficult to identify diversion when it occurs. In contrast, when DEA or the States have discovered identity theft in the context of paper prescriptions, they have been able to prosecute the criminal using the paper trail created by fraudulent prescriptions. The paper prescriptions can prove who wrote them and, for the innocent practitioner, who did not write them. With electronic prescriptions, identities can be stolen, used to issue a large number of prescriptions, then dropped within days, leaving few if any traces, or worse, traces that link to a practitioner who then would have to prove that he or she was an innocent victim, not a criminal.

DEA is proposing to allow DEA-registered hospitals, State licensing boards, and State or local law enforcement agencies to review the identity documents and sign, with the applicant, a letter or form that states that the applicant is who the applicant claims to be. This approach should lessen the burden on service providers and ensure that practitioners will be able to have their documents checked locally.

Assurance Level—Authentication Protocol. NIST SP 800–63 defines tokens as the means that a person wishing to gain access to an electronic system uses to authenticate their identity. In electronic authentication, the person wishing to gain access authenticates to a system or application over a network by proving that he has possession of a token. Therefore, a token must be protected.

Authentication methods are described as one-factor, two-factor, or three-factor, or as something you know, something you have, and something you are. PINs and passwords are something you know; cards such as ATM cards are something you have; biometrics (fingerprints, iris scans, hand prints) are something you are.

NIST SP 800–63 describes a single-factor token as either something the person knows, something the person has, or a biometric. Single-factor tokens include:

- Memorized secret tokens (passwords, passphrases).
- Pre-registered knowledge tokens: responses to a question known by the user (pet's name, favorite color).
- Look-up secret tokens—the user is prompted by the system to look up information stored on a physical or electronic device (the secret may be printed on a card or stored in the computer); the information looked up has been shared between the user and the system being authenticated to.
- Out of band tokens—Receipt of a secret on a physical device separate from the system being authenticated to which is then used to log onto the system (e.g., a password is sent to a cell phone; the person who possesses the cell phone uses the password to log onto the system).
- Single factor one time password (OTP) device—a hardware device that spontaneously generates one time passwords, which usually change every 60 seconds. The one time passwords are used to log onto the system.
- Single factor cryptographic device—a hardware device that uses embedded cryptographic keys; authentication occurs by proving possession of the device.

NIST discussed the vulnerability of single-factor authentication methods, specifically passwords, in Special Publication 800–32:

> The traditional method for authenticating users has been to provide them with a personal identification number or secret password, which they must use when requesting access to a particular system. Password systems can be effective if managed properly, but they seldom are. Authentication that relies solely on passwords has often failed to provide adequate protection for computer systems for a number of reasons. If users are allowed to make up their own passwords, they tend to choose ones that are easy to remember and therefore easy to guess. If passwords are generated from a random combination of characters, users often write them down because they are difficult to remember. Where password-only authentication is not adequate for an application, it is often used in combination with other security mechanisms.
>
> PINs and passwords do not provide non-repudiation, confidentiality, or integrity. If Alice wishes to authenticate to Bob using a password, Bob must also know it. Since both Alice and Bob know the password, it is difficult to prove which of them performed a particular operation.[15]

Pre-registered knowledge tokens usually have answers that may be known by other people in an office. Look-up secrets are as vulnerable as passwords in a medical practice settings. Out-of-band tokens would take more time to use. Single factor hard tokens could be borrowed or stolen and used easily. No single factor approach, therefore, would provide the assurance DEA and the practitioners need.

NIST SP 800–63 describes two-factor tokens as tokens that use two or more factors to achieve authentication. Multi-factor tokens include:

[15] National Institute of Standards and Technology. Special Publication 800–32 *Introduction to Public Key Technology and the Federal PKI Infrastructure; February 26, 2001. http://csrc.nist.gov/*

• Multi-factor software cryptographic tokens—a cryptographic key is stored on a computer and requires activation through a second factor of authentication.

• Multi-factor one time password device—a software device, (e.g., PDAs) or a hardware device (e.g., a card, thumb drive, fob), that generates one time passwords for use in authentication and requires activation through a second factor of authentication, usually a password.

• Multi-factor cryptographic hardware device—hardware device that contains a protected cryptographic key and requires activation through a second authentication factor.

As NIST points out, the use of more than one factor for authentication to a system raises the difficulty of an attacker successfully attacking a system. The more factors used, the more effort it takes to break the system to gain entry.

Briefly, at Level 2, single-factor authentication is allowed. Some combinations of single-factor authentication are still considered Level 2 (e.g., passwords plus pre-registered knowledge tokens are still rated as Level 2).

At Level 3, some combinations of single-factor tokens are acceptable (e.g., a password plus a single-factor one time password device). In addition, a multi-factor software cryptographic device is considered Level 3; this device allows for the storage of the cryptographic key on a disk (e.g., a hard drive of a personal computer).

At Level 4, only two types of tokens are acceptable—a multi-factor one time password device or a multi-factor cryptographic device that is stored on a hard token (e.g., a smart card, a thumb drive).

DEA is proposing that the authentication protocol meet Level 4, which requires two factors, one of which is stored on a hard token, which could be a PDA, a cell phone, a smart card, a thumb drive, or multi-factor one time password token. DEA has determined that only Level 4 meets its requirements based on the risk assessment and on the problems that arise with Level 3, where one of the factors can be stored on a computer rather than a hardware device that the practitioner can possess, or Level 2, where only a single factor is required. NIST describes Level 4 tokens as follows: ''To achieve Level 4 with a single token or token combination, one of the tokens needs to be usable with an authentication mechanism that strongly resists man-in-the-middle attacks—this entails an electronic interface which may be placed under access control by the Claimant's (the person seeking to gain access to the system) operating system.'' [16] [17] DEA would like public comment on the present state of multi-factor tokens as implemented through multi-function devices such as PDAs, cell phones, smart cards, thumb drives and laptop computers.

As DEA is not proposing specific controls regarding the authentication process or the transmission of the prescription information, DEA believes that the security of the authentication itself is critical to bind the practitioner to the prescribing transaction. Level 4 authentication protocols protect the practitioner from the most likely ''attack,'' the use of his password or other token to access the system and issue prescriptions. Because Level 3 allows the storage of authentication protocols on office computers, the practitioner has no assurance that his authentication protocol will be safe or that he will be aware if it is compromised. From a law enforcement perspective, an authentication protocol stored on a computer to which others have access makes linking a prescription to a practitioner or to a staff member who has illegally issued prescriptions all but impossible. Level 4, where the practitioner can retain possession of the hard token, protects the practitioner and provides law enforcement with the necessary nonrepudiation.

Because of the attributes of medical practices, DEA could identify no mitigating factors that could overcome the vulnerabilities that exist and allow a lower level of assurance. In medical practices, most staff members have access to any of the computers in the office. Practitioners and nurses see patients in multiple examination rooms, moving from room to room; of necessity, practitioners must leave their offices and computers unattended for long periods of time. Passwords, which are usually part of two-factor authentication protocols to access the system, are vulnerable to attack because (1) many people write them down; (2) most people choose passwords that are easy to guess; and (3) in medical settings, with multiple people working in the vicinity of a computer, it is easy for someone else to watch a password being keyed into the system. If both parts of a multi-factor identification protocol can be stored on an office computer, or if there is only one factor needed (Level 2), the practitioner will have no assurance that someone in the office is not issuing prescriptions in his name. The practitioner will also be able to repudiate any prescription written in his name; law enforcement officials will not be able to prove beyond a reasonable doubt in a criminal proceeding that his authentication protocol had not been compromised. Storing one of the factors on a hard token means that the practitioner can retain possession of the device and ensures that it is not misused. The practitioner will not be able to repudiate prescriptions issued in his name; the practitioner will either have written the prescription, knowingly given the hard token to someone else, or, if the token was lost, stolen, or compromised, have taken appropriate actions (such as ensuring that the authentication protocol has been revoked to prevent its misuse).

The hard token protects the practitioner in the same way a manually signed written prescription does. If a written prescription is forged, a practitioner can prove that he did not write it by comparing handwriting. By maintaining sole possession of the hard token, the practitioner can eliminate the risk of fraudulent prescriptions and, if the token is lost, stolen, or compromised, he will be immediately alerted to the threat and have the authentication protocol revoked. This assurance that only a legitimate practitioner issued the prescription also protects the pharmacy. As discussed above, with a paper prescription there are potentially many indications that the prescription was not written by a practitioner. If the prescription seems out of the ordinary in any way the pharmacy has a responsibility to verify the prescription before filling the prescription. With electronic prescriptions, it will be much more difficult to identify these potentially telltale characteristics because the software fills in items from a menu of acceptable options; unless the quantity is high, the pharmacist will have little reason to question an electronic prescription.

The requirement for two-factor authentication (something you know and something you have) has been implemented by a number of healthcare systems. One system with almost 300 hospitals and clinics is using a

[16] National Institute of Standards and Technology. Special Publication 800–63–1 *Electronic Authentication Guideline* draft; February 20, 2008. p. 52.

[17] DEA notes that in the course of drafting this rulemaking, the National Institute of Standards and Technology issued a new draft Special Publication 800–63, which revises some guidelines regarding electronic authentication. DEA has taken these new guidelines into account in drafting this Notice of Proposed Rulemaking recognizing, however, that this Special Publication is a draft and subject to revision by NIST when the final SP 800–63–1 is issued.

combination of PINs (something you know) and a one-time-password token or software tokens (PDAs) for almost 30,000 users. Another medical center uses the same approach for more than 4,500 users. A third health care system with a variety of treatment centers has deployed this approach to 8,000 people at more than 40 sites. These deployments indicate that the requirement is feasible in healthcare settings and that it is flexible enough to provide access and access control as practitioners move among settings in which they practice.

Although the electronic prescribing of controlled substances plainly fits in the categories of transactions for which Level 4 assurance is warranted, DEA has decided, following interagency discussions, not to propose all of the authentication requirements that NIST SP 800–63 indicates are appropriate for Level 4. Among other things, as explained below, DEA is not proposing that practitioners digitally sign prescriptions or that pharmacies routinely validate prescriptions that are digitally signed because doing so would be incompatible with many existing systems currently in use for the electronic prescribing of noncontrolled substances. Nonetheless, DEA is proposing here an alternative authentication system that comes as close as reasonably possible to the level of security called for in NIST SP 800–63 while remaining compatible with existing systems used for noncontrolled substance prescriptions and, at the same time, adhering to DEA's overarching obligation to minimize the likelihood of diversion of controlled substances.

Assurance Level—Authentication Process. The authentication process addresses security between the creator of a message and its recipient. At Level 4, the authentication process involves strong cryptographic authentication of all parties and all sensitive data transfers. A variety of technologies can meet Level 2 and 3; the levels are defined by their resistance to certain forms of attack. Level 2 can be met with an encrypted TLS protocol session. Level 3 can be met with authenticated TLS and public key certificates.

DEA is not proposing to set any standards for the authentication process. The NIST requirements apply primarily to the transmission of information. DEA is concerned about the possibility that an electronic prescription could be altered during transmission, but the agency is not proposing specific regulations in this area at this time. DEA is proposing to address the vulnerabilities that exist by having the prescription digitally signed by the service provider prior to transmission and on receipt at the pharmacy. These requirements will not prevent alteration during transmission, but they will allow DEA to identify that it has occurred and protects registrants from being accused of issuing a fraudulent prescription or altering a legitimate prescription. DEA also notes that the security of these records during transmission is subject to HIPAA.

Summary. In conclusion, although the risk of electronic prescribing of controlled substances maps to Assurance Level 4 using the criteria of M–04–04, DEA is not proposing all of the requirements associated with that level. Instead, DEA is proposing in-person identity proofing specific to its needs; these requirements are consistent with, but not equivalent to, Level 3, and address concerns specific to DEA. Further, DEA is proposing use of a hard token, with that hard token meeting the requirements of Level 4. Finally, DEA is not proposing any requirements regarding the authentication process and transmission of the electronic prescriptions. The table below provides a summary of DEA's conclusions regarding its risk assessment of systems to permit the electronic prescribing of controlled substances.

TABLE 5.—SUMMARY OF RISK ASSESSMENT FOR ELECTRONIC PRESCRIPTIONS FOR CONTROLLED SUBSTANCES

M–04–04 Assurance Level	Level 4—High potential impact of harm to agency programs or public interests, personal safety, civil or criminal violations.
NIST identity proofing	In-person identity proofing requirements specific to DEA; requirements consistent with, but not equivalent to, NIST Level 3 in-person identity proofing.
NIST authentication protocol	Level 4—Use of hard token or multifactor one-time-use password token is necessary to bind the prescriber to the prescription.
NIST authentication process	N/A—DEA is not proposing any requirements in this area.

As has been discussed, DEA is proposing in-person identity proofing requirements consistent with, but not equivalent to, Level 3; authentication protocol requirements, use of a hard token and two-factor authentication, meeting the requirements of Level 4; and no requirements regarding the authentication process. DEA welcomes comments and information regarding alternative solutions for the electronic prescribing of controlled substances employing security controls that are as effective as those being proposed in this Notice of Proposed Rulemaking and also would meet DEA statutory and regulatory obligations under the Controlled Substances Act. Information provided should be as specific and detailed as possible to provide the Administration with an understanding of how the commenter believes the alternative solution could be implemented to satisfy the foregoing considerations. Any person providing such comments should discuss the specific risks being addressed and how any such risk-mitigating controls are incorporated into the alternative being discussed, and should state why the commenter believes such controls are adequate to address DEA's concerns. Any person providing such comments should also discuss the system vulnerabilities, risks, and weaknesses of any alternatives provided.

If a commenter believes that any proposed requirement is either too stringent or too lax, the commenter should so state, providing a detailed explanation of how the controls mitigate the identified risks, or how the lack of controls aggravate or fail to address the risks involved in the electronic prescribing of controlled substances and, thus, why the commenter's alternative warrants consideration as an alternative to the requirement being proposed. Hence all comments should clearly identify how all risk-mitigating compensating controls adequately address each security concern outlined in the proposed rule.

For example, DEA welcomes comments on the following topics:

- Whether in-person identity proofing requirements consistent with, but not equivalent to, Level 3, are sufficient to address DEA's concerns, or whether (a) more stringent requirements, such as those required under Level 4, are necessary, or (b) DEA's concerns could be addressed with Level 2 requirements combined with risk-mitigating controls.
- Whether authentication protocol requirements, use of a hard token and two-factor authentication, meeting the requirements of Level 4 are sufficient to

address DEA's concerns, or whether (a) more stringent requirements, such as those imposed in a public key infrastructure system, are necessary, or (b) DEA's concerns could be addressed with Level 3 requirements combined with risk-mitigating controls.

• Whether no requirements regarding the authentication process, as proposed in this rule, should cause DEA concern, such that imposing requirements is necessary.

VIII. Proposed Standards for Electronic Prescription Systems for Controlled Substances

The following discussion relates to requirements DEA is proposing regarding the creation, signature, transmission, processing and dispensing of controlled substance prescriptions. As discussed below, practitioners and pharmacies—DEA registrants—must use systems and service providers which comply with all requirements DEA may finalize. While these requirements pertain specifically to prescriptions for controlled substances, nothing in this rule precludes practitioners, pharmacies, or service providers from using these same standards for prescriptions for noncontrolled substances, if they so desire. However, DEA notes that any references throughout the following discussion relate solely to prescriptions for controlled substances.

In this rule, DEA is proposing various security requirements for systems and service providers that market software and services to practitioners and pharmacies to create, sign, transmit, process and dispense electronic controlled substance prescriptions. It is incumbent upon DEA registrants—practitioners and pharmacies—the entities regulated by DEA, to use systems and service providers that comply with DEA security requirements for the electronic prescribing and dispensing of controlled substances. DEA recognizes that its registrants may not be able to evaluate a service provider's compliance and so is establishing third-party audit and other requirements to assist registrants in determining whether a system or service provider they currently use, or are considering using, meets DEA security requirements. While this preamble and rule require actions of service providers, it is the DEA-registered practitioner or pharmacy DEA will look to if the system or service provider that practitioner is using is not in compliance with DEA regulations. It is, ultimately, the DEA-registered individual practitioner and pharmacy who are responsible for the prescribing and dispensing of any controlled substance prescription, and the requirements of this rule do not change that longstanding responsibility and liability.

DEA is proposing the following requirements for the use of electronic systems to create, sign, dispense, and archive controlled substance prescriptions, which are discussed in detail below:

• The electronic prescription service provider must receive a document prepared by an entity permitted to conduct in-person identity proofing of prescribing practitioners regarding the conduct of the in-person identity proofing. The document may be prepared on the identity proofing entity's letterhead or other official form of correspondence, or the service provider may design a form for use by the identity proofing entity. Regardless of the format, the document must contain certain information required by DEA. Entities DEA is proposing to permit conduct in-person identity proofing of prescribing practitioners include:

○ The entity within a DEA-registered hospital that has previously granted the practitioner privileges at the hospital (e.g., a hospital credentialing office);

○ The State professional or licensing board, or State controlled substances authority, that has authorized the practitioner to prescribe controlled substances;

○ A State or local law enforcement agency.

○ The service provider must check both the practitioner's State license and DEA registration to determine that both are current and in good standing.

• Authentication: Access to the electronic prescribing system for the purposes of signing prescriptions must meet the standards for Level 4 authentication in NIST SP 800–63. That is, the system must require at least two-factor authentication to access the system; one factor must be a cryptographic key stored on a hard token that meets the requirements for Level 4 authentication in NIST SP 800–63 or a multi-factor one time password token. The hard token must be a hardware device that meets the following criteria:

○ The token must require entry of a password or biometric to activate the authentication key.

○ The token is not able to export the authentication key.

○ The token must be validated under Federal Information Processing Standard (FIPS) 140–2 as follows:

■ Overall validation at Level 2 or higher.

■ Physical security at Level 3 or higher.

• The security of the system must be audited annually using a third-party audit that meets the requirements of a SysTrust or WebTrust audit for security and processing integrity.

• The system must limit signing authority to those practitioners that have a legal right to sign prescriptions for controlled substances (i.e., the system must set varying levels of access to the system based on responsibilities).

• The system must have an automatic lock out if the system is unused for more than 2 minutes.

• The prescription must contain all of the required data (date of issuance of the prescription; patient name and address; registrant full name, address, DEA registration number; drug name, dosage form, quantity prescribed, and directions for use; and any other information specific to certain controlled substances prescriptions mandated by law or DEA regulations). Prior to signing the controlled substance prescription, the system must show the prescribing practitioner at least the patient name and address, drug name, dosage unit and strength, quantity, directions for use, and the DEA number of the prescriber whose identity is being used to sign the prescription.

• Where more than one prescription has been prepared for signing, prior to authenticating to the system the practitioner must positively indicate which prescription(s) are to be signed.

• The practitioner must authenticate himself to the system immediately before signing a prescription.

• After authenticating to the system but prior to transmitting the prescription, the system must present the practitioner with a statement indicating that the practitioner understands that he is signing the prescription being transmitted. If the practitioner does not so indicate, by performing the signature function, the prescription cannot be transmitted.

• The system must transmit the electronic prescription immediately upon signature. The system must not transmit a controlled substance prescription unless it is signed by a practitioner authorized to sign such prescriptions.

• The electronic data file must include an indication that the prescription was signed.

• The system must not allow printing of prescriptions that have been transmitted; if a prescription is printed, it must not be transmitted.

• The system must generate a monthly log of controlled substance prescriptions and transmit it to the

practitioner for his review. The practitioner must indicate that the log was reviewed. A record of that indication must be maintained for five years.

- The first recipient of the prescription must digitally sign the prescription and archive the digitally signed version of the prescription as received.
- The first pharmacy system that receives the prescription must digitally sign and archive a copy of the prescription as received. Alternatively, the intermediary that transmits the prescription to the pharmacy may digitally sign the transmitted prescription and transmit both the record and the digitally signed copy for the pharmacy to archive.
- The digital signatures must meet the requirements of FIPS 180–2 and 186–2.
- The pharmacy system must check to determine whether the DEA registration of the prescribing practitioner is valid. (Alternatively, any of the intermediary systems may conduct this check provided that the record indicates that the check has been conducted. The CSA database may be cached for one week from the date of issuance by DEA of the most current database.)
- The pharmacy system must be able to store the complete DEA number including extensions.
- The pharmacy system must have an audit trail that identifies each person who annotates or alters the record. The pharmacy system must conduct daily internal audits to identify any auditable events.
- The system must have a backup system of records stored at a separate location.
- The pharmacy system must have a third-party audit that meets the requirements of SysTrust or SAS 70 audits for security and processing integrity.
- The contents of a controlled substance prescription must not be altered, other than by reformatting, during transmission.
- A prescription created electronically for a controlled substance must remain in its electronic form throughout the transmission process to the pharmacy; electronic prescriptions may not be converted to other transmission methods, e.g., facsimile, at any time during transmission.

DEA would like the public to comment on the ability of those members of industry currently providing electronic prescribing systems for noncontrolled substances to meet the requirements set forth in this proposed rule, and whether there might be entrepreneurs not currently providing electronic prescribing systems who would be willing and able to develop innovative systems that would meet the requirements proposed here.

Other Requirements

In addition to the system requirements, DEA is proposing to require the following:

- A registrant must have separate password/keys for each DEA registration he holds and uses to issue prescriptions. Multiple keys may be stored on the same hard token.
- The registrant must use the appropriate DEA registration for prescriptions issued. Practitioners holding multiple registrations in a single State may use just one for any prescription written in that State.
- The registrant must retain sole possession of the hard token. If a token is lost or compromised and the registrant fails to notify the service provider within 12 hours of discovery, the registrant will be held responsible for any prescriptions written using the token.
- The pharmacy must annotate the record with the same information required for a paper prescription.
- The practitioner and pharmacist must notify DEA and the service provider if they identify problems in the logs they review that indicate that prescriptions have been created without their knowledge or altered.

Discussion of the Proposed Rule System Requirements

As noted previously, electronic prescribing is in addition to existing prescribing methods for controlled substances. DEA's goal is to impose as few new requirements on electronic prescription systems as possible while retaining the ability to enforce the Controlled Substances Act and its implementing regulations. Many of the requirements listed above exist in at least some systems currently in use. The Certification Commission for Health Information Technology EHR certification standards for security cover many of the access and authentication requirements DEA is proposing here. DEA believes that the proposed requirements will protect both practitioners and pharmacies by ensuring that they can meet their legal obligations and lessen the threat of someone misusing their authorities to divert controlled substances. DEA emphasizes that its electronic prescription requirements do not alter the responsibilities of the practitioner and pharmacy in regard to controlled substance prescriptions. Both the prescribing practitioner and the dispensing pharmacy have a legal responsibility to ensure that only prescriptions issued for legitimate medical purposes by DEA registrants acting in the usual course of their professional practice are dispensed. A practitioner who knowingly allows someone to issue prescriptions in the practitioner's name is legally responsible for those prescriptions. A pharmacy that fails to check the validity of a controlled substance prescription before dispensing is legally responsible if the prescription is invalid.

In-person identity proofing. DEA considered requiring service providers to conduct in-person identity proofing of prescribing practitioners as part of their enrollment process. However, after careful consideration, DEA determined that in-person identity proofing by service providers created certain vulnerabilities which could not be overcome. Specifically, DEA was concerned that by requiring service providers to both identity proof practitioners and issue practitioners access to the electronic prescribing system to prescribe controlled substances, the entire system was vulnerable to compromise. Without separation of the identity and enrollment tasks, it could be quite easy for service provider staff to create a fraudulent identity and enroll that identity in the electronic prescribing system. While some service providers have asserted that their staffs are trustworthy, DEA did not want to establish a system which could be easily subverted for the diversion of controlled substances. Further, DEA was concerned that such a system may prove to be inconvenient for prescribing practitioners and service providers alike. Although DEA believes that many service providers would be on site at practitioners' offices routinely due to the complexity of the EHR systems of which electronic prescribing is often a part, DEA recognizes that conducting enrollment activities at that time may be inconvenient. Practitioners may not be at the practice location when the service provider staff is present. If enrollment could not occur, service providers' staff would have to make separate trips specifically for in-person identity proofing. Such trips could be difficult depending on the location of the service provider as compared to the practitioner.

To address DEA's concerns that the identity proofing and enrollment functions not reside within the same entity, and to ensure that practitioners have ready access to the entities

permitted to conduct in-person identity proofing, DEA is proposing that the following entities may conduct in-person identity proofing:

- The entity within a DEA-registered hospital that has previously granted that practitioner privileges at the hospital (e.g., a hospital credentialing office);
- The State professional or licensing board, or State controlled substances authority, that has authorized the practitioner to prescribe controlled substances;
- A State or local law enforcement agency.

DEA is proposing that before a service provider grants access to the electronic prescription system for the prescribing of controlled substances, the service provider must receive a document prepared by one of the above-listed entities regarding the conduct of the in-person identity proofing. DEA is proposing two alternatives for the format of the identity proofing document: The document may be prepared on the identity proofing entity's letterhead or other official form of correspondence, or the service provider may design a form for use by the identity proofing entity. Regardless of the format, the document must contain all of the following information:

- The name and DEA registration number, where applicable, of the entity which conducted the in-person identity proofing of the practitioner;
- The name of the person within the entity who conducted the in-person identity proofing of the practitioner;
- The name and address of the practitioner whose identity is being verified;
- For each State in which the practitioner wishes to prescribe controlled substances electronically, the name of the State licensing authority and State license number of the practitioner whose identity is being verified;
- Except for individual practitioners who prescribe controlled substances using the DEA registration of the institutional practitioner, for each State in which the practitioner wishes to prescribe controlled substances electronically, the DEA registration number and date of expiration of DEA registration of the practitioner whose identity is being verified;
- For individual practitioners who prescribe controlled substances using the DEA registration of the institutional practitioner, a statement by the institutional practitioner acknowledging the authority of the individual practitioner to prescribe controlled substances using the institution's DEA registration, and the specific internal code number assigned to the individual practitioner;
- The type of government-issued photographic identification checked (e.g., the practitioner's driver's license, passport) and a statement that the photograph on the identification matched the person presenting the photographic identification;
- The date on which the practitioner's in-person identity proofing was conducted;
- The signature of the person within the entity who conducted the in-person identity proofing;
- The signature of the practitioner who is the subject of the in-person identity proofing.

Before granting the practitioner access to the system to sign controlled substances prescriptions, the service provider must check with each State and DEA to determine that the practitioner's State license to practice medicine is current and in good standing. In those States in which a separate controlled substance registration is required to prescribe controlled substances, the service provider must also check with the appropriate State authority to determine that the practitioner's State license is current and in good standing. Finally, to ensure that the application to gain access to sign controlled substances is legitimate, the service provider must contact the prescribing practitioner at the practitioner's registered location by telephone to confirm the practitioner's intent to apply to prescribe controlled substances using the service provider's system. The service provider must obtain the telephone number from a public source other than the application received from the practitioner. Alternatively, the service provider may confirm the practitioner's intent in person at the practitioner's registered location.

The service provider must retain the document regarding identity proofing in its files for five years. DEA recognizes that in-person identity proofing will add a step to enrollment, but anything less would make it easy to steal a practitioner's identity and issue fraudulent prescriptions. In-person identity proofing will protect practitioners from this type of abuse. The records may be maintained electronically.

DEA seeks comments on in-person identity proofing requirements, and those requirements' effects, if any, on practitioners, including those practicing at multiple locations. DEA also seeks comments regarding alternatives to in-person identity proofing that achieve the same or higher level of assurance as that which DEA is proposing here.

Authentication. As explained above in the risk assessment, DEA is proposing that the authentication protocol must be two-factor and meet NIST SP 800–63 Level 4 criteria. One factor must be stored on a hard token that meets the FIPS 140–2 standard for the cryptographic module.

The HIPAA Security Guidance issued by HHS on December 28, 2006, also recommends two-factor authentication, beyond a combination of password and user ID, although it does not detail how this should be implemented.[18] The standards for electronic health records system security developed by the Certification Commission for Healthcare Information Technology (CCHIT) require systems to support two-factor identification.[19] Consequently, all of the EHR systems certified by CCHIT (approximately 85 systems) already support two-factor authentication. The requirement to store the key on a token will not impose an incremental cost for these systems.

The highest form of protection would be three-factor authentication (something you know, something you have, and something you are), but given the difficulties that still exist in ensuring that biometric readers function accurately at all times, DEA decided not to require a biometric password. DEA notes that biometric authentication is not prohibited in this rule; DEA supports this method of authentication, but is not requiring it at this time. Practitioners may decide to use a biometric as one of the passwords; some systems, including some PDAs, have, or support the use of, a fingerprint reader for access control.

Federal Information Processing Standard (FIPS) 140–1/140–2 is a standard entitled ''Security Requirements for Cryptographic Modules.'' [20] The standard is issued by NIST to lay out general requirements for cryptographic modules for computer and telecommunications systems. These standards ensure that cryptographic modules, which protect information such as passwords and other records,

[18] HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information December 28, 2006; *http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf.*

[19] CCHIT Security Criteria 2007 Final 16 Mar 07; criteria S21. *http://www.cchit.org/files/Ambulatory__Domain/CCHIT_Ambulatory_SECURITY_Criteria_2007_Final_16Mar07.pdf.*

[20] National Institute of Standards and Technology. FIPS 140–2 ''Security Requirements for Cryptographic Modules'', May, 2001. *http://csrc.nist.gov/publications/PubsFIPS.html.*

are robust enough that ''breaking'' the encryption is generally not feasible. The FIPS standards have been adopted by the United States government and are required for all cryptographic-based security systems that are used by, or approved by, Federal agencies to protect unclassified information. DEA, therefore, must require that the software modules used comply with these standards. A list of vendors whose cryptographic modules have been validated as FIPS 140–2 compliant may be obtained from the NIST Web site at *http://csrc.nist.gov/cryptval/140–1/1401val.htm*. As of March 2008, more than 900 modules have been certificated as compliant. The vendors include providers of PDAs, cell phones (Palm, Blackberry, Nokia), one time password tokens, as well as network and software providers. (When the FIPS 140–1 standard was updated to 140–2, all modules approved under the 140–1 standard were grandfathered and are considered compliant under 140–2.)

DEA notes that practitioners are not required to learn cryptographic keys; a password entered into a hard token accesses the key, which the service provider then recognizes. From the practitioner's perspective, the only difference from the common security controls on computer systems is that one of the keys is stored on a token. If that token is a PDA, the practitioner may not see a difference from the existing electronic prescription systems except when the practitioner wants to use a personal computer, when he would need to connect the PDA to the computer to access the system.

Authentication protocol expiration and revocation. The practitioner's authentication protocol to sign controlled substances prescriptions is based on the validity of the practitioner's DEA registration and on the security of the hard token and password. DEA would require the service provider to revoke the practitioner's authentication protocol if the practitioner's DEA registration expires (unless the service provider determines that the registration has been renewed), is revoked, suspended, or terminated. DEA will make available to service providers information regarding the registration status of prescribing practitioners, including practitioners' names, addresses, DEA registration numbers, and dates of expiration for those DEA registrations. The service provider must check the DEA registration database at least once a week to ensure that the service provider has the most current DEA registration information. DEA will permit service providers to cache this information for one week from the date of issuance by DEA of the most current database. DEA seeks comment regarding the interval for updating by DEA of registration information to service providers.

Further, DEA is proposing to require the service provider to revoke the authentication protocol used to sign controlled substance prescriptions immediately upon receiving notification from the practitioner that a password or token has been compromised, lost, or stolen. In such cases, the service provider may issue a new authentication protocol to the practitioner.

DEA is interested in receiving comment regarding the current industry practices used to authenticate practitioners who use electronic prescribing systems for noncontrolled substances and whether and how such practices prevent noncontrolled substance prescription forgery, fraud, and other related crimes.

Access limitations and signing. DEA is proposing a series of requirements related to the creation, signing, and transmitting of controlled substance prescriptions:

- After authenticating to the system but prior to signing the controlled substance prescription, the system must present the practitioner with a statement indicating that the practitioner understands he is signing the prescription being transmitted. If he does not so indicate, the prescription must not be transmitted.
- The electronic prescription system must include a function that requires a practitioner to electronically ''sign'' the completed prescription prior to transmission. The prescription file must include an indication that the prescription was signed.
- The system must limit access to the signing function for controlled substances to practitioners authorized to sign controlled substance prescriptions.
- The system must transmit the prescription immediately upon signature.
- The system must not transmit the prescription unless it has been signed.

DEA wishes to ensure that the act of signing controlled substances prescriptions is clearly understood by the practitioner. Therefore, DEA is proposing to require that, after authenticating to the system but prior to signing the controlled substance prescription, the system must present to the practitioner certain information regarding controlled substances prescriptions being transmitted. Specifically, the system must display for the practitioner the patient's name and address; the name of the drug being prescribed; the dosage strength and form, quantity, and directions for use; and the DEA registration number under which the prescription will be authorized. While this information is displayed, the practitioner must be presented with the following statement (or its substantial equivalent): ''I, the prescribing practitioner whose name and DEA registration number appear on the controlled substance prescription(s) being transmitted, have reviewed all of the prescription information listed above and have confirmed that the information for each prescription is accurate. I further declare that by transmitting the prescription(s) information, I am indicating my intent to sign and legally authorize the prescription(s).'' The practitioner must positively indicate agreement with this statement. Such agreement can be accomplished through a check box or other means determined by the system. If the practitioner does not indicate agreement to this statement, the controlled substances prescriptions may not be transmitted.

DEA believes that such a statement is necessary to help to positively bind the practitioner to the prescription. DEA believes that this requirement is similar to many banking and online billing systems that require the user to agree to certain terms and conditions before billing or other financial transactions are permitted to occur. This statement will help to provide nonrepudiation of the prescriptions; that is, the inclusion of this statement will make it more difficult for the practitioner to deny having signed the controlled substance prescriptions.

Although the requirement for signing may seem obvious, signing is not currently an automatic part of electronic prescriptions. The standard that the industry has developed and HHS has adopted for the transmission of electronic prescriptions (the National Council for Prescription Drug Programs (NCPDP) SCRIPT) does not include a field that indicates that the prescription has been signed. Signing an electronic prescription does not create a record of the act of signing; it is simply a function that usually is linked to transmission. The SCRIPT fields clearly provide for cases where someone other than the practitioner creates and transmits a prescription under the practitioner's supervision. Although this approach may be legal for prescriptions for noncontrolled substances, it is not legal for controlled substance prescriptions. Agents of a practitioner may prepare the prescription at the practitioner's direction, as they can with paper prescriptions, but only the registered

practitioner may sign and issue the prescription. As noted above, the signature represents the practitioner's attestation of the validity of the prescription and legally binds the practitioner to the prescription.

Another scenario that the SCRIPT standard allows is for two DEA registration numbers associated with two practitioners to appear on a single prescription; the standard allows a practitioner and supervisor to be identified with DEA registration numbers. This scenario is not acceptable for controlled substance prescriptions. The prescribing registrant is solely responsible for issuing the prescription; approval by a supervisor does not alter the legal liability of the prescribing practitioner for the validity of the prescription. Identifying two registrants on a prescription could lead to confusion about which registrant was legally responsible and create confusion in pharmacy record systems.

To ensure that only authorized practitioners sign controlled substance prescriptions, the service provider must ensure that only DEA-registered practitioners are allowed to sign prescriptions for controlled substances and that each practitioner is uniquely identified. Specifically, the system must require that the DEA registrant whose DEA number is listed on the prescription sign the prescription. The system must not allow any other person to sign the prescription. Many office staff may have legitimate reasons to access the system, particularly when the electronic prescription capability is part of an EHR system. Some service providers now explicitly place limits on the level of access granted to various members of a practice. CCHIT Security Criteria require that EHR systems set access controls for specific tasks. DEA would require that all service providers do this if their systems will be used to issue controlled substance prescriptions. Nurses or other members of a practice staff may prepare the prescription, as they may with paper prescriptions, but the systems must allow only a practitioner authorized by the State and DEA to issue controlled substance prescriptions to sign and transmit the prescription.

This requirement is necessary to prevent others with access to the system from creating and signing prescriptions. In a recent discussion of an electronic prescription system, the service provider indicated that the illegality of a staff member issuing a prescription was a sufficient deterrent to prevent this from happening just, the service provider stated, as it prevents staff from stealing prescription pads.[21] Office staff have stolen prescription pads to create fraudulent paper prescriptions and called in fraudulent prescriptions. That they can do so with paper prescriptions is not a reason to facilitate their illegal activities with electronic prescriptions. DEA also notes that medical identity theft—where patient records are sold or misused—is a crime that often involves insiders. The *Report on the Use of Health IT to Enhance and Expand Health and Anti-Fraud Activities* cited a study that found that 70 percent of identity theft cases involved insider theft of data.[22]

This requirement will protect practitioners by eliminating the possibility that a staff member will be able to issue controlled substance prescriptions unless the practitioner grants them access to his authentication methods, which would make the practitioner legally responsible for any prescriptions that staff created. This requirement is also consistent with the HIPAA Security Guidance, issued on December 28, 2006, which recommended setting authorization levels particularly for portable devices and health record systems that can be remotely accessed.

DEA notes that role-based access control lists may need to be modified to comply with this requirement. Not every physician is a DEA registrant; not every DEA registrant is allowed to prescribe all Schedule II–V controlled substances. Authorizations for mid-level practitioners (e.g., nurse practitioners, physicians' assistants) vary across States. Service providers will need to ensure that their access control process reflects the actual authorizations of individuals and does not rely solely on roles.

To ensure that a prescription cannot be altered once it is ''signed,'' DEA is proposing that the prescription must be transmitted immediately on signing. Practitioners would be able to create a group of prescriptions and store them to be signed later. Agents of the practitioner (e.g., nurses) could also, at the practitioner's direction, enter some or all of the data into an electronic prescription as they can do for paper prescriptions. The practitioner, however, must authenticate to the system to sign the prescription because the practitioner is the ultimate authority for the prescription. If others prepare all or part of prescriptions, the practitioner could authenticate to the system and sign one or more prescriptions simultaneously depending on the system. If the system allows a practitioner to sign multiple prescriptions at once, DEA would require that the practitioner be required to indicate separately that he or she intends to sign each controlled substance prescription listed; this can be done by checking a box as some systems currently do. The critical requirement is that once the prescription is signed, it must be immediately transmitted so that there can be no question that someone else at the office had the opportunity to alter it. Many existing systems already have this feature. DEA notes that systems may apply varying labels to the signing function (e.g., sign, transmit); DEA does not think it is necessary to change these labels. The critical element is that the practitioners understand that when they use the function, they are exercising their authority to issue a controlled substance prescription and that they are responsible for accuracy, completeness, and validity of the prescription.

The other part of this requirement is that a controlled substance prescription must not be transmitted unless it has been ''signed.'' The system must be designed to prevent any transmission until the practitioner has ''signed'' the prescription. In addition, the system must not allow a prescription to be printed once it has been transmitted or to be transmitted if it was printed. These conditions are necessary to prevent a single prescription being used to generate multiple copies to be filled.

As noted above, the NCPDP SCRIPT standard does not currently include a field for a ''signature'' or for any indication that the prescription has been signed. DEA would require that controlled substance prescriptions include an indication that the prescription was signed; this indication could be a single character field. The industry has indicated that this alteration is feasible. It will provide pharmacies with additional assurance that the prescription was issued legally.

DEA welcomes comment on the current industry practices used to ''sign'' electronic prescriptions for noncontrolled substances and whether and how such practices prevent noncontrolled substance prescription forgery, fraud, and other related crimes.

Prescription data. Electronic prescriptions must contain the same information that DEA requires for paper prescriptions (21 CFR 1306.05): The date of issuance of the prescription;

[21] *http://www.nationalerx.com/pdf/NEPSI-eRx-faq.pdf.*

[22] The *Report on the Use of Health IT to Enhance and Expand Health Care Anti-Fraud Activities*, prepared for the Office of the National Coordinator, U.S. Department of Health and Human Services, September 30, 2005. *http://www.hhs.gov/healthit/hithca.html.*

practitioner's full name and address; practitioner's DEA registration number; patient's full name and address; drug name, strength, quantity, dosage form, and directions for use. DEA notes that for military or Public Health Service practitioners exempt from registration, the prescription must include the practitioner's service identification number or Social Security Number as required by 21 CFR 1306.05(h). This information may not be altered once the practitioner signs the prescription other than to reformat. The current version of NCPDP SCRIPT provides fields and codes for all of the required data elements, but not all of them are mandatory. For a controlled substance prescription, however, all of this information must be included. Other practitioner identifiers (State license number or National Provider Identifier) may not substitute for the DEA registration number. A system that completes practitioner and patient name and address only by linking to a National Provider Identifier (NPI) number and insurance records is not sufficient for DEA purposes for two reasons. First, practitioners will have a single NPI, but they may have multiple DEA registrations, particularly if they practice in more than one State. A prescription must have the correct DEA registration and location. Second, a system that assumes that details on the patient will be filled in by linking to insurance files will not account for the part of the population that does not have prescription drug insurance. As discussed above, multiple prescribers and their DEA registration numbers on a single prescription are also not acceptable. Electronic prescription systems would not be allowed to transmit a prescription for a controlled substance unless all of the required elements are complete.

DEA is also proposing to require that the system show the practitioner all of the DEA-required prescription information before the prescription is signed to ensure that a practitioner does not inadvertently misprescribe a controlled substance or sign a prescription created by an agent for his signature without having been presented with the contents. Although many systems do this, the RAND study indicated that some do not. In those cases, the practitioner sees only the drop down menus sequentially and may not have the opportunity to review the completed prescription. Where an agent enters the data for the prescription, it is particularly important that the practitioner be able to see the details to ensure that diversion is not occurring. DEA notes that the data may be presented in any format the system devises (e.g., arrayed like a paper prescription, a single line with the data selected shown); the essential items are the patient name and address, drug name, dosage form and units, quantity prescribed, directions for use, and the DEA registration number of the prescribing practitioner. DEA recognizes that systems may not routinely display the patient's address and seeks comments on whether displaying this information would pose technical problems.

DEA believes it is important to allow the signing and transmission of more than one prescription simultaneously. However, it is critical that the practitioner know, and positively indicate, which prescriptions are to be signed and transmitted. Where more than one prescription has been prepared at any one time, DEA is proposing to require that, prior to authenticating to the system, the practitioner indicate which prescription(s) are to be signed and transmitted. Such indication could be as simple as checking a box associated with each prescription the practitioner wishes to sign and transmit. DEA is not proposing any requirements to address a circumstance in which a prescription is not indicated for signature and transmission.

DEA would not allow alteration of any of the required information after the prescription is signed except to reformat. DEA does not believe that the intermediaries are altering the data because formulary checks appear to occur prior to signing. If, however, there are cases where the content of the required elements is altered (e.g., to change the prescribed drug to a generic drug) after signing, DEA would consider the prescription invalid and the parties that changed the data to have issued a prescription without being authorized to do so, a violation of the Controlled Substances Act.

Automatic timeout. For security reasons, many computer systems now lock the computer if it is not used for a period of time, often 5 or 10 minutes. The user must then reauthenticate himself to the system before being able to use the computer again. This feature ensures that there is a very limited possibility that someone else could use the computer or PDA after the practitioner authenticates to the system. This requirement is unlikely to be a problem for electronic prescription systems run by ASPs; if the feature does not exist in installed systems, it will require some reprogramming. DEA notes that automatic timeout after system inactivity is required under the CCHIT security criteria for EHRs, so should not impose a burden on those system providers. DEA is proposing that if the system is inactive for 2 minutes after the practitioner authenticates to the system to sign controlled substances prescriptions, the system must require the practitioner to reauthenticate himself to the system. DEA notes that it is not proposing that practitioners authenticate themselves to the system before creating the prescription, but only when the practitioner is ready to sign and transmit the prescriptions. Practitioners may create multiple prescriptions or have staff create the prescriptions for one or more patients, then authenticate to the system and sign the entire set at one time if the system allows this.

Digitally Signed Records. DEA is proposing that when an electronic prescription is signed and transmitted the first recipient would have to digitally sign and archive the digitally signed copy for five years from the date of issuance by the practitioner. Some electronic prescription systems already do this. In one case, the practitioner applies the service provider's digital signature when the practitioner signs the prescription; this is an acceptable practice under the proposed rule. Similarly, the first pharmacy system to receive the prescription (or the last intermediary transmitting it to the pharmacy) would have to digitally sign and archive a copy of the record as received. If the last intermediary digitally signs the record, it must forward both the record and the digitally signed copy to the pharmacy for dispensing. DEA notes that the service providers already have digital certificates.

As explained in detail below, digitally signing a record ensures that DEA and other law enforcement agencies can prove that the record is the prescription that the practitioner signed and the record that the pharmacy received. Industry representatives have stated that their internal audit trails provide similar evidence of record integrity; audit trails are computer functions that record each time a record is opened or altered. DEA has two concerns with relying on such audit trails for proof of record integrity. First, insiders will know how to turn off or erase audit trails. If they want to alter a prescription or insert fraudulent new prescriptions, they may be able to do so without leaving a trace. Second, DEA and other law enforcement agencies cannot be in the position of having to prove that such alterations did not occur each time they have to prove that a practitioner signed fraudulent prescriptions or a pharmacy altered a

record. The standard for criminal cases is ''beyond a reasonable doubt.'' If DEA relied on audit trails, it would have to subpoena both records and technical experts from each system and intermediary that handled each suspect prescription and hope that the possibility of insider action did not create a reasonable doubt. (As discussed in more detail below, insider threats to computer systems are relatively common.)

The burden of relying on intermediary and service provider audit trails would fall on the service providers and intermediaries as well. Even a simple case against a single practitioner could require substantial time for each service provider and intermediary as they would need to produce records and experts to explain the systems to grand juries, attorneys on both sides, and petit juries. Many diversion cases are not simple. For example, in February 2007, a county district attorney in New York filed charges against a Florida pharmacy and at least six practitioners in a case involving diversion of steroids (Schedule III). The investigation involved at least 20 branch offices of State, local, and Federal agencies in four States with connected investigations in two other States. If the prescriptions had been electronic, each service provider and intermediary could have been required to make records and experts available to each investigating agency. Neither the service providers, intermediaries, nor law enforcement would be well served by a system that demanded the industry prove the integrity of its systems every time a case is brought against a practitioner or pharmacy.

Digital Signatures. Digital signatures, as opposed to electronic signatures, are created as part of a public key infrastructure. A trusted party, a certification authority, conducts identity proofing and provides the subscriber with the means to generate an asymmetric pair of cryptographic keys. The subscriber retains control of the private key; the public key is available to anyone. What one of the keys encrypts only the other key can decrypt.

When a person digitally signs a record, the text of the record is run through an algorithm that produces a fixed-length digest (known as the hash). The private key is used to encrypt the digest. The encrypted digest is the digital signature. When the record is sent to someone else, both the plain text and the digital signature are sent along with the signer's digital certificate, which includes the public key. If the recipient wants to confirm that the record has not been altered during transmission, the recipient can use the public key to decrypt the digest. This step confirms who sent the message (i.e., no one other than the holder of the private key could have sent the message and the holder cannot repudiate the message). The recipient's system can run the plain text received through the same hashing algorithm. If the two digests match, the recipient knows that the message sent has not been altered.

The advantage of digital signatures is that they provide, in a single step, what other systems do not: a straightforward means of determining record integrity. If the first recipient of an electronic prescription signs it digitally, DEA will be able to prove what the practitioner signed. If the prescription is altered after that point, the practitioner will be able to demonstrate that he did not issue the altered prescription. Similarly, if the contents of the prescription sent and prescription received match, DEA and the intermediaries will be able to prove that the contents of the record were not altered in transit.

DEA is not proposing that practitioners digitally sign prescriptions or that pharmacies routinely validate prescriptions that are digitally signed because the existing system of intermediaries makes this requirement infeasible. As explained above, electronic prescriptions often need to be reformatted during transmission. This reformatting makes it impossible to validate the digitally signed record. That is, the digest generated for the prescription signed will not match the digest generated for the prescription received if even a single space is changed. DEA is, therefore, proposing only that the prescription as sent by the prescribing practitioner and as received by the dispensing pharmacy be digitally signed and archived. This approach will enable DEA and other law enforcement agencies to prove what the practitioner signed and what the pharmacy received. The approach also allows the service providers to apply their digital signatures, which most of them already have, rather than requiring the 1.2 million DEA-registered practitioners to obtain digital certificates. Digital signatures are an integral component of secure transmission systems in use by businesses that use the Internet.

The requirements for the digital signatures that the service providers or pharmacies apply are based on NIST FIPS standards for digital signatures and the hashing algorithm. Specifically, the signature would have to comply with FIPS 186–2, the digital signature standard. The algorithm used to process the record would have to comply with FIPS 180–2, the secure hash standard. Compliance with FIPS 186–2 requires compliance with FIPS 180–2. These standards are commonly used in the technology industry and, therefore, should not impose a burden on service providers; specifying the standards ensures the security of the digitally signed record.

Check on validity of the DEA registration. DEA is proposing that the validity of the DEA registration must be checked prior to dispensing a prescription. For paper prescriptions, this responsibility rests with the pharmacy. If a pharmacist has reason to doubt the validity of a prescription, he is required to, among other things, check the registration of the prescribing practitioner to determine whether, in fact, the practitioner is authorized to prescribe controlled substances in the schedule of the prescription. Chain pharmacies sometimes purchase the CSA registration database to conduct these checks. To parallel the paper system, DEA would require that prior to dispensing the pharmacy verifies that the practitioner is authorized by DEA to issue the prescription. DEA recognizes, however, that any of the service providers or intermediaries could offer this check as part of their service. Therefore, DEA is proposing simply that the registration be checked at some point prior to dispensing; if the check occurs before the prescription is delivered to the pharmacy, the record must indicate that the check has occurred and that the prescription is valid. If an electronic prescription service provider chooses to check the validity before transmitting the prescription and indicate that the check has occurred and the registration is valid, that would meet the requirement as would checks by any intermediary or pharmacy service provider. This requirement will give pharmacies greater assurance than they now have that the prescription is legitimate. DEA notes that regardless of which party checks the validity of the prescribing practitioner's DEA registration, the pharmacy is solely responsible and liable for the dispensing of the controlled substance. A pharmacy that relies on an intermediary or its own service provider to conduct the check must ensure that the reliance is warranted.

Pharmacy system record requirements. The pharmacy system must archive and retain the digitally signed prescription as received for five years from the date of receipt. The pharmacy system must require that each annotation include the information needed for paper prescription annotation (what was dispensed, by

whom, and when). The annotated record or linked records must be maintained for five years.

System security requirements. Beyond the requirements for handling controlled substance prescriptions at the point of origin, DEA is concerned about the security of the service providers' systems and whether that security protects against both insider and outsider threats. As noted above, insider threats may be a greater threat. Two FBI surveys on computer crime indicate that 42 to 44 percent of the companies surveyed reported insider misuse of their computer systems.[23] The 2006 survey also found that the most commonly used security technologies were directed toward outsiders. The Secret Service and Carnegie Mellon Institute have conducted studies of insider threats. They found that across all industries insiders who ''attacked'' company systems were likely to be disgruntled technology employees or former technology employees. In the financial sector, however, insiders did not hold technical positions. These insiders, who were usually acting for personal gain, attacked the system during work hours (70 percent) and in the work place (83 percent). In the financial sector, 78 percent of the cases involved modification or deletion of information.[24]

DEA is particularly concerned about insider threats. Although it is possible for hackers to break into computer systems, most service providers have invested in security technologies to protect against outsider attacks. It would also be possible for someone to create identity documents good enough to convince a service provider that the person was a DEA registrant, but this could be a costly exercise that could involve setting up a fictitious office. It is more likely that someone outside or inside a service provider organization will find an insider willing to create a fictitious subscriber, using a real practitioner's name and DEA registration number, who can then issue fraudulent prescriptions that the system, intermediaries and pharmacies will assume are genuine. Staff at intermediaries could also create and transmit fictitious prescriptions. The profits to be made from such action would be sufficient to bribe service provider insiders or to tempt them to take action on their own. In addition, with 10 percent of the adult population abusing prescription drugs at some time,[25] it is likely that some insiders or their family members or friends may be addicted to prescription drugs that they cannot obtain as easily elsewhere. DEA does not question the good intentions of service providers or intermediaries, but it would be naïve to think that they are immune from the threat of insider action when it is so widespread across all industries.

Pharmacy internal audits. For pharmacies, DEA is proposing that the pharmacy system include an internal audit trail; at the July 2006 public meeting regarding electronic prescriptions for controlled substances, the industry indicated that audit trails are a common feature of existing systems. The system operator would be required to define and implement a list of auditable events and conduct a daily analysis of the system to identify if any auditable events have occurred. The list of auditable events would have to include, at a minimum, attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in the controlled substances prescription system. The minimum list is based on the HIPAA definition of a security incident (45 CFR 164.304) and should, therefore, impose no new requirements on pharmacy systems, which are already subject to HIPAA. If the daily audit report identifies any events that indicate that the prescription system has been, or could have been, compromised, the pharmacy would be required to report this to DEA.

Pharmacy backup storage system. DEA is also proposing that the pharmacy system have a backup storage system for the prescription records required to be maintained by DEA. The backup system would have to be at another location so that it would not be subject to the same hazards (e.g., fires, power surges) as the main server. Such backup systems are common features provided by pharmacy system ASPs. DEA believes that pharmacies will generally need such systems for normal business reasons, particularly as their records become solely electronic. Backup systems will prevent the loss of records that DEA has seen when pharmacies have fires or power surges between the time DEA, or another law enforcement agency, serves a subpoena and the time the records must be delivered.

Third-party audits. DEA realizes that its registrants would not be able to determine, on their own, whether a particular service provider or system meets DEA's requirements. In addition, the security of the service provider's operations is critical to preventing insider threats and outsider attacks on the system. A registrant would have no way to determine whether a service provider had adequate protection against the range of potential security threats. It can be argued that service providers' primary goal is to sell their systems; the assertions that any service provider makes about its system cannot be accepted at face value. The accepted way for demonstrating that a system or a company is meeting a standard is to have a qualified third party audit the system or program and make a determination regarding the system's compliance. A qualified third party allows the party relying on the information the assurance that the determination is impartial and complete.

DEA considered developing a series of security requirements derived from NIST SP 800–53, which details security requirements for Federal information technology systems, and mandating that compliance with the requirements be verified through a third-party audit. DEA has concluded, however, that separate detailed standards were not warranted because an alternative approach would provide equivalent assurance of security practices at a lower cost. Detailed requirements based on NIST SP 800–53 could limit the flexibility of service providers to develop different procedures and practices that meet the need for security. Many service providers may already have adequate security practices and procedures in place, which might have to be altered to meet a NIST SP 800–53 requirement. DEA is aware that most private sector companies are unfamiliar with NIST SP 800–53. In addition, auditors would have to develop new protocols, a cost that would be passed on to the service providers. Because there are relatively few service providers, it is possible that there would not be an incentive for auditors to develop a common protocol that could be applied nationally. Another Federal agency that created third-party audit standards based on NIST SP 800–53 indicates that audits of compliance with a NIST SP 800–53-derived standard cost at least $250,000.

[23] 2005 FBI Computer Crime Survey and the 2006 CSI/FBI Computer Crime and Security Survey.

[24] Insider Threat Study: Illicit Cyber Activity in the Banking and Financial Sector, August 2004; Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, May 2005.

[25] Substance Abuse and Mental Health Services Administration. (2007). *Results from the 2006 National Survey on Drug Use and Health: National Findings detailed tables (Office of Applied Studies, NSDUH Series H–32, DHHS Publication No. SMA 07–4293. Rockville, MD. Table 1.18B—Nonmedical Use of Pain Relievers in Lifetime, Past Year, and Past Month by Detailed Age Category: Percentages, 2005 and 2006. http://www.oas.samhsa.gov/nsduh/2k6nsduh/2k6Results.cfm#TOC.*

DEA, therefore, is proposing that rather than attempting to dictate security requirements, the Administration would require electronic prescribing system service providers and pharmacies to obtain a third-party audit that addresses security and processing integrity. The third-party audit would also give practitioners and pharmacies a basis for determining if their systems meet DEA's standards. DEA seeks comments on this approach and whether this approach is preferable to a NIST SP 800–53-based audit approach.

Specifically, DEA is proposing that any system that will be used to create controlled substance prescriptions must have a third-party audit prior to accepting controlled substances prescriptions for processing and annually thereafter that meets the criteria for a SysTrust or WebTrust audit for security and processing integrity. For pharmacies, a SAS 70 audit would also be acceptable. As discussed below, SysTrust, WebTrust, and SAS 70 audits are professional services provided by qualified certified public accounting firms. For security, the audit determines whether the system is protected against unauthorized access (physical and logical); for processing integrity, the audit determines if the system processing is complete, accurate, timely, and authorized. SysTrust and WebTrust audits may also address issues of system availability, privacy, and confidentiality. Although practitioners and pharmacies may well be interested in these aspects of their systems, DEA does not believe that they are directly connected to the authentication and integrity of prescription records and, therefore, is not proposing to require audits that address these elements.

Third-party audits are frequently used by companies to prove compliance with standards and regulations. Organizations such as the International Standards Organization (ISO) routinely require third-party audits to demonstrate compliance and continuing compliance with its standards. Industry organizations, such as the American Chemistry Council, require third-party audits for their members to prove compliance with industry programs (e.g., Responsible Care in the chemical industry). The FDA recommends third-party audits for food processors and medical device manufacturers. The Federal Financial Institutions Examination Council (FFIEC), an interagency body that prescribes uniform principles, standards, and report forms for the Federal examination of financial institutions, allows third-party audits of technology service providers. Specifically, the Council cites American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) 70 and Trust Services audits as providing the examination and information needed by Federally regulated financial institutions. FFIEC states that:

> SAS 70 provides a uniform reporting format for third-party reviews of technology service providers (TSP) to facilitate the description and disclosure of the service provider's processes and controls to customers and their auditors. SAS 70 is a widely recognized standard and indicates that a service provider has had its control objectives and activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion (service auditor's report) is issued to the TSP at the conclusion of the SAS 70 process. The report contains a detailed description of the TSP's controls and an independent assessment of whether the controls are in place and suitably designed for the service provider's operations. The independent assessment of controls is based on testing certain controls to determine whether they are designed and operating with sufficient effectiveness to achieve the related control objective for the specified time period.[26]

SAS 70 audits are intended for the company's internal use. AICPA has developed two Trust Services audits to provide information to external users. FFIEC describes them as follows:

> SysTrust—In this type of review, a licensed CPA provides independent verification that a TSP has effective controls in place so that the system can function reliably. The institution prepares a description of the aspects of the system subject to be reviewed so that the scope of the review is clear to readers of the report. This system description is attached to the CPA's report. The auditor determines the presence of system controls and tests the effectiveness of the controls during the period covered by the SysTrust report. If the review is an attest-level engagement, the CPA firm's attestation is represented by the report to management and may also be represented by a SysTrust seal on the institution's Web site.
>
> WebTrust—The objective of a WebTrust engagement is for a licensed CPA to provide independent verification that an institution's Web site complies with the Trust Services Principles and Criteria in the particular subject matter reviewed (i.e., confidentiality, security, etc.). If the engagement is an attest-level review, assurance is represented by the CPA's report to management. An institution whose Web site has met the Trust Services Principles and Criteria in a particular subject matter area is eligible to display the WebTrust seal for that area to provide independent verification that an institution's Web site is in compliance. Clicking on the WebTrust seal reveals the date the seal was granted and the date it expires, the site's business practices and policies, Trust Services Principles and Criteria used to examine the site, the report of the independent accountant, as well as links to other sites with active WebTrust seals.[27]

Some electronic prescription systems already obtain these audits and display the seals on their Web sites.

Because the AICPA Trust audits are already in use and widely recognized, DEA is proposing to specify their use. DEA, however, seeks comments on whether other recognized audit protocols exist that provide similar services to those covered by the SysTrust/WebTrust/SAS 70 systems. DEA recognizes that audits can be expensive; SysTrust audits can cost from $15,000 to $250,000 depending on the size of the company and complexity of the information technology system. These recognized audits, however, provide assurance to the service providers' customers and investors that the systems will protect them and their information.

For prescribing systems, DEA is proposing that service providers must make the audit report available to any practitioner currently using the service provider's system and any practitioner considering use of the system. DEA believes that, at a minimum, the service provider must make the report available on its Web site, although a service provider may choose to make the report available through other means as well. If the third-party audit determines that the system does not meet one or more of DEA's regulatory requirements regarding the electronic prescribing of controlled substances, or does not provide adequate security against insider and outsider threats, the service provider must not accept for transmission any controlled substance prescription. The service provider would be required to notify practitioners that they should not use the system to generate and transmit controlled substance prescriptions. The service provider must also notify DEA of the adverse audit report and provide the report to DEA. For service providers that install the prescription-writing system on a practitioner's computers and that are not involved in the subsequent transmission of the prescription, the service provider must notify its DEA registrant customers of the results of any third-party audit that finds that the system does not meet one or more of DEA's regulatory requirements regarding the electronic prescribing of controlled substances. The service provider must also notify DEA of the

[26] *http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit_06_3_party.html.*

[27] *http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit_06_3_party.html.*

adverse audit report and provide the report to DEA.

The practitioner must determine initially and at least annually thereafter that the third-party audit report of the service provider indicates that the system and service provider meet DEA's regulatory requirements regarding the electronic prescribing of controlled substances. If the third-party audit report indicates that the system or the service provider does not meet the requirements of this part, or the service provider notifies the practitioner that the system does not meet the requirements of this part, DEA is proposing to require that the practitioner must immediately cease issuance of electronic controlled substance prescriptions using the system. As DEA has discussed throughout this rule, electronic prescribing of controlled substances is in addition to existing methods for prescribing of these substances. Therefore, DEA believes that this requirement will not impede the prescribing of controlled substances by practitioners.

For pharmacy systems, DEA is proposing that service providers must make the audit report available to any pharmacy currently using the service provider's system. DEA believes that, at a minimum, the service provider must make the report available on its Web site, although a service provider may choose to make the report available through other means as well. If the third-party audit determines that the system does not meet one or more of DEA's regulatory requirements regarding the dispensing of electronic controlled substances prescriptions, or does not provide adequate security against insider and outsider threats, the service provider must not accept or process any controlled substance prescription. The service provider would be required to notify pharmacies that they should not use the system to accept and process controlled substance prescriptions. The service provider must also notify DEA of the adverse audit report and provide the report to DEA. For service providers that install the prescription-processing system on a pharmacy's computers and that are not involved in the subsequent processing of the prescription, the service provider must notify its DEA registrant customers of the results of any third-party audit that finds that the system does not meet one or more of DEA's regulatory requirements regarding the electronic prescribing of controlled substances. The service provider must also notify DEA of the adverse audit report and provide the report to DEA.

Prescribing logs. DEA is proposing that electronic prescription service providers generate and send practitioners a log of all controlled substance prescriptions the practitioner has written in the previous month. The practitioner would be required to review the log and indicate to the service provider that the practitioner has reviewed it. A record of the indication that the review has occurred must be retained for five years. Further, DEA is proposing that the service provider must make available, at the practitioner's request, a record of all controlled substance prescriptions transmitted by the practitioner over the previous five years, the length of time for which the service provider is required to retain the digitally signed archive of the controlled substance prescriptions. DEA is not proposing that the pharmacy system generate dispensing logs, as they are required to do for refills under 21 CFR 1306.22. The internal audit trail and daily check for auditable events will serve to identify problem records without the need for a daily printout of the daily dispensing record. DEA recognizes that audit trails are not perfect and that insiders can subvert them. Diversion from pharmacies, however, usually involves pharmacy staff altering records to cover diversion or knowingly filling fraudulent prescriptions. Most pharmacists and other pharmacy staff are unlikely to be knowledgeable enough to be able to manipulate audit system controls. DEA seeks comments regarding these record requirements.

Discussion of Other Proposed Rule Requirements

A. Practitioner Requirements

DEA emphasizes that the use of electronic prescriptions is voluntary. No registrant would be required by DEA to issue controlled substance prescriptions electronically. Those registrants that wish to do so, however, would have to comply with the rules governing electronic prescribing of controlled substances.

DEA would require that practitioners who are registered in more than one State have a separate key to sign prescriptions for their registration in each State. Some practitioners hold multiple registrations within a single State because they administer or dispense controlled substances directly to patients at multiple locations. As a practical matter, however, they may issue prescriptions in the State under a single registration (see 71 FR 69478, December 1, 2006 for further discussion of this). Consequently, DEA is proposing that practitioners would need to have multiple access keys only when they practice in more than one State. The ''keys'' could be stored on the same hard token. The practitioner would be responsible for selecting the correct DEA registration to use to sign the prescription.

The practitioner must ensure that only the practitioner uses the hard token and must not share the password with any other person. The practitioner must adopt procedures and controls to (1) secure the hard token and password against loss, theft, or unauthorized use, and (2) clearly identify any attempt to compromise the private key. In practice, a practitioner can secure the hard token by retaining physical control of it. The practitioner must not lend the token, whether it is a PDA, cell phone, smart card, or other device, to anyone. If the practitioner has reason to believe that the password or other method used to authenticate to the token has been compromised, the practitioner must notify the service provider as soon as possible, but no later than 12 hours after discovery, and change the authentication. The practitioner must report to the service provider the loss or theft of the hard token within 12 hours of identifying the loss or theft even if the practitioner does not believe that someone else will be able to authenticate to the system. If the hard token is lost or the key can no longer be accessed for any reason, the service provider must revoke the authorization to sign controlled substances prescriptions. If a practitioner fails to notify the service provider of the loss or compromise within 12 hours or if the practitioner purposefully allows someone else to use the hard token to create and sign electronic prescriptions, DEA will hold the practitioner responsible for any controlled substance prescriptions issued under his name.

Regarding the third-party audits of electronic prescribing service providers' prescribing systems, the practitioner must determine initially and at least annually thereafter that the third-party audit report of the service provider indicates that the system and service provider meet the DEA requirements for electronic prescribing systems. If the third-party audit report indicates that the system or the service provider does not meet DEA's requirements, or the service provider notifies the practitioner that the system does not meet DEA's requirements, the practitioner must immediately cease to issue electronic controlled substance prescriptions using the system.

B. Prescription Logs and Security Incidents

The practitioner would be required to review the log of his controlled substance prescriptions transmitted by the service provider and indicate that he has reviewed the log; the indication can be as simple as checking a box. DEA emphasizes that it does not expect practitioners to crosscheck the log with medical records. DEA expects practitioners to review the list to determine if something seems unusual, such as prescriptions for a patient the practitioner has not seen, prescriptions for substances the practitioner does not usually prescribe, or more prescriptions for a particular controlled substance than a particular patient would normally require. If the practitioner finds problems, the practitioner would be required to notify DEA and the service provider within 12 hours.

Pharmacy systems would also be required to conduct a daily analysis of the pharmacy system audit trail to check for auditable events. If an auditable event occurs, the pharmacy must determine whether it represents a security incident that compromised, or could have compromised, the integrity of the prescription system and report any such incidents to the system provider and DEA within one business day. Both the practitioner log check and the pharmacy audit trail analysis will assist registrants, service providers, and DEA in identifying any diversion that has occurred.

Finally, DEA is proposing that service providers must audit their records and systems at least once a day. Service providers would be required to notify DEA of any security incidents that could compromise the security of controlled substance prescriptions. These incidents would include, but not be limited to, the discovery that prescriptions were being written by nonregistrants (identity theft), that access had been granted without proper identity proofing, that prescriptions were being or could have been altered after transmission, or that outsiders had penetrated the system.

C. Electronic Records and Record Retention

Record retention. The CSA (21 U.S.C. 827(b)(3)) requires that records of dispensing, i.e., prescriptions retained by pharmacies, shall be kept and made available ''for at least two years'' for inspection and copying by authorized personnel, including DEA. As DEA has noted previously, however, many States require that these records be maintained for longer periods of time. DEA reviewed existing State board of pharmacy requirements regarding record retention and found that 21 States require that records be retained for two years, nine for three years, one for four years, 17 for five years, one for six years, and one State required that records be retained for seven years.

As has been mentioned throughout this document, electronic prescribing poses new threats and vulnerabilities for diversion due to the increased velocity of these authenticated automated transactions. Unlike the paper system, where only one prescription is created and provided to a patient who brings that prescription directly to the dispensing pharmacy, electronic systems provide the opportunity to create and transmit many prescriptions simultaneously. These many prescriptions can be simultaneously transmitted to pharmacies over a broad geographic area, without the need to physically move a paper prescription from one location to another. Further, as DEA has discussed, the introduction of service providers and other intermediaries into the system poses new vulnerabilities for insider attacks on the electronic prescribing systems.

DEA is concerned that a significant amount of time may elapse between the time a controlled substance is diverted and the time DEA becomes aware of the potential or suspected diversion. DEA is also concerned that administrative, civil, and criminal cases will become more complex and time-consuming as more parties become involved in the movement of the prescription from the practitioner to the pharmacy.

The statute of limitations for non-capital offenses is five years. That is, the United States cannot prosecute, try, or otherwise punish anyone for any non-capital offense unless the person is indicted, or an information instituted, within five years after the offense was committed (18 U.S.C. 3282). Due to the potential length and complexity of cases relating to the diversion of electronic prescriptions for controlled substances, DEA believes that a longer retention period is necessary and permissible within its statutory authority.

Therefore, to address these concerns, DEA is proposing to require that all records regarding electronic prescribing of controlled substances be maintained for five years from the date the record was created. This record retention requirement shall not pre-empt any longer period of retention which may be required now or in the future, by any other federal or State law or regulation, applicable to practitioners, pharmacists, or pharmacies. Records affected by this requirement would include, but are not necessarily limited to:

- The document received by the service provider from an entity permitted to conduct in-person identity proofing regarding the conduct of that in-person identity proofing for the specific practitioner.
- The electronic controlled substance prescription as digitally signed by the service provider or first processor.
- The electronic controlled substance prescription as digitally signed by the pharmacy or last intermediary.
- The dispensing annotations added to or linked to the prescription record.
- The backup copy of the pharmacy controlled substances prescription records.
- The internal audit trail records created by the pharmacy system.
- The monthly log of controlled substances prescriptions provided to each practitioner by the practitioner's service provider and the record of the indication by the practitioner that the log has been reviewed.
- The third-party SysTrust, WebTrust, or SAS 70 report of the electronic prescribing or pharmacy system.

DEA believes that these record retention requirements will not pose any new burdens on service providers and pharmacies. Many service providers indicate that they retain these records for longer periods of time, to comply with State laws and other Federal agency requirements. Further, as all of the records in question can be retained electronically, there will be limited costs associated with the storage of these records. DEA seeks comment regarding the extent to which service providers and intermediaries store electronic records of noncontrolled substance prescriptions.

Electronic Records. DEA is proposing that pharmacies must maintain records of electronic prescriptions and any linked records for five years. Records must be maintained electronically. Records regarding controlled substances that are maintained electronically must be immediately retrievable from all other records by prescriber's name, patient's name, drug dispensed, and date filled. They must be easily readable or easily rendered in a human readable format. The databases in which prescription records are maintained must be capable of exporting the records into database or spreadsheet format that will allow the data to be sorted by prescriber name, patient name, drug dispensed, and date filled. Such records must be made available to the Administration upon request. Records must also be capable of being immediately printed upon request.

D. Preventing This Rule From Being Exploited by Rogue Internet Operators

In recent years, there has been a significant rise in the amount of prescription controlled substances sold without a legitimate medical purpose by Internet-based entities such as so-called ''rogue Internet pharmacies.'' The typical ''rogue Internet pharmacy'' is actually a criminal conspiracy run by a Web ''entrepreneur'' who contracts with one or more unscrupulous DEA-registered practitioners to write prescriptions and one or more unscrupulous DEA-registered pharmacies to fill the prescriptions. Drug seekers easily find their way onto these Web sites through an Internet search engine (such as by typing the search terms ''hydrocodone no prescription'') or through spam e-mail advertisements. Once on such sites, the drug seeker is immediately shown a price list of controlled substances (with such prices usually inflated well above those of a legitimate pharmacy). After the drug seeker chooses the drug(s) he wants, the Web site assists the buyer in obtaining a prescription from an unscrupulous practitioner employed by the site, who has no bona fide doctor-patient relationship with the buyer. Generally, all that is needed for the buyer to obtain a prescription is to supply a credit card number, fill out a questionnaire and, in some cases, fax in some form of ''documentation'' that purports to show a medical condition.

The prescribing practitioner employed by the typical rogue Web site never sees the drug buyer in person, conducts no meaningful review of the documentation supplied by the buyer, and makes no attempt to rule out the possibility that the ''medical records'' supplied by the buyer are fraudulent. Instead, the practitioner employed by these sites generally writes as many prescriptions as possible, often from a location far from the patient. For example, DEA has found evidence that many practitioners located in the Caribbean have been employed by rogue Web sites to write prescriptions for ''patients'' located throughout the continental United States. Once the prescription has been generated, the same Web operation typically arranges for the prescription to be transmitted to the unscrupulous brick-and-mortar pharmacy, which fills it unquestioningly, turning a blind eye to the circumstances under which it was issued.

Using the foregoing methods, DEA estimates that the total amount of controlled substances illegally distributed via the Internet is well in excess of 100 million dosage units per year. DEA has taken numerous enforcement actions recently to shut down pharmacies, practitioners, and distributors found to have misused their DEA registrations to facilitate this Internet-based diversion. Yet, even with focused enforcement efforts, there will remain some unscrupulous individuals who will continue to seek to exploit the anonymity of the Internet to profit from the illegal sales of controlled substances. Moreover, given that a single rogue Web site can divert enormous amounts of controlled substances throughout the United States in a relatively short period of time, allowing such sites to operate even for brief periods can cause substantial harm to the public health and safety. It is, therefore, essential that DEA avoid any regulatory action that could be exploited by such rogue actors.

Based on the historical practices of these rogue Web sites and the claimed legal defenses they have put forth (asserting, for example, that their ''business model'' is having practitioners prescribe controlled substances without ever seeing the ''patient'' and without establishing a legitimate doctor-patient relationship), DEA is particularly concerned that the operators of these rogue sites might attempt to use this proposed rule as a justification for their illicit activities or to expand upon such activities. Absent a clear statement to the contrary in the regulations, operators of rogue sites might argue that, if their site generates prescriptions for controlled substances that are transmitted using electronic prescriptions in a manner that complies with authentication requirements of this proposed rule, they are automatically engaging in legal activity. Of course, all prescriptions for controlled substances must be issued for a legitimate medical purpose in the usual course of professional practice. Mere compliance with the authentication requirements of this proposed rule with respect to a given prescriptions does not—by itself—establish that the prescription was issued for a legitimate medical purpose. To avoid any possible confusion about this point, the proposed rule contains a provision that reaffirms this basic principle.

In addition, to minimize the likelihood that operators of rogue Internet sites would attempt to exploit this proposed rule, DEA wishes to reiterate some additional basic principles that the agency has stated in prior **Federal Register** documents. First, it is axiomatic that, in the absence of a bona fide doctor-patient relationship, a practitioner cannot satisfy the requirement of issuing a prescription for a legitimate medical purpose in the usual course of professional practice.[28] An arrangement whereby a Web site solicits drug seekers and refers them to practitioners who issue prescriptions for controlled substances without ever having seen the patient in person, based solely on such unreliable information as an online questionnaire, telephone conversation, or faxed documents that purport to be a drug buyer's medical records, inherently fails to satisfy the requirement of issuing a prescription for a legitimate medical purpose in the usual course of professional practice.[29] This is true regardless of whether the rogue Web site that operates in such a fashion utilizes paper, oral, faxed, or electronic prescriptions. Thus, it bears repeated emphasis that the use of electronic prescriptions in accordance with this proposed rule will in no way relieve the practitioner of the longstanding obligation to issue a prescription for a controlled substance only for a legitimate medical purpose in the usual course of professional practice. Likewise, as has always been the case, a corresponding responsibility will continue to rest with the pharmacist who fills the electronic prescription to ensure not only that the prescription was issued in accordance with the provisions for electronic prescribing contained in this proposed rule, but further that the prescription was issued for a legitimate medical purpose in the usual course of professional practice.

E. Other Prescription Issues

Transfers

A pharmacy would be allowed to transfer an original unfilled electronic prescription to another pharmacy if that pharmacy is unable to or chooses not to fill the prescription.

A pharmacy would also be allowed to transfer an electronic prescription with remaining refills to another pharmacy for filling provided the transfer is communicated between two licensed pharmacists. The pharmacy transferring the prescription would have to void the remaining refills in its records and note in its records to which pharmacy the prescription was transferred. The notations may occur electronically. The pharmacy receiving the transferred

[28] *See United Prescription Services, Inc.* (72 FR 50397, August 31, 2007); *Southwood Pharmaceuticals, Inc.* (72 FR 36487, July 3, 2007); *Trinity Health Care Corp., D/B/A/ Oviedo Discount Pharmacy* (72 FR 30849, June 4, 2007); *William Lockridge, M.D.*, (71 FR 77791, December 27, 2006); *Dispensing and Purchasing Controlled Substances over the Internet*, (66 FR 21181, April 27, 2001).

[29] *Id.*

prescription would have to note from whom the prescription was received and the number of remaining refills.

Applicability of Current Rules

The CSA provides that a pharmacist may only dispense a controlled substance in Schedule II pursuant to a written prescription, except in emergency circumstances, where a pharmacy may dispense pursuant to an oral prescription (21 U.S.C. 829(a)). The CSA further provides that a pharmacist may dispense a Schedule III and IV prescription pursuant to either a written or an oral prescription (21 U.S.C. 829(b)). The CSA was enacted in 1970, long before the advent of electronic prescriptions, and thus the Act makes no mention of electronic prescriptions. As a result, electronically created and transmitted prescriptions are subject to the same provisions of the CSA and DEA regulations that apply to paper prescriptions. The DEA regulations provide, as set forth in 21 CFR 1306.11 and 1306.21, that a pharmacist may dispense a controlled substance under a written prescription signed by the practitioner. This requirement applies equally to manually written and electronically written prescriptions. In either case, the prescription can be prepared by an agent of the practitioner, such as a nurse or office assistant, but only the practitioner can apply his signature to that prescription. Of course, for Schedule III through V controlled substances, the prescription could still be transmitted orally or by facsimile (including a manual signature by the practitioner) to the pharmacy at the practitioner's discretion.

IX. Summary of Proposed Rule Requirements

As has been discussed throughout this rulemaking, DEA is proposing electronic prescribing of controlled substances as an addition to, not a replacement of, existing prescribing and dispensing methods already permitted by the CSA and DEA regulations. DEA has discussed its law enforcement concerns as they relate to electronic prescribing and dispensing of controlled substances. Any requirements DEA implements for electronic prescribing and dispensing of controlled substances must ensure that DEA and other law enforcement needs under the Controlled Substances Act and implementing regulations can be met. DEA is convinced that its concerns can be addressed without creating insurmountable barriers to electronic prescribing. In addition, DEA wishes to adopt an approach that is flexible enough that future changes in technologies will not make the system obsolete or lock registrants into more expensive systems. As has been discussed throughout this rulemaking, many of the requirements DEA is proposing are already required by other Federal agencies or third-party organizations, and are in practice in electronic prescribing and electronic pharmacy systems today. The table below summarizes the requirements DEA is proposing by this rule, the rationale for each, and the current implementation status of each requirement.

TABLE 6.—SUMMARY OF PROPOSED REQUIREMENTS FOR ELECTRONIC PRESCRIPTIONS FOR CONTROLLED SUBSTANCES

Requirement	Rationale	Current practice
In-person identity proofing § 1311.105	Ensures only DEA registrants are granted access and protects against identity theft.	Prescribing practitioners have ready access to hospitals, State licensing boards, and State/local law enforcement agencies, any of which may conduct in-person identity proofing.
Check validity of State license and DEA registration § 1311.105.	Ensures that only eligible practitioners are granted access.	At least some service providers already do this.
Maintain record of identity proofing § 1311.105	Provides a record that protects both the practitioner and service provider.	
Two-factor Level 4 authentication § 1311.110	Provides a direct link between the prescriber and prescription; prevents misuse of passwords without the practitioner's knowledge. Protects the practitioner from staff issuing prescriptions in the practitioner's name.	EHRs certified by CCHIT must support 2-factor authentication so majority of existing systems have this capability. HIPAA security guidance recommends 2-factor authentication.
Limit access to signing function § 1311.125	Ensures that only authorized registrants may sign controlled substance prescriptions.	EHRs certified by CCHIT must do this so majority of existing systems have this capability.
Automatic lockout after a period of inactivity § 1311.110.	Ensures that system cannot be accessed by other people once the practitioner has authenticated to the system.	EHRs certified by CCHIT must do this so majority of existing systems have this capability.
Prescription must contain all DEA data elements § 1311.115.	Meets the legal requirements for a controlled substance prescription.	All systems should already have this capability.
Present the required data elements to the practitioner § 1311.120.	Ensures that the practitioner has the opportunity to identify any miskeying.	Most systems present the full prescription information on a single screen.
Indicate that each prescription is ready to be signed § 1311.120.	Ensures that the practitioner has positively indicated that the prescription is to be transmitted when multiple prescriptions are being signed at one time.	Some existing systems already do this, requiring practitioners to check off each prescription they want to sign.
Authenticate to the system just before signing § 1311.125.	Ensures that only the practitioner signs the prescription.	Unclear when current systems require authentication. At least one requires entry of separate password to sign.
Transmit as soon as signed § 1311.130	Prevents any alteration after the practitioner has signed.	May be common practice in existing systems because signing is the equivalent of transmitting.
Do not transmit if printed; do not print if transmitted § 1311.130.	Prevents other staff from printing extra copies that can be used to divert.	May be a new function for most systems. (This requirement does not prevent printing a copy of a medical record.)
Indicate that the prescription was signed § 1311.125.	Provides assurance to pharmacy that the practitioner authorized the prescription.	A new field for electronic prescriptions; industry has indicated that this is not a problem.

TABLE 6.—SUMMARY OF PROPOSED REQUIREMENTS FOR ELECTRONIC PRESCRIPTIONS FOR CONTROLLED SUBSTANCES—Continued

Requirement	Rationale	Current practice
Generate monthly logs for practitioner review § 1311.140.	Provides practitioner a chance to review record and identify problems.	All systems should be able to generate records.
First recipient digitally signs the prescription as transmitted § 1311.130.	Provides record integrity. Ensures that DEA and the practitioner can prove what the practitioner signed.	At least one service provider is already doing so. Service providers all have digital certificates and the capability to sign records digitally.
Do not convert to fax if cannot be delivered § 1311.130.	Faxed prescriptions must be manually signed. Converting an electronic file to a fax during transmission creates an invalid written prescription.	May alter existing practice for some intermediaries. HHS has proposed removing an exemption from the SCRIPT standard for faxes.
No alteration of the content during transmission except for formatting § 1311.130.	Protects against changes during transmission	Industry says this does not happen so requirement should not impose a burden.
First pharmacy (or last transmitter) digitally signs the prescription as received § 1311.160.	Provides record integrity. Ensures that DEA and the pharmacy can prove what the pharmacy received. Eliminates the need to examine the intermediaries' records in most cases and provides a basis for identifying alteration at the pharmacy.	Intermediaries and at least some pharmacy system providers have digital certificates and the capability to sign records.
Check the validity of the prescriber's DEA registration (Pharmacy) § 1311.165.	Ensures that the practitioner is still authorized to issue prescriptions.	Many pharmacies already check the DEA database for registration information.
Store all of the DEA data in the pharmacy system § 1311.165.	Parallels paper records	Pharmacy systems already do this. Some may have problems with extensions to DEA numbers.
Have an internal audit trail and analyze for auditable events (Pharmacy) § 1311.170.	Provides a record of who annotated or altered a prescription. Needed to identify diversion at the pharmacy.	Most systems have this capability.
Electronic prescription records stored electronically. (pharmacy) § 1311.180.	All information is created and received electronically.	Pharmacy systems already maintain electronic information for paper prescriptions.
Have a backup system for records at another location. (Pharmacy) § 1311.170.	Protects against loss of records (accidental or intentional).	Many pharmacy system providers, particularly ASPs, have such backup systems.
SysTrust, WebTrust, or SAS 70 audit § 1311.150, § 1311.170.	Provides assurance of the physical and processing integrity of the system. Protects against insider and outsider attacks on the system.	At least one service provider already has adopted this audit.
Report security incidents § 1311.145, § 1311.155, § 1311.170.	Provides system provider and DEA with immediate notice of potential problems.	Imposes no system requirements.

X. Section-By-Section Discussion of the Proposed Rule

In Part 1300, DEA is proposing to add a new § 1300.03, definitions relating to electronic orders for controlled substances and electronic prescriptions for controlled substances. The definitions currently in § 1311.02 would be moved to § 1300.03. Definitions of the following would be added: Audit, audit trail, authentication, authentication protocol, electronic prescription, hard token, identity proofing, intermediary, paper prescription, PDA, service provider, token, and valid prescription. In addition, a definition of NIST special publication 800–63 and SAS 70, SysTrust, and WebTrust would be added. Where possible, DEA is proposing to use definitions taken from NIST publications (audit, audit trail, authentication, authentication protocol, hard token, identity proofing, service provider, and token). DEA is using standard definitions developed for information technology systems to reduce the possibility that service providers will be confused by definitions as they might be if DEA translated the definitions into ''plain'' language.

DEA is also proposing to add a definition of ''intermediary'' to cover any system that receives and transmits an electronic prescription after it is signed and before it is received by a pharmacy system. An intermediary could be the original service provider if it is the first recipient of the prescription, SureScripts or any other system that processes and reformats prescriptions, and a pharmacy system provider if it processes a prescription before routing it to the pharmacy.

Further, definitions of electronic and paper prescription would be added. The definition of electronic prescription would state that an electronic prescription must meet the requirements of parts 1306 and 1311. The definition also clarifies that a computer-generated prescription that is printed out or faxed is not an electronic prescription for DEA purposes. The definition of paper prescription clarifies that such prescriptions can be created on paper or computer-generated to be printed or faxed; all paper prescriptions must be manually signed. Finally, the definition of valid prescription from § 1300.02 would be repeated in the new section.

In Part 1304, § 1304.04 would be revised to limit records that cannot be maintained at a central location to paper order forms for Schedule I and II controlled substances and paper prescriptions. In paragraph (b)(1), DEA would remove the reference to prescriptions; all prescription requirements would be moved to paragraph (h). Paragraph (h), which details pharmacy recordkeeping, would be revised to limit the current requirements to paper prescriptions and to state that electronic prescriptions must be retrievable by prescriber's name, patient name, drug dispensed, and date filled. The electronic records must be in a format that will allow DEA or other law enforcement agencies to read the records and manipulate them; preferably the data would be downloadable to a spreadsheet or

database format that allows DEA to sort the data. The data extracted should only include the items DEA requires on a prescription. Records would also be required to be capable of being printed upon request.

In Part 1306, prescriptions, § 1306.05 would be amended to state that electronic prescriptions must be created and signed using a system that meets the requirements of part 1311 and to limit some requirements to paper prescriptions (e.g., the requirement that certain paper prescriptions have the practitioner's name stamped or hand-printed on the prescriptions). The section would also add ''computer printer'' to the list of methods for creating a paper prescription and clarify that a computer-generated prescription that is printed out or faxed must be manually signed. DEA is aware that in some cases, an intermediary transferring an electronic prescription to a pharmacy may convert a prescription to a facsimile if the intermediary cannot complete the transmission electronically. For controlled substance prescriptions, this is not an acceptable solution. The intermediary must notify the practitioner that the transmission could not be completed and have the practitioner create and sign a written prescription (for Schedule III, IV, or V controlled substances) before faxing it to the pharmacy. For most Schedule II prescriptions, the practitioner would have to provide a written prescription to the patient if notified that the transmission failed. The section would also be revised to divide paragraph (a) into shorter units.

Section 1306.08 would be added to state that practitioners may sign and transmit controlled substance prescriptions electronically if the systems used are in compliance with part 1311 and all other requirements of part 1306 are met. Pharmacies would be allowed to handle electronic prescriptions if the pharmacy system complies with part 1311 and the pharmacy meets all other applicable requirements of parts 1306 and 1311.

Sections 1306.11, 1306.13, and 1306.15 would be revised to clarify how the requirements for Schedule II prescriptions apply to electronic prescriptions.

Section 1306.21 would be revised to clarify how the requirements for Schedule III–V prescriptions apply to electronic prescriptions.

Section 1306.22 would be revised to clarify how the requirements for Schedule III–IV refills apply to electronic prescriptions and to clarify that requirements for electronic refill records for paper, fax, or oral prescriptions do not apply to electronic refill records for electronic prescriptions. Pharmacy systems used to process and retain electronic controlled substance prescriptions would have to comply with the requirements in part 1311. In addition, DEA is proposing to break up the text of the existing section into shorter paragraphs to make it easier to read.

Section 1306.25 would be revised to include separate requirements for transfers of electronic prescriptions. These revisions are needed because an electronic prescription could be transferred without a telephone call between pharmacists. Consequently, the transferring pharmacist must provide, with the electronic transfer, the information that the recipient transcribes when accepting an oral transfer.

Section 1306.28 would be added to state the basic recordkeeping requirements for pharmacies for all controlled substance prescriptions. These requirements are now in § 1304.22 and remain there as well. DEA is proposing to add them to part 1306 to place all of the requirements in a single part on prescriptions.

Part 1311 would be amended to add requirements related to electronic prescriptions for controlled substances.

Section 1311.02 providing definitions related to electronic orders for controlled substances would be revised to remove the definitions and replace them with a cross reference to new § 1300.03.

Section 1311.08 would be amended to add an incorporation by reference for NIST Special Publication 800–63.

A new subpart C would be added for the rules that govern the systems that may be used to issue and process electronic controlled substance prescriptions and the responsibilities of practitioners and pharmacies.

In § 1311.100, DEA would state that only DEA registrants or persons exempted from registration under part 1301 would be allowed to issue electronic prescriptions for controlled substances and only if they use a system and service provider that meet the requirements of part 1311. An electronic prescription for controlled substances issued through a system and service provider that did not meet the requirements of part 1311 would not be considered valid. The section would reiterate the requirement from § 1306.05 that the practitioner is responsible if the prescription does not conform in all essential respects to the CSA and implementing regulations.

Sections 1311.105 through 1311.150 would establish minimum requirements that a service provider and system must meet before a practitioner would be able to use the system to create and sign an electronic controlled substance prescription. Although the service providers and their systems must meet the requirements, the ultimate responsibility rests on the practitioner to use only a system and service provider that comply with DEA's requirements.

Section 1311.105 would require that the service provider receive a document regarding in-person identity proofing of the prescribing practitioner by an entity authorized by DEA to conduct the identity proofing. The service provider must check the DEA registration and State licensure to ensure they are current and in good standing, and maintain records of the identity proofing.

Section 1311.110 would require the system to use two-factor authentication that meets the requirements of NIST SP 800–63, level 4 as discussed above. The practitioner must reauthenticate to the system if the system is inactive for more than 2 minutes. The system must provide separate authentication protocols for separate DEA registrations that a practitioner uses to issue controlled substances prescriptions. Finally, the authentication protocol must expire no later than the expiration date of the DEA registration with which it is associated. A DEA registration is valid for three years and can be renewed prior to its expiration.

Section 1311.115 would require that electronic prescriptions for controlled substances contain all of the information required under paragraph (b) of that section and § 1306.05. It would also require that a controlled substance prescription include only the DEA number and practitioner information for the prescribing practitioner. As discussed above, the SCRIPT standard allows multiple DEA numbers to be associated with a prescription; this is not acceptable to DEA.

Section 1311.120 would set the requirements for creating an electronic prescription as discussed above. Consistent with current regulations governing paper prescriptions, DEA is proposing that the electronic prescribing system may allow the registrant or his agent to enter data for a controlled substance prescription, but only the registrant may sign and authorize the prescription. This would include the requirement that, where more than one controlled substance prescription has been prepared, the practitioner positively indicate that he has reviewed and approved the information for each

prescription prior to signing and authorizing electronic transmission of the prescriptions.

Section 1311.125 would set the requirements for signing an electronic prescription as discussed above. This would include the practitioner's declaration that information contained in the record constitutes the practitioner's legal authorization and signature.

Section 1311.130 would require that the system transmit the prescription immediately upon signing. The section would disallow the printing of an electronically transmitted prescription and would also disallow the electronic transmission of a printed prescription as discussed above. These requirements are to prevent an individual electronic prescription from being transmitted more than once to a pharmacy (or pharmacies). The service provider or first recipient would be required to digitally sign and archive a copy of the prescription as received. Finally, the section would specify that the DEA required contents of the prescription could not be altered after signature without rendering the prescription invalid. The contents could be reformatted; reformatting includes altering the structure of fields or machine language so that the receiving pharmacy system can read the prescription and import the data into the system.

Section 1311.135 would set the requirements revoking the authentication protocol used to sign controlled substances prescriptions upon notification that the password or token has been compromised, lost, or stolen or when the DEA registration expires unless the registration has been renewed and at any time that the registration is suspended or revoked.

Section 1311.140 would require the service provider to generate and transmit to the practitioner a log of all controlled substance prescriptions written under the practitioner's DEA number in the previous month. The section would also require that the service provider make available, at the practitioner's request, a record of all controlled substance prescriptions transmitted over the previous five years.

Section 1311.145 would require the service provider to notify DEA of certain security incidents, as discussed above.

Section 1311.150 would require each service provider to have at least an annual third-party SysTrust or WebTrust audit for security and processing integrity as well as compliance with part 1311. Audits must be conducted prior to accepting any controlled substances prescriptions for transmission and annually thereafter. The audit report must be made available to any practitioner using or considering use of the system. If the audit finds that the system does not meet the requirements of the part, the service provider must not transmit controlled substance prescriptions and must notify practitioners that they should not attempt to send electronic controlled substance prescriptions until the problems have been addressed and another audit indicates that the system meets the requirements of part 1311.

Section 1311.155 would specify the practitioner's responsibilities as discussed above. The section would require practitioners to check the third-party audit reports and notifications from the service providers about system inadequacies and cease to use the system for controlled substance prescriptions if the audit report or service provider indicated problems. The practitioner would be required to provide, or cause to be provided, documents regarding in-person identity proofing to the service provider. The practitioner would be required to maintain sole possession of the hard token and notify the service provider no later than 12 hours after the discovery of its loss or theft or any indication that the hard token had been compromised. The practitioner would be required to check the monthly log and indicate having done so. The section would reiterate that the practitioner has the same responsibility for the validity of an electronic prescription as the practitioner does for a paper prescription.

Section 1311.160 would require the pharmacy or the last system transmitting the prescription to the pharmacy to digitally sign and archive the prescription record.

Section 1311.165 would require the pharmacy to check the validity of the DEA registration prior to dispensing the prescription. The pharmacy system must reject a controlled substance prescription if it is not signed or is otherwise not valid. The pharmacy system would have to be able to include all of the information required under part 1306 in the electronic record and be capable of downloading the records in a readable and sortable format, as well as printing the records, if requested.

Section 1311.170 would specify the security requirements for the pharmacy system including a backup storage system at another location, maintaining an internal audit trail, the implementation of a list of auditable events, a daily internal audit to identify if any auditable events have occurred, reporting any security incidents that could affect the integrity of the prescription records, and the annual SAS 70 or SysTrust audit. Audits must be conducted prior to accepting any controlled substances prescriptions for processing and annually thereafter. The audit report must be made available to any pharmacy using or considering use of the system. If the audit finds that the system does not meet the requirements of the part, the service provider must not process controlled substance prescriptions and must notify pharmacies that they should not attempt to process electronic controlled substance prescriptions until the problems have been addressed and another audit indicates that the system meets the requirements of part 1311.

Section 1311.175 would specify the pharmacy's responsibility not to dispense controlled substances in response to an electronic prescription if the pharmacy's system does not meet the requirements of part 1311. In addition, the pharmacy must not dispense a controlled substance if the DEA registration of the prescriber was not valid at the time of signing. Finally, the section would state that nothing in part 1311 relieves a pharmacy of its corresponding responsibility to dispense only in response to a prescription written for a legitimate medical purpose by a prescribing practitioner acting in the usual course of professional practice.

Section 1311.180 would specify recordkeeping requirements for records required by part 1311.

XI. Digitally Signed Prescriptions for Federal Health Care Agencies

Federal healthcare providers have indicated that the electronic prescription option described above is not consistent with the electronic prescription system they currently use, a system that is based on public key infrastructure and digital signature technology. They also stated that the proposed rule described above did not meet their security needs. Thus, these Federal health care providers indicated that their existing system based on public key infrastructure and digital signature technology is more secure than, and incompatible with, the above system requirements that DEA is proposing. As a result, if they were obligated to adhere to the above system requirements, they would have to abandon their existing systems in favor of a less secure system, and would have to incur substantial cost and devote significant time to do so. Such a result would plainly be counterproductive. For these reasons, DEA is proposing—for Federal health care systems only—a

second approach that is consistent with their current systems. Federal health care systems will also have the option of using the above system that will be allowable for all practitioners in the private sector. The two systems have some elements in common—for example, the pharmacy requirements are almost identical—but the digital signature option adds some steps and removes others as compared with the electronic prescription system.

Public Key Infrastructure and Digital Signatures. Digital signatures are created as part of a public key infrastructure (PKI). In a PKI system, a certification authority (CA) verifies the identity of an applicant and issues a digital certificate to the applicant. A Certification Authority operates under a publicly available Certificate Policy, a set of rules that covers subjects such as obligations of the Certification Authority, obligations of certificate holders, enrollment and renewal procedures, operational requirements, security procedures, and administration.[30] A digital certificate is a data record that contains, at a minimum, the identity of the issuing Certification Authority, identity information for the certificate holder, the public key that corresponds to the certificate holder's private key, validity dates, and a serial number. The certificate is digitally signed by the CA. The certification authority provides the subscriber with the means to generate an asymmetric pair of cryptographic keys. The subscriber retains control of the private key; the public key is available to anyone. What one of the keys encrypts, only the other key can decrypt.

When a person digitally signs a record, the text of the record is run through an algorithm that produces a fixed-length digest (known as the hash). The private key is used to encrypt the digest. The encrypted digest is the digital signature. When the record is archived or sent to someone else, both the plain text and the digital signature are sent along with the signer's digital certificate, which includes the public key. If the recipient wants to confirm that the record has not been altered during transmission, the recipient can use the public key to decrypt the digest. This step confirms who sent the message (i.e., no one other than the holder of the private key could have sent the message and the holder cannot repudiate the message). The recipient's system can run the plain text received through the same hashing algorithm. If the two digests match, the recipient knows that the message sent has not been altered. For an in-depth explanation of digital signatures, see NIST FIPS 186–2.

Discussion of Proposed Requirements for Digitally Signed Prescriptions

Certification Authorities and Digital Certificates. Because this alternative applies only to Federal agencies, DEA is proposing that the Certification Authority will be one that is operated under the Federal PKI Bridge Certificate Policy and is either a Federal Certification Authority or cross-certified with a Federal CA. Digital certificates are already an option for Federal employees as part of the Personal Identification Verification (PIV) cards (usually a smart card). DEA, therefore, is proposing that a PIV or other Federal identity card to be used for signing controlled substance prescriptions include a digital certificate. Federal identity proofing and the smart card with a digital certificate already meet Assurance Level 4, so no further requirements are needed. PIV cards include both the holder's photograph and a biometric.

As with the proposed electronically signed prescription system, the system provider (the Federal agency) would be required to set access controls, set lock-out times at 2 minutes, require the practitioner to indicate which prescriptions he is authorizing when signing multiple controlled substance prescriptions at one time, provide screens showing the prescription information, and show the warning screen prior to signing. The system would be required to have the practitioner authenticate to the system just prior to signing. The system provider would also be required to check the CA's certificate revocation list (CRL) prior to transmission to ensure that the certificate is still valid. The CRL may be cached until a new CRL is issued.

DEA is proposing that any software system may be used to sign electronic controlled substances prescriptions provided that it has been enabled to process digital signatures and that the PKI module meets the following requirements:

1. The encryption module must comply with FIPS 140–2.

2. The digital signature generation system must comply with FIPS 186–2.

3. The secure hash algorithm must comply with FIPS 180–1.

4. For software implementations, when the signing module is deactivated, the system must clear the plain text password from the system memory to prevent the unauthorized access to, or use of, the private key.

5. The system must have a time system that is within five minutes of the official National Institute of Standards and Technology (NIST) time source.

Item four would ensure that the password cannot be retrieved from the certificate holder's computer memory following its use. Software systems may not automatically clear items from memory when the application is shut down. Therefore, it is necessary to specify that the system clear the password from the system's memory whenever the signing application is closed to ensure that someone cannot recover the password. Item five requires the system to have a time system within five minutes of the official National Institute of Standards and Technology time source. It is important that all users of digitally signed electronic prescriptions be synchronized to a single, consistent time source.

Once the prescription record is digitally signed, both the record and the digital signature must be archived. DEA is proposing that the system provider would be able to adopt one of two options for transmission after signing. The system provider could require transmission immediately on digitally signing or the system provider could ''lock'' and archive the prescription as digitally signed and allow other elements (e.g., pharmacy URL) to be added later. The ''lock'' would have to ensure that any element that was digitally signed could not be altered prior to transmission. For example, the system provider could program its system so that only the DEA-required elements would be digitally signed and only those elements and their digitally signed version are archived.

Unlike the electronically signed prescription approach, the system provider would not be required to apply its own digital signature to the record received from the prescribing practitioner. Because digital certificates from a Federal CA and digital signatures provide a level of security and record integrity that electronically signed prescriptions do not have, DEA is not proposing that a monthly log be generated and checked for digitally signed prescriptions.

When prescriptions are transmitted to retail pharmacies, they are frequently reformatted, making it impossible to validate a digitally signed prescription. DEA is not, therefore, proposing that the digital signature be transmitted with the

[30] National Institute of Standards and Technology. Special Publication 800–32 *Introduction to Public Key Technology and the Federal PKI Infrastructure; February 26, 2001. http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.*

prescription. This provision should eliminate the concern that intermediaries had about the difficulty of transmitting the digital signature. The pharmacy would be required to digitally sign the record as received and archive it, as with electronically signed prescriptions. Where a prescription is sent to a Federal pharmacy, however, the Federal agency may elect to transmit the digital signature and have the pharmacy validate the prescription. In that case, the Federal pharmacy would not be required to digitally sign the prescription. The other pharmacy requirements would be the same as for electronically signed prescriptions. The pharmacy would be required to check the DEA registration and maintain internal audit trails with daily computer checks for auditable events.

DEA is also proposing that Federal agencies using digital signatures would have to have an annual third-party audit of their system processing integrity to ensure that the systems meet DEA's requirements. Prescribing practitioners' use of digital certificates from a Federal or cross-certified CA would make insider identity theft much more difficult, eliminating the need to require the audit to review system security as is the case for the electronically signed prescription systems.

The practitioner would be required to notify the CA if the hard token was lost, stolen, or compromised within 12 hours of discovery of the loss, theft, or compromise. The CA would be required to revoke the certificate upon notification. These requirements are already met by the Federal systems.

Section-By-Section Discussion of the Proposed Rule for Digitally Signed Controlled Substances Prescriptions for Federal Health Care Agencies

In Part 1311, as proposed to be amended as discussed above, DEA is proposing to add a new Subpart D regarding requirements for electronic prescriptions for controlled substances for Federal health care agencies.

Section 1311.200 would state that a practitioner prescribing controlled substances at a Federal health care facility in the course of their official duties may issue a controlled substance prescription electronically if the practitioner is registered as an individual practitioner, or exempt from the requirement of registration, and is authorized under the registration or exemption to dispense the controlled substance, and the practitioner uses an electronic prescription system that meets all of the applicable requirements of the subpart. DEA would propose to define ''Federal health care facility'' as a hospital or other institution that is operated by an agency of the United States (including the U.S. Army, Navy, Marine Corps, Air Force, Coast Guard, Department of Veterans Affairs, Public Health Service, or Bureau of Prisons). An electronic prescription for controlled substances issued through a system that did not meet the requirements of part 1311 would not be considered valid. The section would reiterate the requirement from § 1306.05 that the practitioner is responsible if the prescription does not conform in all essential respects to the CSA and implementing regulations.

Section 1311.205 would establish requirements for issuance and storage of digital certificates. It would require that only Federal Certification Authorities or Certification Authorities cross-certified with a Certification Authority operated by the Federal Public Key Infrastructure Policy Authority may issue digital certificates to practitioners prescribing controlled substances at a Federal health care facility in the course of their official duties to sign electronic controlled substance prescriptions. The digital certificate must be stored on a hardware token that meets the requirements of NIST SP 800–63 Level 4.

Section 1311.210 would state the system requirements for digitally signed prescriptions. Any system may be used to digitally sign electronic prescriptions for controlled substances provided that the system has been enabled to accept digitally signed documents and that it meets the requirements discussed above. DEA would require the system to use two-factor authentication that meets the requirements of NIST SP 800–63, Level 4 as discussed above. The practitioner must reauthenticate to the system if the system is inactive for more than 2 minutes.

Section 1311.215 would require that a digitally signed electronic prescription for a controlled substance created by the system must include all of the data elements required under part 1306.

Section 1311.220 would set the requirements for creating an electronic prescription. Consistent with current regulations governing paper prescriptions, DEA is proposing that the electronic prescribing system may allow the registrant or his agent to enter data for a controlled substance prescription, but only the registrant may sign and authorize the prescription. The system must display information regarding the prescriptions including: The patient's name and address; the name of the drug being prescribed; the dosage strength and form, quantity, and directions for use; and the DEA registration number under which the prescription will be authorized. Finally, the section would require that, where more than one controlled substance prescription has been prepared, the practitioner positively indicate that he has reviewed and approved the information for each prescription prior to signing and authorizing electronic transmission of the prescriptions.

Section 1311.225 would set the requirements for signing an electronic prescription. The practitioner must authenticate to the system using two-factor authentication. This would include the practitioner's declaration that information contained in the record constitutes the practitioner's legal authorization and signature. DEA would require the system to check the certificate revocation list of the Certification Authority that issued the digital certificate of the practitioner who digitally signed the controlled substance prescription. If the certificate is not valid, the system would not be permitted to transmit the prescription. DEA would permit the certificate revocation list to be cached until the Certification Authority issues a new certificate revocation list. If the prescription is being transmitted to a pharmacy that does not accept digitally signed prescriptions, DEA would require the system to include in the data file transmitted an indication that the prescription was signed by the issuing practitioner.

Section 1311.230 would disallow the printing of an electronically transmitted prescription and would also disallow the electronic transmission of a printed prescription as discussed above. These requirements are to prevent an individual electronic prescription from being transmitted more than once to a pharmacy (or pharmacies). The system would be required to retain the archived digitally signed prescription for five years from the date of issuance by the practitioner. Finally, the section would specify that the DEA required contents of the prescription could not be altered after signature without rendering the prescription invalid. The contents could be reformatted; reformatting includes altering the structure of fields or machine language so that the receiving pharmacy system can read the prescription and import the data into the system.

Section 1311.235 would set the requirements for revocation of access authorization. The system would be required to revoke access to sign controlled substance prescriptions on the expiration date of the practitioner's DEA registration, if applicable, unless the Federal agency determines that the

registration or Federal agency authorization has been renewed. The system would be required to check the DEA CSA database at least once a week and revoke access to signing controlled substance prescriptions for any practitioner using the system whose registration or Federal agency authorization has been terminated, revoked, or suspended.

Section 1311.245 would require the Federal agency to notify DEA of certain security incidents, including:

- An individual who is not a DEA registrant authorized by the Federal agency to prescribe controlled substances in the course of their official duties at the Federal agency has been granted access to issue controlled substance prescriptions.
- Access to issue controlled substance prescriptions has been granted to a person using another person's identity.
- Prescription records have been created or altered by an employee not authorized to create or annotate a controlled substance record.
- There have been one or more successful attempts to penetrate the system from the outside.
- The Federal agency has identified any other incident that may indicate that the integrity of the system in regard to controlled substance prescriptions has been compromised.

Section 1311.250 would require the Federal agency to have a third-party audit to verify that the system used to create and transmit controlled substance prescriptions meets the requirements of this subpart prior to accepting any controlled substances prescriptions for transmission and annually thereafter. If the third-party audit finds that the system does not meet one or more of the requirements of the part, the system must not accept for transmission any controlled substance prescription. The Federal agency must also notify the Administration of the adverse audit report and provide the report to the Administration.

Section 1311.255 would specify the practitioner's responsibilities as discussed above. The practitioner would be required to maintain sole possession of the hard token and notify the Certification Authority no later than 12 hours after the discovery of its loss or theft or any indication that the hard token had been compromised. The section would reiterate that the practitioner has the same responsibility for the validity of an electronic prescription as the practitioner does for a paper prescription.

Section 1311.260 would require that if a pharmacy receives a controlled substance prescription from a Federal agency system that is not transmitted with its digital signature, either the pharmacy must digitally sign the prescription immediately upon receipt, or the last intermediary transmitting the record to the pharmacy must digitally sign the prescription immediately prior to transmission and transmit to the pharmacy the prescription and the digitally signed record. The pharmacy must archive the record as received and the digitally signed copy. If a Federal pharmacy receives a digitally signed prescription that includes the digital signature, the pharmacy must validate the prescription and archive the digitally signed record. The pharmacy record must retain an indication that the prescription was validated upon receipt. No additional digital signature is required.

Section 1311.265 would require the pharmacy to check the validity of the DEA registration prior to dispensing the prescription. The pharmacy system must reject a controlled substance prescription if it is not signed or is otherwise not valid. The pharmacy system would have to be able to include all of the information required under part 1306 in the electronic record and be capable of downloading the records in a readable and sortable format, as well as printing the records, if requested.

Section 1311.270 would specify the security requirements for the pharmacy system including a backup storage system at another location, maintaining an internal audit trail, the implementation of a list of auditable events, a daily internal audit to identify if any auditable events have occurred, reporting any security incidents that could affect the integrity of the prescription records, and the annual third-party audit to ensure compliance with the requirements of this part. Audits must be conducted prior to accepting any controlled substances prescriptions for processing and annually thereafter. If the audit finds that the system does not meet the requirements of the part, the system must not process controlled substance prescriptions until the problems have been addressed and another audit indicates that the system meets the requirements of part 1311. The Federal agency must also notify the Administration of the adverse audit report and provide the report to the Administration.

Section 1311.275 would specify the pharmacy's responsibility not to dispense controlled substances in response to an electronic prescription if the pharmacy's system does not meet the requirements of part 1311. In addition, the pharmacy must not dispense a controlled substance if the DEA registration of the prescriber was not valid at the time of signing. Finally, the section would state that nothing in part 1311 relieves a pharmacy of its corresponding responsibility to dispense only in response to a prescription written for a legitimate medical purpose by a prescribing practitioner acting in the usual course of professional practice.

Section 1311.280 would specify recordkeeping requirements for records required by Subpart D of part 1311.

XII. Incorporation by Reference

The following standard is proposed to be incorporated by reference:

NIST SP 800–63, Electronic Authentication Guideline, April 2006.

XIII. Required Analyses

Executive Order 12866

Under Executive Order 12866 (58 FR 51735, October 4, 1993), DEA must determine whether a regulatory action is ''significant'' and, therefore, subject to Office of Management and Budget review and the requirements of the Executive Order. The Order defines ''significant regulatory action'' as one that is likely to result in a rule that may:

(1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal government or communities.

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another agency.

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof.

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in the Executive Order.

A copy of the *Initial Economic Impact Analysis of the Electronic Prescriptions for Controlled Substances Rule* can be obtained by contacting the Liaison and Policy Section, Office of Diversion Control, Drug Enforcement Administration, 8701 Morrissette Drive, Springfield, VA 22152, Telephone (202) 307–7297. The initial analysis is also available on DEA's Diversion Control Program Web site at *http://www.deadiversion.usdoj.gov*. DEA seeks comments on the assumptions used in the economic analysis and is interested in any data that commenters can provide on the time required to comply with the proposed rule.

It has been determined that this Notice of Proposed Rulemaking is an economically significant regulatory action; therefore, DEA has conducted an analysis of the options. The following sections summarize the economic analysis conducted in support of this proposed rule.

Options Considered

DEA considered four options for the electronic prescribing of controlled substances: the rule as proposed with service providers conducting the identity proofing (Base Case); the rule as proposed (Option 1); a modified PKI option (not limited to Federal agencies) (Option 2); and an option that allowed the use of any existing electronic system with no additional requirements except callbacks from the pharmacy to the practitioner to verify the authenticity and integrity for all controlled substance prescriptions (Option 3). Table 7 shows the differing requirements for the rule elements for each of the options.

TABLE 7.—OPTIONS CONSIDERED

Requirement	Base case	Option 1	Option 2	Option 3
Identity Proofing	Conducted by service provider.	Conducted by hospital, state board, law enforcement.	Conducted by hospital, state board, law enforcement.	N/A.
Two-factor, Hard token	Required	Required	Required	N/A.
Authentication protocol	Issued by service provider	Issued by service provider	Digital certificate from CA	N/A.
System requirements	Required	Required	Required	N/A.
Digitally signed record	System level	System level	Practitioner	N/A.
Pharmacy	Digitally sign record on receipt.	Digitally sign record on receipt.	Validate practitioner digital signature.	Call practitioner to confirm each prescription.
Internal Audits	Required	Required	Required	N/A.
Third-party audits	SysTrust/SAS 70 security and processing.	SysTrust/SAS 70 security and processing.	Processing integrity	N/A.

Universe of Affected Entities

The entities that are most directly affected economically by the adoption of electronic prescriptions for controlled substances fall into two groups—practitioners who sign prescriptions and the firms that provide the computer and Internet software and services required for the creation, transmission, and receipt of electronic prescriptions. These firms serve either practitioners' offices or pharmacies. The affected universe does not include pharmacies directly, because the rule does not require any change in their operating practices; although their computer systems may need to be updated, the additional prescription processing steps (primarily digitally signing the record on receipt) will be handled by the system, not the pharmacist. For options 1 and 2, DEA-registered hospitals or other officials allowed to conduct identity proofing would also be affected.

The registered practitioners are primarily physicians, dentists, and mid-level practitioners (physician's assistants and nurse practitioners). Most other practitioner registrants are less likely to prescribe as opposed to administer or dispense controlled substances (e.g., veterinarians).

As discussed above, the service providers are vendors of the computer software and Internet services required by practitioners' offices for electronic creation and transmission of prescriptions and of the services required by pharmacies for receiving and processing electronic prescriptions. Many service providers to practitioners are application service providers (ASPs). Some of the service providers to pharmacies are ASPs, but most are not. Table 8 displays data on current numbers of practitioners and estimated future growth rates.

TABLE 8.—PRACTITIONER UNIVERSE

Affected Universe—Practitioners		
	Current No.	Future annual growth rate (percent)
Physicians	312,759	0.1
Dentists	170,969	0.5
Mid-levels	89,744	2.2
Total	573,472	0.5

The number of physicians is based on CDC data on the number of physicians in office-based practices. Current numbers for dentists and mid-level practitioners are DEA registrants as of December 3, 2007, with two modifications. The number of mid-level practitioners reported in this count includes, in addition to physician's assistants and nurse practitioners, workers in other health occupations who rarely sign prescriptions and who, therefore, have not been included. In addition, because many mid-level practitioners work at hospitals, the total was reduced by 25 percent because these practitioners may not write prescriptions. Estimated growth rates are based on recent trends. Regarding physicians, the trend since 2000 indicates a very slight negative growth rate. DEA does not believe this downward trend will continue; therefore, an annual growth rate for physicians of 0.1 percent has been estimated. The rate for the total number is the weighted average of the separate rates.

While the current count of systems certified by SureScripts or CCHIT (or both) for practitioners is 119, DEA has adjusted that figure downward to 110 for Year 1 of the analysis. With 119 firms offering these services and products to practitioners, it seems certain that some of them are in a marginal business condition with respect to this market. Consequently, DEA projects a steady diminution over time in the number of firms. It also seems reasonable to assume that some of them will withdraw from the market at the outset. There are three reasons for this result. First, the market has already seen firms leave the market as the demand for the products has not met expectations. Second, the security arrangements at some firms may be insufficient to withstand the required security audit, and, for a number of reasons, some of these firms may be unwilling or unable to remedy this defect. Third, some firms may not want to incur the reprogramming costs necessary to include electronic prescriptions for controlled substances capability in their service, and it is highly unlikely that a firm would try to stay in the market without controlled substances capability, as that would place it at a severe competitive disadvantage. A relevant point here is that most current firms offer electronic

health records (EHRs), with electronic prescription functionality as part of the EHR; the reprogramming costs may be much higher for firms that support only electronic prescriptions—just under $150,000 compared to a little under $40,000 for firms with EHR capability. To gain certification from CCHIT, EHR products must already include many of the security functions DEA is specifying in the proposed rule. Of the 119 vendors now in the market, 103 are EHRs. Those that are not EHRs are clearly more likely to be deterred by cost. DEA assumes that six of the electronic prescription-only vendors will withdraw from the market rather than add electronic controlled substances prescribing capability, while three of those that support EHR will also withdraw. Table 9 presents the service provider universe.

TABLE 9.—SERVICE PROVIDER UNIVERSE

Affected Universe—Service Providers		
	Current No.	Projection
Service providers to practitioners ...	119 Adjusted to 110	The number of firms is expected to diminish over time, stabilizing at 20 vendors after ten years.
Vendors to pharmacies (some are ASPs, most are not).	20	Provision of computer and Internet services to pharmacies is already a mature market segment; the number is not expected to change.

Unit Costs

In estimating unit costs of the rule, the first step is to establish the baseline with which to determine the costs that are incremental with respect to the rule. DEA presumes that no practitioner's office will adopt electronic prescribing simply to write controlled substance prescriptions; controlled substance prescriptions constitute about 11 percent of the total number of prescriptions. The costs to a practitioner's office of complying with the rule, therefore, are only the costs directly required by the electronic prescriptions for controlled substances rule and do not include any of the costs that the office would incur for setting up electronic prescription capability without electronic prescribing of controlled substances.

Requirements

- In-person identity proofing (§ 1311.105) imposes costs on practitioners, the institutions that conduct the identity proofing, and service providers (filing the information submitted and confirming the application).
- Two-factor authentication (§ 1311.110) requires that each practitioner with authority to sign controlled substance prescriptions has a unique hard token to gain access to the system. This imposes costs on some practitioners who do not already have a token (e.g., a PDA).
- Monthly review of controlled substance prescription logs (§ 1311.140) by practitioners imposes a cost on practitioners. (Applies only to Base Case and Option 1)
- System requirements (§§ 1311.110–1311.145) imposes reprogramming costs on service providers.
- Requirements (§ 1311.150) for annual third-party audits imposes costs on service providers.

Costs

Identity proofing. Identity proofing requires a face-to-face meeting between each practitioner who will use the system and either the service provider (Base Case) or a person from a DEA-registered hospital or other official (Options 1 and 2). For the Base Case, DEA assumes that the practitioner and service provider would spend 2 minutes each at the practice; the service provider would spend another 8 minutes at its offices checking the State license and DEA registration and filing the information gathered. Because most physicians have privileges at hospitals, DEA assumes that for Option 1 and 2 identity proofing would take only 10 minutes for physicians. All other practitioners are assumes to need an hour to travel to and from a hospital or police station plus the 10 minutes for the proofing. Each practitioner would also spend another 1 minute verifying the application when called by the provider. For each practitioner, the hospital staff are assumes to spend 10 minutes checking the identity documents and completing the form. The service provider will spend another 11 minutes at the service provider's office verifying State license and DEA registration information, entering the practitioner's data into the service provider's record of identity proofing, and calling the practitioner to verify. These costs are the same for Options 1 and 2, although under Option 2 the cross-signed identity proofing document would be sent to the Certification Authority.

Two-factor authentication. Two-factor authentication requires that access to the system can be gained only with a hard token, uniquely coded for each practitioner. A number of devices will serve for this purpose: *e.g.*, PDAs, Blackberries, thumb drives, multi-factor one-time-use password tokens. It is assumes that physicians and dentists will already have one of these devices and be familiar with its use. The same cannot be assumed for mid-level practitioners. DEA assumes that tokens will have to be purchased for 75.0 percent of mid-level practitioners and those mid-level practitioners will require training in the use of the tokens. DEA assumes that the tokens will be thumb drives. Time required for training is estimated to be ten minutes per mid-level practitioner. Using the hourly wages (including fringes and overhead) for physician's assistants for $77, the training cost is estimated to be $12.82. A thumb drive costs $12.00. One-time-password tokens may be more or less expensive; some of these can be installed on cell phones, which any practitioner would have.

Digital Certificate. Under Option 2, practitioners would be required to obtain a digital certificate from a certification authority cross-certified with a Federal Certification Authority. The annual cost of digital certificates varies from CA to CA depending on the security characteristics. DEA assumes an annual cost of $30.

Monthly review of controlled substance prescription logs. Under the Base Case and Option 1, once a month, each practitioner must review a log of his controlled substance prescriptions for that month. As discussed above, DEA is not proposing to require a comprehensive review. DEA estimates that a practitioner can review the log for unusual controlled substance prescriptions in an average of two minutes. DEA recognizes that there will be a considerable range in review time

based on the number of controlled substance prescriptions a practitioner writes. The average cost is estimated to be $89 per year, using a weighted hourly wage for all practitioners.

Reprogramming requirements. Under the Base Case, Option 1, and Option 2, all service providers, including those that serve pharmacies, will have to do some reprogramming to add electronic controlled substance prescription-required functions to their systems. Depending on the functionalities of their existing systems, they will need more or less reprogramming. Two requirements in particular will necessitate some reprogramming for almost all systems that serve practitioners. These are the provision that the first recipient system digitally sign and archive the controlled substance prescription on receipt and that the system will transmit from a practitioner's office immediately following the practitioner's signature with the hard token. (At least one service provider already digitally signs prescriptions, and more than one transmit the prescription immediately upon signature.) The requirement for a screen indicating that the prescriber understands that the prescription is being signed will also be new for systems. Other requirements will affect only some providers. Limiting access to signing to practitioners may require reprogramming of some systems, though this functionality is generally part of systems. The need to show all of the selected prescription information on a single screen may require new programming for a few systems. For some stand-alone systems, the requirements for two-factor authentication at Level 4 will require reprogramming as will requirements for reauthentication after a period of inactivity. As shown in the table of requirements in Section IX above, most EHRs already support these functions. Consequently, the reprogramming required for EHR systems will be less than for stand-alone systems.

Systems that serve pharmacies will also require some reprogramming, primarily for digitally signing the record as received. Those pharmacy systems that operate as ASPs should already have digital signature capability; others may need to do additional programming to add that functionality. Both will need to add programming to sign the record. The industry has indicated that the requirements for internal audit trails and internal audit analysis are part of existing systems.

DEA has estimated that EHR systems and pharmacy ASP systems will require an additional 500 hours to program and test the new functions. For stand-alone electronic prescription systems and installed pharmacy systems, DEA estimates that they will spend 2,000 hours to program and test the new functions. Using the hourly wage rate for programmers of $73 (loaded), the initial programming cost will be $36,700 for EHR and pharmacy ASP systems and $146,500 for stand-alone systems and installed pharmacy systems.

Auditing requirements. Under the Base Case, Option 1, and Option 2, all system providers that serve practitioners and those that serve pharmacies must undergo an annual third-party audit. Under the Base Case and Option 1, the audit would have to meet the requirements for a SysTrust, WebTrust, or SAS 70 audit for security and processing integrity. The first such audit for a service provider is generally more costly than subsequent audits. DEA estimates the following per-vendor costs for audits: First-year audits: $125,000; Subsequent audits: $100,000. Under Option 2, the audit would need to address only processing integrity (*i.e.*, that the system reliably meets DEA's requirements). Because of the limited scope of this audit, it could be conducted by a broader range of auditors; DEA estimates an annual cost of $25,000.

DEA notes that the costs of a SysTrust or SAS 70 audit range from $15,000 to $250,000 depending on the size of the company. DEA used a conservative estimate of $125,000 for the initial audit although in many cases the cost for the DEA required audit elements would be less. A full SysTrust or SAS 70 audit covers five areas; DEA is requiring that the audit address only two of those, physical security and processing integrity.

Callbacks. For Option 3, the only cost of electronic prescriptions for controlled substances would be the callback from the pharmacy to the practitioner to confirm the prescription. DEA estimates that this would take 3 minutes of staff time at the practitioner's office to pull the file and refile it, 1 minute of the practitioner's time, and 3 minutes of a pharmacy technician's time; the total cost per call would be $6.55.

Table 10 summarizes unit costs.

TABLE 10.—UNIT COSTS

Requirement	Unit time	Wage rate	Unit cost
Identity Proofing			
Practitioner (Base)	2 minutes	$222.51	$7.42
Service Provider (Base)	2 minutes	83.80	2.79
Service Provider clerk (Base)	8 minutes	33.89	4.52
Service Provider	10 minutes	33.89	5.65
Storage at service provider			0.01
Service Provider (1)	13 minutes	33.89	5.35
Practitioner (1 & 2):			
MDs	11 minutes	269.00	49.32
Dentists	11 minutes	214.07	39.25
Mid-level practitioners	11 minutes	76.94	14.11
Practitioner travel time:			
Dentists	1 hour	214.07	214.07
Mid-level practitioners	1 hour	76.94	76.94
Hospital	10 minutes	35.55	5.93
Mailing time	2 minutes	30.33	1.01
Mailing cost			0.41
Total—MDs (1 & 2)			62.32
Total—Dentists (1 & 2)			266.31
Total—Mid level practitioners (1 & 2)			104.05

TABLE 10.—UNIT COSTS—Continued

Requirement	Unit time	Wage rate	Unit cost
2-Factor Token			
Learning time	10 minutes	76.94	12.82
Token			12
Digital Certificate			30/year
Log review	24 minutes/year	222.51	89.01
Programming			
EHR/Pharmacy ASP	500 hours	73	36,623
Other systems	2,000 hours	73	146,490
Third-Party Audit (Base, 1)			125,000 (first year) 100,000 (following)
Third-Party Audit (2)			25,000 per year
Option 3:			
Callback	1 minute practitioner	222.51	6.55
	3 minutes med. staff	30.60	
	3 minutes pharmacy tech	26.23	

Total costs

To estimate total costs, it is first necessary to establish the distribution of costs over time. The costs to be considered in the analysis may be divided into start-up costs and ongoing costs. For a practitioner's office, the start-up costs are incurred in the year in which the office implements electronic prescribing of controlled substances, and the ongoing costs are incurred in every year thereafter. For service providers, all the start-up costs are incurred in Year 1 of the analysis. DEA presumes that all service providers will add controlled substance electronic prescribing capability to their systems in the first year, lest they be placed at a competitive disadvantage. But this will not be the case for practitioners' offices. They will implement electronic prescribing of controlled substances over time as they implement electronic prescriptions and EHRs. DEA has projected complete implementation of electronic prescribing of controlled substances over a 15-year period; i.e., at the end of the 15th year of the analysis, all practitioners' offices will have controlled substance electronic prescribing capability in their electronic prescription systems. This is essentially an estimate of the rate of electronic prescription implementation. As practitioners adopt electronic prescription capabilities, they will include electronic prescribing of controlled substances in the package, as the incremental cost of doing so for an office is very slight. DEA notes that although the selection of the implementation period is somewhat arbitrary, DEA believes that 15 years is a reasonable estimate to reflect the balance between pressure from insurers, who want practitioners to implement EHR systems, and the reluctance of practitioners to invest in expensive systems that are time-consuming to implement and perhaps not yet fully tested.

Table 11 shows the schedule at which DEA projects implementation over time.

TABLE 11.—IMPLEMENTATION SCHEDULE

	Percentage of offices implementing in a year	Cumulative implementation percentage
Year 1	6.0	6.0
Year 2	4.0	10.0
Year 3	4.0	14.0
Year 4	5.0	19.0
Year 5	5.0	24.0
Year 6	5.0	29.0
Year 7	6.0	35.0
Year 8	6.0	41.0
Year 9	7.0	48.0
Year 10	9.0	57.0
Year 11	10.0	67.0
Year 12	11.0	78.0
Year 13	11.0	89.0
Year 14	6.0	95.0
Year 15	5.0	100.0

The rate in Year 1 is somewhat higher than the rate in the next several years, because about 6 percent of offices have already adopted electronic prescription systems. After dropping in Year 2, the rate rises gradually to a peak in Years 12 and 13 and then drops as full implementation approaches. This is based on the observation that adoption of electronic prescribing has been slow to date and that many practitioners are very reluctant to accept changes in the basic methods with which they conduct their practices, especially the direct introduction of computer-based systems into their own work.

The start-up costs incurred by practitioners' offices in each year will be based on the number of practitioners in offices implementing controlled substances electronic prescribing capabilities in that year. Ongoing costs for practitioners will be based on the total number of practitioners in offices where electronic prescribing of controlled substances has been implemented in a given year, i.e., the cumulative percentage of practitioners in offices that have adopted electronic prescribing of controlled substances. Both start-up costs and ongoing costs will also reflect the annual growth rates of the different classes of practitioners—0.1 percent for physicians, 0.5 percent for dentists, and 2.2 percent for mid-level practitioners.

Start-up costs for practitioners are the initial identity proofing and the purchase of hard tokens, and training in their use, for some of the mid-level practitioners. The major ongoing cost under the Base Case and Option 1 is the monthly log review. But there is also some ongoing cost associated with turnover of personnel in practitioners' offices. When a practitioner moves to a new office, there is a high likelihood that the transfer will also be a move between system vendors; when that is the case, there must be a new identity proofing for that individual. Transfers of mid-level practitioners may require new purchases of hard tokens.

Some further assumptions beyond implementation and growth rates must be made to estimate total costs for practitioners' offices and service providers. These are as follows:

- For the Base Case, percentage of initial identity proofing visits by service provider staff where the travel to the office is needed only for the identity

proofing: 15.0 percent. (Percentage of non-EHR systems). For ongoing identity proofing visits due to personnel turnover, there is no incremental travel.

- Percentage of personnel transfers between offices that are also transfers between service providers: 90.0 percent.
- Annual turnover rate for physicians and dentists: 2.5 percent.
- Annual turnover rate for mid-level practitioners: 5.0 percent.

As noted earlier, the service providers will incur all their start-up costs, apart from identity proofing, in Year 1 of the analysis. Aside from identity proofing, their ongoing costs will be the annual audits. The cost per service provider will remain the same over time, but the total cost will diminish as the number of service providers serving practitioners declines in an ongoing process of attrition due to over-population on the supply side of the market. Although this reduction may seem large, DEA notes that in the mid-1980s, there were about 400 word processing software systems; only a few remain.[31] The number of service providers serving pharmacies remains stable at 20 throughout the analysis period. Table 12 shows DEA's projection of the number of providers serving practitioners.

TABLE 12.—PROJECTED REDUCTION IN ELECTRONIC PRESCRIPTION SERVICE PROVIDERS

	Number of providers serving practitioners
Year 1	110
Year 2	95
Year 3	80
Year 4	70
Year 5	60
Year 6	50
Year 7	40
Year 8	30
Year 9	25
Year 10	25
Year 11	20
Year 12	20
Year 13	20
Year 14	20
Year 15	20

The results of the unit costs and the foregoing assumptions about distribution of costs over time and other items are summarized in Tables 13 and 14, showing the annualized cost, over 15 years at a 7 percent and a 3 percent discount rate. Table 15 presents a summary of annualized costs for the four options.

TABLE 13.—ANNUALIZED COST PER OPTION AND REQUIREMENTS

[7% Discount rate]

	Practitioners	Providers	Total
	Base Case 7.0 percent		
Identity Proofing	$352,367	$459,425	$811,792
Tokens	90,757		90,757
Training	75,147		75,147
Log reviews	22,495,039		22,495,039
Reprogramming		824,224	824,224
Audits		8,264,492	8,264,492
Total			32,561,452
	Option 1		
Identity Proofing	6,151,445	354,910	6,506,355
Tokens	90,757		90,757
Training	75,147		75,147
Log reviews	22,495,039		22,495,039
Reprogramming		824,224	824,224
Audits		8,264,492	8,264,492
Total			38,256,015
	Option 2		
Identity Proofing	6,151,445	354,910	6,506,355
Tokens	90,757		90,757
Training	75,147		75,147
Digital Certificates	7,582,154		7,582,154
Reprogramming		703,606	703,606
Audits		3,636,812	3,636,812
Total			18,594,831
	Option 3		
Callbacks	1,023,778,891	256,261,645	1,280,040,536

[31] Bergin, T.J., ''The Proliferation and Consolidation of Word Processing Software: 1985–1995.'' *IEEE Annals of the History of Computing.* Volume 28, Issue 4, Oct.–Dec. 2006 Page(s):48–63.

TABLE 14.—ANNUALIZED COST PER OPTION AND REQUIREMENTS

[3% Discount rate]

	Practitioners	Providers	Total
	Base Case 3.0 percent		
Identity Proofing	$357,789	$443,823	$801,612
Tokens	94,227	.....	94,227
Training	76,832	.....	76,832
Log reviews	24,389,580	.....	24,389,580
Reprogramming	.....	628,833	628,833
Audits	.....	7,401,186	7,401,186
Total	.....	.....	33,392,270
	Option 1		
Identity Proofing	6,269,439	360,851	6,630,290
Tokens	94,227	.....	94,227
Training	76,832	.....	76,832
Log reviews	24,389,580	.....	24,389,580
Reprogramming	.....	628,833	628,833
Audits	.....	7,401,186	7,401,186
Total	.....	.....	39,220,948
	Option 2		
Identity Proofing	6,269,439	360,851	6,630,290
Tokens	94,227	.....	94,227
Training	76,832	.....	76,832
Digital Certificates	8,220,726	.....	8,220,726
Reprogramming	.....	536,808	536,808
Audits	.....	3,369,812	3,369,812
Total	.....	.....	18,928,003
	Option 3		
Callbacks	1,123,085,458	281,119,029	1,404,204,487

TABLE 15.—TOTAL ANNUALIZED COSTS

	7.0 percent	3.0 percent
Base Case	$32,561,000	$33,392,000
Option 1	38,256,000	39,221,000
Option 2	18,595,000	18,928,000
Option 3	1,280,041,000	1,404,205,000

The two largest cost drivers for the Base Case are the monthly log review for practitioners and the annual audits for the service providers. The cost for practitioners almost disappears without the log review; with the 7.0 percent interest rate, it drops to under $1.0 million. The annual audits account for approximately $8 million of the cost to service providers at the 7.0 percent rate. For Options 1 and 2, identity proofing is a significant cost; these costs fall mainly on practitioners who do not routinely visit hospitals as part of their practices. For Option 2, digital certificates are also a significant cost, but audits are a lower cost. Option 3 is far more costly than any of the other options although it entails no upfront costs and imposes no costs on the service providers.

Benefits

The benefits often ascribed to electronic prescriptions are not directly attributable to this rule except to the extent the rule facilitates implementation of electronic prescribing. Electronic prescriptions may provide benefits to patients by reducing medication errors caused by illegible or misunderstood prescriptions. They may also reduce processing time at the pharmacy, callbacks to practitioners, and waiting time for patients. To estimate the part of these benefits that may accrue to the proposed rule, DEA estimated the number of controlled substance prescriptions that may require callbacks (approximately 27 percent of original prescriptions). Assuming that electronic controlled substance prescriptions phased in over 15 years, as described above, the annualized time-saving for eliminating these callbacks would be $316 million (at 7% discount) or $346 million (at 3% discount). Electronic prescriptions could also reduce the patient's wait time at the pharmacy. Assuming the average wait time is 15 minutes for the 81 percent of original prescriptions that are presented on paper to retail pharmacies (not mail order or long-term care prescriptions), at the current United States average hourly wage ($19.62), the annualized savings over 15 years would be $589 million (at 7% discount) or $646 million (at 3%

discount). The estimates for public wait time are upper bounds. They assume that the practitioner will transmit the prescription and that the pharmacist will open the record and fill it before the patient arrives at the pharmacy. It is probably more realistic to assume that only a fraction of these benefits will be gained. There may also be some offsetting costs to the pharmacy. The industry estimates that about 20 percent of prescriptions written are never presented to pharmacies. If these are sent to pharmacies electronically and prepared before the patient arrives, the pharmacy will have spent time for which it will not be reimbursed if the patient does not pick up the prescription. (It may be reasonable to expect the 20 percent to decline with electronic prescriptions, although probably not to zero.) Table 16 presents the annualized benefits at a 7 percent and 3 percent discount rate.

TABLE 16.—ANNUALIZED BENEFITS

	7.0 percent	3.0 percent
Callbacks Avoided	$315,626,000	$346,242,000
Public Wait Time Avoided	588,732,000	645,839,000

The benefits, both of which represent time savings, clearly exceed by a wide margin the costs of the Base Case and Options 1 and 2. The costs of Option 3 at $1.3 to $1.4 billion a year exceed the benefits, which would not, of course, include callbacks eliminated.

Other Benefits. DEA has not attempted to quantify any reduction in medical errors. Most of the studies on medication errors have been done in hospital settings; the studies of outpatient errors do not usually disaggregate the types of errors to distinguish those that could be prevented by accurate electronic prescriptions (e.g., misread illegible prescriptions versus a dispensing error such as inadvertently selecting the wrong drug or wrong strength); and none indicate what percentage of errors are related to controlled substances. In addition, although electronic prescriptions should eliminate illegibility issues, some of these mistakes may be replaced by keying errors. DEA expects that there will be reduced medication errors linked to more readable prescriptions, but decided that it did not have a reasonable basis for quantifying the benefits.

Another benefit of electronic prescriptions for controlled substances that is ascribable to the proposed rule, but not easily quantified and monetized, would come from reductions in controlled substance prescription forgery and alteration. Prescription forgery, alteration, and misuse (e.g., faxing the same prescription to multiple pharmacies) is a part of the total illegal market for diversion of legal drugs. Diversion of legal medication for illegal consumption usually involves controlled substances. Diversion and abuse are significant social problems; the proposed rule is intended to help curb some of these illegal activities.

As discussed above, diversion of prescription drugs through forgery, doctor shopping, and alteration of pharmacy records is a growing problem. Controlled substances are diverted in a number of ways, some of which will not be affected by electronic prescriptions. For example, diversion occurs when:

- Drugs are stolen from practitioners and pharmacies.
- Practitioners knowingly write nonlegitimate prescriptions.
- Practitioners write prescriptions for people who have lied about symptoms to obtain the drugs. A commonly used term for these types of patients is ''doctor shoppers,'' people who routinely visit different doctors with the same ailment to obtain multiple prescriptions for controlled substances, usually pain relievers. These prescriptions are then filled at various pharmacies and the drugs are abused or sold on the illicit market.

Although DEA does not expect this rule to eliminate these problems, it may act as a deterrent to practitioners who write nonlegitimate prescriptions and to doctor shoppers because it will be easier for States that have prescription monitoring programs to monitor prescriptions when they are electronic and because digitally signed prescriptions will make it very difficult for a practitioner to claim that a digitally signed prescription has been forged or altered. Some States are already using prescription monitoring programs to identify practitioners who prescribe unusual quantities of controlled substances and patients filling multiple prescriptions at different pharmacies.

Electronic prescriptions for controlled substances will directly affect the following types of diversion:

- Stealing prescription pads or printing them, and writing nonlegitimate prescriptions.
- Altering a legitimate prescription to obtain a higher dose or more dosage units (e.g., changing a ''10'' to a ''40'').
- Phoning in nonlegitimate prescriptions late in the day when it is difficult for a pharmacy to complete a confirmation call to the practitioner's office.
- Faxing a prescription to multiple pharmacies.
- Altering a pharmacy record to cover the diversion of controlled substances.

These are examples of prescription forgery that contribute significantly to the overall problem of drug diversion. DEA expects this rule to reduce significantly these types of forgeries because only practitioners with secure prescription-writing systems will be able to issue electronic prescriptions for controlled substances and because any alteration of the prescription at the pharmacy will be discernible from the audit log and a comparison of the digitally signed records. DEA expects that over time, as electronic prescribing becomes the norm, practitioners issuing paper prescriptions for controlled substances may find that their prescriptions are examined more closely.

DEA is not aware of any comprehensive data on controlled substance prescription diversion in general, and forgeries in particular. DEA does not track information on prescription forgeries and alterations because enforcement is generally handled by State and local authorities. The cost of enforcement is, however, considerable. In 2007, DEA spent between $2,700 for a small case and $147,000 for a large diversion case just for the primary investigators; adjudication costs and support staff are additional. It is reasonable to assume that State and local law enforcement agencies are spending similar sums per case. As discussed above, some cases involve multiple jurisdictions, all of which bear costs for collecting data and deposing witnesses. The rule as proposed could reduce the number of cases and, therefore, reduce the costs to governments at all levels. A reduction in forgeries would also benefit practitioners who would be less likely to be at risk of being accused of diverting controlled substances and of then having to prove that they were not

responsible. In contrast, a less secure electronic prescription system could greatly increase diversion and the number of forgeries and diversion cases and dramatically increase investigation costs if every provider and intermediary involved in a transaction had to provide testimony.

A reduction in forged controlled substance prescriptions could also result in a reduction in drug addiction-related deaths, injuries, and crime. The 2006 NSDUH found that 6.7 million people in the United States currently use prescription-type therapeutic drugs for nonmedical reasons. SAMHSA reported that in 2003, in six States (Maine, Maryland, New Hampshire, New Mexico, Utah, and Vermont) there were 352 deaths from misuse of oxycodone and hydrocodone, both prescription controlled substances.[32] The 32 metropolitan areas that are part of the Drug Abuse Warning Network reported 3,530 deaths from misuse of oxycodone and hydrocodone and 1,381 deaths that involved the misuse of benzodiazepines in 2003.[33] In another report, SAMHSA stated that in 2004 there were 42,491 emergency room visits involving nonmedical use of hydrocodone, 36,559 visits for nonmedical use of oxycodone, and 144,000 visits for nonmedical use of benzodiazepines (Schedule IV).[34] By 2005, the number of emergency visits for nonmedical use of these drugs rose to 51,225 for hydrocodone, 42,810 for oxycodone, and 172,388 for the benzodiazepines. For all non-medical use of prescription opiates except methadone, the number of visits was about 155,000.[35] The costs of the deaths in the six States is more than $1 billion (at $3 million per life) and in the metropolitan areas more than $10 billion. The cost of the emergency room visits is above $300 million (at $1,000 per visit). A recent study of drug diversion and insurance fraud estimated that drug diversion costs health insurers $72 billion a year because of claims for fraudulent prescriptions and treating patients for the effects of drug abuse.[36] If the proposed rule prevents even a small fraction of these costs, the benefits will far exceed the implementation costs.

Regulatory Flexibility Act

Under the Regulatory Flexibility Act of 1980 (5 U.S.C. 601–612) (RFA), Federal agencies must evaluate the impact of rules on small entities and consider less burdensome alternatives. DEA has conducted an initial Regulatory Flexibility Analysis and concluded that although the rule will affect a substantial number of small entities, it will not impose a significant economic impact on any regulated entities. The only entities regulated by DEA under this rule would be DEA registrants—prescribing practitioners and pharmacies. The service providers, although indirectly affected by the rule, are not registrants. Under the proposed rule, service providers may design and implement their systems and services in any way they choose. A DEA registrant, however, may not use a system that does not meet the requirements of the rule to create, transmit, receive, or process a controlled substance prescription. Nothing in this rule compels a DEA registrant to issue or process controlled substance prescriptions electronically. Practitioners may continue to issue controlled substances prescriptions on paper and, where permitted, by fax or telephone. Besides being only indirectly affected by the rule, the service providers are expected to recover their costs from registrants and others who purchase the software and systems.

Characteristics of Small Entities

As discussed in previous sections, the small entities directly affected by the proposed rule are practitioners and to a limited extent pharmacies. The firms marketing services and software are not directly affected by the rule because they will recover their costs from practitioners. Nonetheless, DEA will discuss the impact on these firms. Table 17 shows Small Business Administration's standards for these firms.

TABLE 17.—SBA DEFINITIONS OF SMALL ENTITIES

Affected entity	Industry description	NAICS code	Small business definition (sales in $)
Practitioner and Mid-Level Practitioner	Offices of Physicians	62111	$9,000,000
	Offices of Dentists	621210	6,500,000
Service Provider	Software Publishing	511210	23,000,000
Pharmacy	Pharmacies and Drug Stores	44611	6,500,000
	Supermarkets and Other Grocery Stores	44511	25,000,000
	General Merchandise Stores	45291	25,000,000
	Mail Order Houses	454113	23,000,000

Although some practitioners are part of large practices that may qualify as large businesses, so few practitioners fall into the large category that it is simpler to assume that they are all small entities. It is also the case that the service providers generally charge on a per practitioner basis rather than a per practice basis so that the costs may be considered as applying to individual practitioners. Mid-level practitioners are generally employed by a practice so their costs would be incurred by the practice, not the individual. They are not, therefore, small businesses.

The lowest average net income for a physician in private practice listed in the Allied-Physician Survey is $135,000.[37] The American Dental Association states that the average net

[32] The New DAWN Report—Opiate-related Drug Misuse Deaths in Six States, 2003. Issue 19, 2006; *http://dawninfo.samhsa.gov/pubs/shortreports/*.

[33] Substance Abuse and Mental Health Services Administration, Office of Applied Studies. *Drug Abuse Warning Network, 2003: Area Profiles of Drug-Related Mortality*. DAWN series D–27, DHHS Publication No. (SMA) 05–4023, Rockville, MD, March 2005; *http://dawninfo.samhsa.gov/pubs/mepubs/*.

[34] Substance Abuse and Mental Health Services Administration, Office of Applied Studies. The DAWN Report—Emergency Department Visits Involving Nonmedical Use of Selected Pharmaceuticals. Issue 23, 2006; *http://dawninfo.samhsa.gov/pubs/shortreports/*.

[35] Substance Abuse and Mental Health Services Administration, Office of Applied Studies. *Drug Abuse Warning Network, 2005: National Estimates of Drug-Related Emergency Department Visits*. DAWN Series D–29, DHHS Publication No. (SMA) 07–4256, Rockville, MD, March 2007; *http://dawninfo.samhsa.gov/pubs/edpubs/default.asp*.

[36] Coalition Against Insurance Fraud, ''Prescription for Peril: How Insurance Fraud Finances Theft and Abuse of Addictive Prescription Drugs,'' December 2007.

[37] *http://www.allied-physicians.com/salary-surveys*, accessed 1/16/2008.

income of a dentist in private practice is $185,940 for a general practitioner. The average gross billings for a dentist in general practice per dentist is $595,340.[38] For pharmacies, the 17,500 independent pharmacies are small entities; the other pharmacies belong to about 200 chains that are mostly large firms. There may be a few chains with fewer than 3 pharmacies, which could be small. In 2006, National Association of Chain Drug Stores data indicate that the average independent pharmacy had prescription sales of $2.48 million a year; average total sales are about $2.675 million.[39]

As discussed above, DEA estimates that there are about 130 service providers (110 for electronic prescriptions, 20 for pharmacies) that will be indirectly affected by this rule. A few of these are large entities or part of large companies (e.g., General Electric and McKesson). DEA has no information on the revenues of most of these firms. DEA notes that fully electronic EHRs cost between $20,000 and $50,000 per practitioner, with a usual monthly maintenance fee of $500 per practitioner. A provider, therefore, would need fewer than 4,000 practitioners to qualify as a large business. The providers of stand-alone electronic prescribing systems charge a tenth as much and are assumed to be small entities.

Costs to Small Entities

The costs to DEA registrants are relatively small. As noted above, the initial costs to the practitioner would range from about $62 to $266 for identity proofing, mostly for the time to have the identification checked. The main ongoing costs for the proposed rule would be the monthly log review by practitioners (about $89 a year) plus any incremental cost of the software or service. The initial and ongoing costs for the basic rule elements represent less than 0.2 percent of the annual income of the lowest paid practitioner.

Determining the incremental cost of the system requirements per practitioner is difficult because it depends on the number of providers, the number of customers, the number of system requirements that a service provider does not already meet, and how costs are recovered (in the year in which the money is spent or over time). For example, an EHR system that had to reprogram to the full extent would have incremental system costs of $161,000 ($125,000 for the third-party audit and $37,000 for reprogramming). If the service provider had 1,000 practitioners enrolled in the first year, it would also incur about $5,660 for identity proofing. If the service provider recovered the costs ($167,000) from its 1,000 customers, the incremental cost to those customers would be $167 or about $14 a month. The costs in the out years would be lower because no further programming is needed and the audit cost is lower ($100,000). If the service provider added 1,000 practitioners a year over 15 years, the incremental cost per practitioner would fall as shown in Table 18. The costs shown are conservative because the audits may cost considerably less depending on the complexity of the system; many EHRs may need little reprogramming. Either or both of these factors in combination could reduce their costs considerably and, therefore, reduce the incremental costs to practitioners.

TABLE 18.—INCREMENTAL COST OF EHR SYSTEMS TO PRACTITIONERS

Year	No. Practitioners	Total provider costs	Annual cost/ practitioner	Monthly cost/ practitioner
1	1000	$167,70	$167.27	$13.94
2	2000	105,648	52.82	4.40
3	3000	105,648	35.22	2.93
4	4000	105,648	26.41	2.20
5	5000	105,648	21.13	1.76
6	6000	105,648	17.61	1.47
7	7000	105,648	15.09	1.26
8	8000	105,648	13.21	1.10
9	9000	105,648	11.74	0.98
10	10000	105,648	10.56	0.88
11	11000	105,648	9.60	0.80
12	12000	105,648	8.80	0.73
13	13000	105,648	8.13	0.68
14	14000	105,648	7.55	0.63
15	15000	105,648	7.04	0.59

In the first year, the total cost to a physician for DEA's requirements would be less than $300; dentists would have higher initial costs because of travel time. After that, the cost will decline over time to about $100 to $150 a year including the incremental costs charged for the systems. The lowest paid physician earns about $135,000 a year. For none of the registrants will the cost represent a significant economic impact.

For pharmacies, the only costs will be the incremental cost that their service provider charges to cover the costs of reprogramming and audits. In the first year, if the service providers recover the programming costs in a single year, the average incremental cost to a pharmacy would be $85. After that, the incremental charge to recover the cost of the third-party audit would be $35 per pharmacy, assuming the cost is evenly distributed across all pharmacies. The first year charge represents 0.003 percent of an independent pharmacy's annual sales. It also represents a far lower cost than the pharmacy will pay SureScripts or another intermediary for processing the prescriptions. Currently, SureScripts charges the pharmacy $0.215 per electronic prescription to process and reformat prescriptions to ensure that the pharmacy system will be able to capture the data electronically. Based on National Association of Chain Drug Stores data on the average price of prescriptions ($68.26) and the average value of prescription sales, an independent pharmacy processes about 36,400 prescriptions a year and would have to pay SureScripts about $7,800.[40]

[38] *http://www.ada.org/ada/prod/survey/faq.asp*, accessed 1/16/2008.

[39] *http://www.nacds.org/wmspage.cfm?parm1=507*, accessed 1/18/2008.

[40] *http://www.nacds.org/wmspage.cfm?parm1=507*, accessed 1/18/2008.

Although these costs do not represent a significant economic impact, as discussed above, DEA considered options. The Base Case option would be less expensive initially, particularly for dentists and mid-level practitioners, because much less time would be needed for identity proofing. Once the identity proofing has occurred, however, the costs would be the same for the Base Case and Option 1. Option 2 would be less expensive for practitioners because the monthly log check would not be needed and the service provider costs would be lower because less stringent auditing requirements would be imposed. DEA has not proposed the Base Case because of two concerns about identity proofing. First, DEA is concerned that having a service provider employee checking the documents would make it easier for insider collusion to occur. Putting the in-person identity proofing in the hands of a DEA registrant or a public employee lessens that threat. Second, others expressed a concern that service providers would not visit practitioners' offices often, which could delay implementation and adoption, particularly for rural practices. DEA is not proposing the PKI option except for Federal health care agencies because of the concerns expressed by industry with regard to the use of digital signatures and the problems they would create for intermediaries. The third option, which would impose no costs on service providers, would be very expensive for pharmacies and practitioners. If the average independent pharmacy processes 36,400 prescriptions, about 11 percent of those are likely to be for controlled substances. Their annual cost for conducting callbacks on each of those would be about $5,200 in 2008; eliminating callbacks that already occur, the costs would be about $3,800 in 2008. If the number of controlled substance prescriptions (359 million original and newly authorized refills in 2008) were equally distributed among practitioners (about 573,000 in 2008), the average practitioner would incur costs of about $3,300 for callbacks under Option 3. Eliminating the callbacks that already occur, the average practitioner would incur new costs of about $2,200 under Option 3.

DEA has, therefore, determined that the proposed rule would not impose a significant economic impact on a substantial number of small entities directly subject to the rule. Less expensive options are considered too burdensome by the service providers and intermediaries. The option that would impose no burden on service providers would impose substantially higher costs on practitioners and pharmacies.

Another issue that DEA considered is whether the incremental costs might affect practitioners' decisions about purchasing a system that provides electronic prescribing. As discussed in previous sections of this preamble, the market for these systems has shifted away from stand-alone systems to EHRs. The cost of an EHR system for the functionalities that CCHIT requires ranges from $20,000 to $50,000 per practitioner with a usual annual maintenance charge of $6,000 per practitioner. (There are some less expensive systems marketed as EHRs that have only some of the functions; some appear to provide billing, scheduling, and simple records, but none of the more complex functions such as electronic prescribing, database links, etc.) Even in the first year, where the incremental cost of adding DEA's requirements would be between $150 and $200, this additional charge is unlikely to affect the decision to invest in an EHR, where the first year cost would be, at the low end $26,000 ($20,000 plus the $6,000 maintenance fee). The incremental costs would add less than 1 percent of the cost of the system; in the out-years, the incremental costs would similarly be a small fraction of the annual system maintenance cost. For stand-alone electronic prescription systems, the initial incremental costs will be higher because they are expected to need more programming. After the initial year, however, their incremental costs should be similar. These costs will represent a greater percentage increase in their monthly charges, which average $50 per month, but this is unlikely to affect the initial decision of whether to adopt electronic prescribing systems because most of these systems are being provided free to practitioners by insurers that want to encourage electronic prescribing.

DEA considers it unlikely that any service provider would attempt to market a product or service that could not be used for controlled substance records and, therefore, no service provider will be disadvantaged by complying because all service providers will incur costs and recover them from customers. The situation may be similar to certification of EHRs by CCHIT. Some were concerned that the standards would create barriers, but most of the companies certified have been small. The chairman of CCHIT, Mark Leavitt, stated that the data on the revenues of firms that gained certification ''laid to rest this concern that it was going to squeeze out small vendors. It actually seems to have done the opposite. It's created a level playing field.'' [41]

DEA notes that the barriers to adoption of electronic prescribing cited in various government studies relate to the high cost of the systems, the disruption caused by implementing these systems, and the relatively early stage of system development and interoperability provided by the existing systems. Despite the benefits of legible prescriptions, both in terms of patient safety and fewer callbacks from pharmacies, practitioners have resisted adoption of electronic prescriptions. Insurance companies that have offered the systems for free have had difficulty finding practitioners willing to accept them because while the service is free, the cost of additional hardware, training, and staff disruption is a barrier to adoption. In 2005, Wellpoint offered physicians $42 million in hardware, software, and support. ''Of the 25,000 physicians contacted, only 19,000 accepted these free gifts,'' Wellpoint then-CEO Leonard Schaeffer said. ''And of those 19,000, only 2,700 physicians chose e-prescribing PDAs. The rest selected a paperwork reduction package. * * * Free is not cheap enough,'' Schaeffer concluded.[42] The likelihood that the electronic prescribing systems will be part of EHR systems probably is also slowing adoption because practices do not want to invest in a stand-alone system that will be redundant later.

A study of physicians' experiences with commercial electronic prescription systems that was funded by HHS and published in Health Affairs on April 3, 2007, examined the implementation of electronic prescribing.[43] The study focused on larger medical practices (12 of the 21 practices had more than 50 doctors; none had fewer than 5), which meant that many of the practices had IT staff and support. Many of the problems encountered involved not the basic function of writing a prescription, but other functions that are designed to improve patient safety (e.g., medication histories, clinical decision support) and formulary compliance. Connectivity with pharmacies was also a problem.

[41] California HealthCare Foundation, ''Gauging the Progress of the National Health Information Technology Initiative: Perspectives from the Field.'' January 2008.

[42] Schaeffer, L. WellPoint Health Networks, Thousand Oaks, CA. Transforming an IT-Enabled Health Care System: The Health Plan Role. Presentation at the Second Annual National Health Information Summit. Washington DC, October 20, 2004. *http://www.managedcaremag.com/archives/0504/0504.pharmacy.html.*

[43] Grossman, Joy M. *et al.*, ''Physicians' Experiences Using Commercial E-Prescribing Systems,'' *Health Affairs*, 26, no. 3 (2007), w393–w404.

Practice estimates of the number of prescriptions printed out for the patient ranged from 10 percent to close to 100 percent. Despite the theoretical level of pharmacy readiness for electronic prescriptions, ''most practices using electronic fax or EDI [electronic data interchange] reported spending substantial time educating pharmacies about e-prescribing.'' Many practices noted that ''at least some of the mail-order PBMs [pharmacy benefit managers] routinely rejected prescriptions sent via electronic fax or EDI* * *''

Implementing a system was reported to be very complicated. One physician reported working with the IT department 4 hours a week for 6 months to iron out the ''kinks'' in the electronic prescribing module before the system could be tested. Maintenance of the system continued to demand staff resources. The study concluded:

> Much of the literature assessing barriers to electronic prescribing adoption and use has focused on cost, physician resistance, and changing practice workflow. Our findings highlight the role of product limitations, external implementation challenges, and physicians' preferences for how to use system features and are consistent with several other assessments of e-prescribing system functionality and provider pharmacy connectivity.
>
> Respondents' implementation hurdles belie the view that electronic prescribing products are relatively simple ''plug-and-play'' applications. It is hard to imagine that e-prescribing as it exists today can be the ''killer app'' that will drive further IT adoption. All of the practices we examined, regardless of size, IT expertise, geographic location, or vendor, had invested many financial and human resources in implementing and maintaining e-prescribing.

These findings are consistent with the CDC study cited above, which found that electronic prescribing was one of the less used functions in a fully or partially electronic EMR system.[44]

Creating an electronic prescription takes more time than writing a paper prescription and handing it to a patient. The electronic prescription system shifts some responsibility from the pharmacy to the practitioners. At present, it is the pharmacy that checks to see if a particular drug is covered by the patient's insurance and that checks for drug interactions by examining other medications the patient is taking. With electronic prescriptions, all of these checks may occur before the practitioner signs the prescription. While this process may significantly reduce processing time at the pharmacy and ensure that more prescribed drugs are on the insurance companies' formularies, it may substantially increase the time a practitioner must spend to create a prescription. Rather than spending a few seconds writing a prescription while talking to the patient, the practitioner has to move through a series of drop-down menus to select the patient, drug, dosage unit, and directions, then determine whether the insurance company will cover it and at what level of co-pay. Finally the practitioner will have to find the pharmacy from a drop-down menu. Electronic prescriptions are likely to save practices staff time in reduced callbacks, but the practitioners may initially see mainly the additional time that needs to be spent creating the prescription and the office disruption that occurs when staff need to be trained on new systems. (An earlier Rand study noted that although electronic prescriptions will eliminate errors caused by misread or misunderstood prescriptions, practitioners may not review the prescription to check that the right items from successive menus have been selected. Electronic prescriptions may introduce new errors through system design flaws. They may also reduce the likelihood that the pharmacy will check the prescription for errors.)[45]

DEA recognizes that the rule could potentially impose a burden on service providers, but the costs are not so great that a service provider would not be able to recover them from customers or that the incremental price increase would discourage customers from purchasing a system. The programming that may be needed to implement a conforming system is not so onerous that a service provider would find it a significant burden; designing and programming systems is what these companies do. The cost of the annual third-party audit may be burdensome, but without the audit there is no assurance that the system is protected against identity theft and insider attacks, two of the most likely sources of diversion. DEA expects that some service providers may drop out of the market if they cannot meet the security standards that an auditor would demand, but given other government requirements for security under HIPAA and the public's expectations for secure medical records, DEA believes that these providers would not be able to meet other standards and public expectations. The market for healthcare IT is evolving rapidly. As discussed above, DEA anticipates that most of the current providers will not be in this market by the time most practitioners have adopted EHR systems. Eventually, for reasons unrelated to DEA, a few systems will dominate the market; for these service providers, DEA's requirements will not be a burden.

Further information on small business costs is included in the *Initial Economic Impact Analysis of the Electronic Prescriptions for Controlled Substances Rule*.

Paperwork Reduction Act

The Department of Justice, Drug Enforcement Administration, has submitted the following information collection request to the Office of Management and Budget for review and clearance in accordance with review procedures of the Paperwork Reduction Act of 1995. The proposed information collection is published to obtain comments from the public and affected agencies.

All comments and suggestions, or questions regarding additional information, to include obtaining a copy of the proposed information collection instrument with instructions, should be directed to Mark W. Caverly, Chief, Liaison and Policy Section, Office of Diversion Control, Drug Enforcement Administration, 8701 Morrissette Drive, Springfield, VA 22152.

Written comments and suggestions from the public and affected agencies concerning the proposed collection of information are encouraged. Comments regarding the information collection-related aspects of this proposed rule should address one or more of the following four points:

(1) Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology,

[44] Centers for Disease Control and Prevention, ''Electronic Medical Record Use by Office-Based Physicians and Their Practices: United States 2006.'' *Advance Data from Vital and Health Statistics*, Number 393, October 26, 2007.

[45] Bell, D.S. *et al.*, ''Recommendations for Comparing Electronic Prescribing Systems: Results of An Expert Consensus Process,'' *Health Affairs*, May 25, 2004, W4–305–317.

e.g., permitting electronic submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection:* New collection.

(2) *Title of the Form/Collection:* Recordkeeping for electronic prescriptions for controlled substances.

(3) *Agency form number, if any, and the applicable component of the Department of Justice sponsoring the collection:*

Form number: None.

Office of Diversion Control, Drug Enforcement Administration, Department of Justice.

(4) Affected public who will be asked or required to respond, as well as a brief abstract:

Primary: Business or other for-profit.

Other: None.

Abstract: DEA would require that a DEA-registered hospital, State board, or law enforcement agency check a government-issued photographic identification. The practitioner would mail the signed document that the identification check has occurred to the service provider, which would be required to check the validity of a registrant's DEA registration and State license and retain a record of the check. The service provider would also be required to contact the practitioner by phone to verify the submission. DEA would require practitioners to review, on a monthly basis, a log of controlled substance prescriptions they have written and indicate that they have done so. The service provider would be required to retain a record that the log was reviewed and would be required to retain a digitally signed copy of the prescription as transmitted. Pharmacy systems would be required to digitally sign and archive the prescription as received. All service providers would be required to post a copy of the report of an annual third-party audit.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:*

Over the three years of this information collection request, DEA estimates that a maximum of 110 electronic prescription service providers, 20 pharmacy service providers, and 81,000 practitioners will comply with this proposed rule. The practitioners are estimated to spend 11 minutes for identity proofing, 2 minutes for mailing, and 24 minutes a year for log review. The entity conducting the in-person identity proofing would spend 10 minutes for identity proofing. Service providers would spend 13 minutes on identity proofing per practitioner. They will also spend 500 hours (for EHR and pharmacy ASP systems) or 2,000 hours (for stand-alone electronic prescription and installed pharmacy systems) in the first year programming the systems to meet the requirements. No costs are associated with digitally signing or retaining electronic records. These functions are handled by computers; service providers already retain prescription records as part of normal business practices.

(6) *An estimate of the total public burden (in hours) associated with the collection:* 211,000 hours over three years, an average of 70,200 hours per year.

If additional information is required contact: Lynn Bryant, Department Clearance Officer, Information Management and Security Staff, Justice Management Division, Department of Justice, Patrick Henry Building, Suite 1600, 601 D Street, NW., Washington, DC 20530.

Congressional Review Act

It has been determined that this rule is a major rule as defined by Section 804 of the Small Business Regulatory Enforcement Fairness Act of 1996 (Congressional Review Act). This rule is voluntary and could result in a net reduction in costs. This rule will not result in a major increase in costs or prices; or significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based companies to compete with foreign-based companies in domestic and export markets.

Executive Order 12988

This regulation meets the applicable standards set forth in Sections 3(a) and 3(b)(2) of Executive Order 12988 Civil Justice Reform.

Executive Order 13132

This rulemaking does not preempt or modify any provision of State law; nor does it impose enforcement responsibilities on any State; nor does it diminish the power of any State to enforce its own laws. Accordingly, this rulemaking does not have federalism implications warranting the application of Executive Order 13132.

Unfunded Mandates Reform Act of 1995

This rule will not result in the net expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $120,000,000 or more (adjusted for inflation) in any one year and will not significantly or uniquely affect small governments. Because this proposed rule will not affect other government, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995. The economic impact on private entities is analyzed in the *Draft Economic Impact Analysis of the Proposed Electronic Prescription Rule*. Cost savings will exceed direct costs.

List of Subjects

21 CFR Part 1300

Chemicals, Drug traffic control.

21 CFR Part 1304

Drug traffic control, Reporting and recordkeeping requirements.

21 CFR Part 1306

Drug traffic control, Prescription drugs.

21 CFR Part 1311

Administrative practice and procedure, Certification authorities, Controlled substances, Digital certificates, Drug traffic control, Electronic signatures, Prescription drugs, Reporting and recordkeeping requirements.

For the reasons set out above, 21 CFR parts 1300, 1304, 1306, and 1311 are proposed to be amended as follows:

PART 1300—DEFINITIONS

1. The authority citation for part 1300 continues to read as follows:

Authority: 21 U.S.C. 802, 871(b), 951, 958(f).

2. Section 1300.03 is added to read as follows:

§ 1300.03 Definitions relating to electronic orders for controlled substances and electronic prescriptions for controlled substances.

Audit means an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Trail means a record showing who has accessed an information technology system and what operations the user performed during a given period.

Authentication means verifying the identity of the user as a prerequisite to allowing access to the information system.

Authentication protocol means a well specified message exchange process that verifies possession of a token to remotely authenticate a prescriber.

Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both unique to the individual and measurable.

Cache means to download and store information on a local server or hard drive.

Certificate Policy means a named set of rules that sets forth the applicability of the specific digital certificate to a particular community or class of application with common security requirements.

Certificate Revocation List (CRL) means a list of revoked, but unexpired certificates issued by a Certification Authority.

Certification Authority (CA) means an organization that is responsible for verifying the identity of applicants, authorizing and issuing a digital certificate, maintaining a directory of public keys, and maintaining a Certificate Revocation List.

CSOS means controlled substance ordering system.

Digital certificate means a data record that, at a minimum—

(1) Identifies the certification authority issuing it;

(2) Names or otherwise identifies the certificate holder;

(3) Contains a public key that corresponds to a private key under the sole control of the certificate holder;

(4) Identifies the operational period; and

(5) Contains a serial number and is digitally signed by the Certification Authority issuing it.

Digital signature means a record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed.

Digitally sign means to affix a digital signature to a data file.

Electronic prescription means a prescription that is generated on an electronic system and transmitted as an electronic data file. An electronic prescription must comply with the requirements of parts 1306 and 1311 of this chapter. A prescription generated on an electronic system that is printed out or transmitted via facsimile to a pharmacy is not considered to be an electronic prescription and must be manually signed.

Electronic signature means a method of signing an electronic message that identifies a particular person as the source of the message and indicates the person's approval of the information contained in the message.

FIPS means Federal Information Processing Standards. These Federal standards, as incorporated by reference in § 1311.08 of this chapter, prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, etc.

FIPS 140–2, as incorporated by reference in § 1311.08 of this chapter, means a Federal standard for security requirements for cryptographic modules.

FIPS 180–2, as incorporated by reference in § 1311.08 of this chapter, means a Federal secure hash standard.

FIPS 186–2, as incorporated by reference in § 1311.08 of this chapter, means a Federal standard for applications used to generate and rely upon digital signatures.

Hard token means a cryptographic key stored on a special hardware device (e.g., a PDA, cell phone, smart card) rather than on a general purpose computer.

Identity Proofing means the process by which a service provider validates sufficient information to uniquely identify a person.

Intermediary means any technology system that receives and transmits an electronic prescription between the practitioner and pharmacy.

Key pair means two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key and (2) even knowing one key, it is computationally infeasible to discover the other key.

NIST means the National Institute of Standards and Technology.

NIST SP–800–63, as incorporated by reference in § 1311.08 of this chapter, means a Federal standard for electronic authentication.

Paper prescription means a prescription created on paper or computer generated to be printed or transmitted via facsimile that meets the requirements of part 1306 of this chapter including a manual signature.

PDA means a Personal Digital Assistant, a handheld computer used to manage contacts, appointments, and tasks.

Private key means the key of a key pair that is used to create a digital signature.

Public key means the key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair.

Public Key Infrastructure (PKI) means a structure under which a Certification Authority verifies the identity of applicants, issues, renews, and revokes digital certificates, maintains a registry of public keys, and maintains an up-to-date Certificate Revocation List.

SAS 70 Audit means a third-party audit of a technology provider that meets the American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) 70 criteria.

Service provider means a trusted entity that does one or more of the following:

(1) Issues or registers practitioner tokens and issues electronic credentials to practitioners.

(2) Provides the technology system (software or service) used to create and send electronic prescriptions.

(3) Provides the technology system (software or service) used to receive and process electronic prescriptions at a pharmacy.

SysTrust means a professional service performed by a qualified certified public accountant to evaluate one or more aspects of electronic systems.

Token means something a person possesses and controls (typically a key or password) used to authenticate the person's identity.

Valid prescription means a prescription that is issued for a legitimate medical purpose by an individual practitioner licensed by law to administer and prescribe the drugs concerned and acting in the usual course of the practitioner's professional practice.

WebTrust means a professional service performed by a qualified certified public accountant to evaluate one or more aspects of Web sites.

PART 1304—RECORDS AND REPORTS OF REGISTRANTS

3. The authority citation for part 1304 continues to read as follows:

Authority: 21 U.S.C. 821, 827, 871(b), 958(e), 965, unless otherwise noted.

4. Section 1304.04 is amended by revising paragraph (b) introductory text, paragraph (b)(1), and paragraph (h) to read as follows:

§ 1304.04 Maintenance of records and inventories.

* * * * *

(b) All registrants that are authorized to maintain a central recordkeeping system under paragraph (a) of this section shall be subject to the following conditions:

(1) The records to be maintained at the central record location shall not

include executed order forms and inventories, which shall be maintained at each registered location.

* * * * *

(h) Each registered pharmacy shall maintain the inventories and records of controlled substances as follows:

(1) Inventories and records of all controlled substances listed in Schedule II shall be maintained separately from all other records of the pharmacy.

(2) Paper prescriptions for Schedule II controlled substances shall be maintained at the registered location in a separate prescription file.

(3) Inventories and records of Schedules III, IV, and V controlled substances shall be maintained either separately from all other records of the pharmacy or in such form that the information required is readily retrievable from ordinary business records of the pharmacy.

(4) Paper prescriptions for Schedules III, IV, and V controlled substances shall be maintained at the registered location either in a separate prescription file for Schedules III, IV, and V controlled substances only or in such form that they are readily retrievable from the other prescription records of the pharmacy. Prescriptions will be deemed readily retrievable if, at the time they are initially filed, the face of the prescription is stamped in red ink in the lower right corner with the letter ''C'' no less than 1 inch high and filed either in the prescription file for controlled substances listed in Schedules I and II or in the usual consecutively numbered prescription file for noncontrolled substances. However, if a pharmacy employs a computer system for prescriptions that permits identification by prescription number and retrieval of original documents by prescriber's name, patient's name, drug dispensed, and date filled, then the requirement to mark the hard copy prescription with a red ''C'' is waived.

(5) Records of electronic prescriptions for controlled substances shall be maintained in a system that meets the requirements of Part 1311 of this chapter. The computers on which the records are maintained may be located at another location, but the records must be immediately accessible at the registered location if requested by the Administration or other law enforcement agent. The electronic system must be capable of printing out or transferring the records in a format that is readily understandable to an Administration or other law enforcement agent at the registered location. Electronic copies of prescription records must be sortable by prescriber name, patient name, drug dispensed, and date filled.

* * * * *

PART 1306—PRESCRIPTIONS

5. The authority citation for part 1306 continues to read as follows:

Authority: 21 U.S.C. 821, 829, 871(b), unless otherwise noted.

6. Section 1306.05 is revised to read as follows:

§ 1306.05 Manner of issuance of prescriptions.

(a) All prescriptions for controlled substances must be dated as of, and signed on, the day when issued and must bear the full name and address of the patient, the drug name, strength, dosage form, quantity prescribed, directions for use, and the name, address and registration number of the practitioner.

(b) A prescription for a Schedule III, IV, or V narcotic drug approved by FDA specifically for ''detoxification treatment'' or ''maintenance treatment'' must include the identification number issued by the Administrator under § 1301.28(d) of this chapter or a written notice stating that the practitioner is acting under the good faith exception of § 1301.28(e).

(c) Where a prescription is for gamma-hydroxybutyric acid, the practitioner shall note on the face of the prescription the medical need of the patient for the prescription.

(d) A practitioner may sign a paper prescription in the same manner as he would sign a check or legal document (e.g., J.H. Smith or John H. Smith). Where an oral order is not permitted, paper prescriptions must be written with ink or indelible pencil, typewriter, or printed on a computer printer and must be manually signed by the practitioner. A computer-generated prescription that is printed out or faxed must be manually signed.

(e) Electronic prescriptions must be created and signed using a system that meets the requirements of part 1311 of this chapter.

(f) A prescription may be prepared by the secretary or agent for the signature of a practitioner, but the prescribing practitioner is responsible in case the prescription does not conform in all essential respects to the law and regulations. A corresponding liability rests upon the pharmacist, including a pharmacist employed by a central fill pharmacy, who fills a prescription not prepared in the form prescribed by DEA regulations.

(g) An individual practitioner exempted from registration under § 1301.22(c) of this chapter must include on all prescriptions issued by him/her the registration number of the hospital or other institution and the special internal code number assigned to him/her by the hospital or other institution as provided in § 1301.22(c) of this chapter, in lieu of the registration number of the practitioner required by this section. Each paper prescription must have the name of the physician stamped, typed, or handprinted on it, as well as the signature of the physician.

(h) An official exempted from registration under § 1301.23(a) must include on all prescriptions issued by him/her his/her branch of service or agency (e.g., ''U.S. Army'' or ''Public Health Service'') and his/her service identification number, in lieu of the registration number of the practitioner required by this section. The service identification number for a Public Health Service employee is his/her Social Security identification number. Each paper prescription must have the name of the officer stamped, typed, or handprinted on it, as well as the signature of the officer.

7. Section 1306.08 is added to read as follows:

§ 1306.08 Electronic prescriptions.

(a) An individual practitioner may sign and transmit electronic prescriptions for controlled substances provided the practitioner meets all of the following requirements:

(1) The practitioner must comply with all other requirements for issuing controlled substance prescriptions in this part;

(2) The practitioner must use a system or service provider that meets the requirements of part 1311 of this chapter; and

(3) The practitioner must comply with the requirements for practitioners in part 1311 of this chapter.

(b) A pharmacy may fill an electronically transmitted prescription for a controlled substance provided the pharmacy complies with all other requirements for filling controlled substance prescriptions in this part and with the requirements of part 1311 of this chapter.

(c) To annotate an electronic prescription, a pharmacist must include all of the information required by this part for the record.

(d) If the content of any of the information required under § 1306.05 for a controlled substance prescription is altered during the transmission, the prescription is deemed to be invalid and the pharmacy may not dispense the controlled substance.

8. In § 1306.11, paragraphs (a), (c), (d)(1), and (d)(4) are revised to read as follows:

§ 1306.11 Requirement of prescription.

(a) A pharmacist may dispense directly a Schedule II controlled substance that is a prescription drug as determined under the Federal Food, Drug, and Cosmetic Act only pursuant to a written prescription signed by the practitioner, except as provided in paragraph (d) of this section. A paper prescription for a Schedule II controlled substance may be transmitted by the practitioner or the practitioner's agent to a pharmacy via facsimile equipment, provided that the original manually signed prescription is presented to the pharmacist for review prior to the actual dispensing of the controlled substance, except as noted in paragraph (e), (f), or (g) of this section. The original paper prescription must be maintained in accordance with § 1304.04(h) of this chapter.

* * * * *

(c) An institutional practitioner may administer or dispense directly (but not prescribe) a controlled substance listed in Schedule II only pursuant to a written prescription signed by the prescribing individual practitioner or to an order for medication made by an individual practitioner that is dispensed for immediate administration to the ultimate user.

(d) * * *

(1) The quantity prescribed and dispensed is limited to the amount adequate to treat the patient during the emergency period (dispensing beyond the emergency period must be pursuant to a paper or electronic prescription signed by the prescribing individual practitioner); * * *

(4) Within 7 days after authorizing an emergency oral prescription, the prescribing individual practitioner must cause a written prescription for the emergency quantity prescribed to be delivered to the dispensing pharmacist. In addition to conforming to the requirements of § 1306.05, the prescription must have written on its face ''Authorization for Emergency Dispensing,'' and the date of the oral order. The paper prescription may be delivered to the pharmacist in person or by mail, but if delivered by mail it must be postmarked within the 7-day period. Upon receipt, the dispensing pharmacist must attach this paper prescription to the oral emergency prescription that had earlier been reduced to writing. For electronic prescriptions, the pharmacist must annotate the record of the electronic prescription with the original authorization and date of the oral order. The pharmacist must notify the nearest office of the Administration if the prescribing individual practitioner fails to deliver a written prescription to him/her; failure of the pharmacist to do so shall void the authority conferred by this paragraph to dispense without a written prescription of a prescribing individual practitioner.

* * * * *

9. In § 1306.13, paragraph (a) is revised to read as follows:

§ 1306.13 Partial filling of prescriptions.

(a) The partial filling of a prescription for a controlled substance listed in Schedule II is permissible if the pharmacist is unable to supply the full quantity called for in a written or emergency oral prescription and he makes a notation of the quantity supplied on the face of the written prescription, written record of the emergency oral prescription, or in the electronic prescription record. The remaining portion of the prescription may be filled within 72 hours of the first partial filling; however, if the remaining portion is not or cannot be filled within the 72-hour period, the pharmacist must notify the prescribing individual practitioner. No further quantity may be supplied beyond 72 hours without a new prescription.

* * * * *

10. In § 1306.15, paragraph (a)(1) is revised to read as follows:

§ 1306.15 Provision of prescription information between retail pharmacies and central fill pharmacies for prescriptions of Schedule II controlled substances.

* * * * *

(a) * * *

(1) Write the word ''CENTRAL FILL'' on the face of the original paper prescription and record the name, address, and DEA registration number of the central fill pharmacy to which the prescription has been transmitted, the name of the retail pharmacy pharmacist transmitting the prescription, and the date of transmittal; for electronic prescriptions the name, address, and DEA registration number of the central fill pharmacy to which the prescription has been transmitted, the name of the retail pharmacy pharmacist transmitting the prescription, and the date of transmittal must be added to the electronic prescription record.

* * * * *

11. In § 1306.21, paragraphs (a) and (c) are revised to read as follows:

§ 1306.21 Requirement of prescriptions.

(a) A pharmacist may dispense directly a controlled substance listed in Schedule III, IV, or V that is a prescription drug as determined under the Federal Food, Drug, and Cosmetic Act, only pursuant to either a paper prescription signed by a practitioner, a facsimile of a signed paper prescription transmitted by the practitioner or the practitioner's agent to the pharmacy, an electronic prescription that meets the requirements of this part and part 1311 of this chapter, or an oral prescription made by an individual practitioner and promptly reduced to writing by the pharmacist containing all information required in § 1306.05, except for the signature of the practitioner.

* * * * *

(c) An institutional practitioner may administer or dispense directly (but not prescribe) a controlled substance listed in Schedule III, IV, or V only pursuant to a paper prescription signed by an individual practitioner, a facsimile of a paper prescription or order for medication transmitted by the practitioner or the practitioner's agent to the institutional practitioner-pharmacist, an electronic prescription that meets the requirements of this part and part 1311 of this chapter, or an oral prescription made by an individual practitioner and promptly reduced to writing by the pharmacist (containing all information required in § 1306.05 except for the signature of the individual practitioner), or pursuant to an order for medication made by an individual practitioner that is dispensed for immediate administration to the ultimate user, subject to § 1306.07.

12. Section 1306.22 is revised to read as follows:

§ 1306.22 Refilling of prescriptions.

(a) No prescription for a controlled substance listed in Schedule III or IV shall be filled or refilled more than six months after the date on which such prescription was issued. No prescription for a controlled substance listed in Schedule III or IV authorized to be refilled may be refilled more than five times.

(b) Each refilling of a prescription shall be entered on the back of the prescription or on another appropriate document or electronic prescription record. If entered on another document, such as a medication record, or electronic prescription record, the document or record must be uniformly maintained and readily retrievable.

(c) The following information must be retrievable by the prescription number:

(1) The name and dosage form of the controlled substance.

(2) The date filled or refilled.

(3) The quantity dispensed.

(4) The initials of the dispensing pharmacist for each refill.

(5) The total number of refills for that prescription.

(d) If the pharmacist merely initials and dates the back of the prescription or annotates the electronic prescription record, it shall be deemed that the full face amount of the prescription has been dispensed.

(e) The prescribing practitioner may authorize additional refills of Schedule III or IV controlled substances on the original prescription through an oral refill authorization transmitted to the pharmacist provided the following conditions are met:

(1) The total quantity authorized, including the amount of the original prescription, does not exceed five refills nor extend beyond six months from the date of issue of the original prescription.

(2) The pharmacist obtaining the oral authorization records on the reverse of the original paper prescription or annotates the electronic prescription record with the date, quantity of refill, number of additional refills authorized, and initials the paper prescription or annotates the electronic prescription record showing who received the authorization from the prescribing practitioner who issued the original prescription.

(3) The quantity of each additional refill authorized is equal to or less than the quantity authorized for the initial filling of the original prescription.

(4) The prescribing practitioner must execute a new and separate prescription for any additional quantities beyond the five refill, six-month limitation.

(f) As an alternative to the procedures provided by paragraphs (a) through (e) of this section, a computer system may be used for the storage and retrieval of refill information for original paper prescription orders for controlled substances in Schedule III and IV, subject to the following conditions:

(1) Any such proposed computerized system must provide online retrieval (via computer monitor or hard-copy printout) of original prescription order information for those prescription orders that are currently authorized for refilling. This shall include, but is not limited to, data such as the original prescription number, date of issuance of the original prescription order by the practitioner, full name and address of the patient, name, address, and DEA registration number of the practitioner, and the name, strength, dosage form, quantity of the controlled substance prescribed (and quantity dispensed if different from the quantity prescribed), and the total number of refills authorized by the prescribing practitioner.

(2) Any such proposed computerized system must also provide online retrieval (via computer monitor or hard-copy printout) of the current refill history for Schedule III or IV controlled substance prescription orders (those authorized for refill during the past six months.) This refill history shall include, but is not limited to, the name of the controlled substance, the date of refill, the quantity dispensed, the identification code, or name or initials of the dispensing pharmacist for each refill and the total number of refills dispensed to date for that prescription order.

(3) Documentation of the fact that the refill information entered into the computer each time a pharmacist refills an original paper, fax, or oral prescription order for a Schedule III or IV controlled substance is correct must be provided by the individual pharmacist who makes use of such a system. If such a system provides a hard-copy printout of each day's controlled substance prescription order refill data, that printout shall be verified, dated, and signed by the individual pharmacist who refilled such a prescription order. The individual pharmacist must verify that the data indicated are correct and then sign this document in the same manner as he would sign a check or legal document (*e.g.*, J. H. Smith, or John H. Smith). This document shall be maintained in a separate file at that pharmacy for a period of two years from the dispensing date. This printout of the day's controlled substance prescription order refill data must be provided to each pharmacy using such a computerized system within 72 hours of the date on which the refill was dispensed. It must be verified and signed by each pharmacist who is involved with such dispensing. In lieu of such a printout, the pharmacy shall maintain a bound log book, or separate file, in which each individual pharmacist involved in such dispensing shall sign a statement (in the manner previously described) each day, attesting to the fact that the refill information entered into the computer that day has been reviewed by him and is correct as shown. Such a book or file must be maintained at the pharmacy employing such a system for a period of two years after the date of dispensing the appropriately authorized refill.

(4) Any such computerized system shall have the capability of producing a printout of any refill data that the user pharmacy is responsible for maintaining under the Act and its implementing regulations. For example, this would include a refill-by-refill audit trail for any specified strength and dosage form of any controlled substance (by either brand or generic name or both). Such a printout must include name of the prescribing practitioner, name and address of the patient, quantity dispensed on each refill, date of dispensing for each refill, name or identification code of the dispensing pharmacist, and the number of the original prescription order. In any computerized system employed by a user pharmacy, the central recordkeeping location must be capable of sending the printout to the pharmacy within 48 hours, and if a DEA Special Agent or Diversion Investigator requests a copy of such printout from the user pharmacy, it must, if requested to do so by the Agent or Investigator, verify the printout transmittal capability of its system by documentation (e.g., postmark).

(5) In the event that a pharmacy which employs such a computerized system experiences system down-time, the pharmacy must have an auxiliary procedure which will be used for documentation of refills of Schedule III and IV controlled substance prescription orders. This auxiliary procedure must ensure that refills are authorized by the original prescription order, that the maximum number of refills has not been exceeded, and that all of the appropriate data are retained for online data entry as soon as the computer system is available for use again.

(g) When filing refill information for original paper, fax, or oral prescription orders for Schedule III or IV controlled substances, a pharmacy may use only one of the two systems described in paragraphs (a) through (e) or (f) of this section.

(h) When filing refill information for electronic prescriptions, a pharmacy must use a system that meets the requirements of part 1311 of this chapter.

13. Section 1306.25 is revised to read as follows:

§ 1306.25 Transfer between pharmacies of prescription information for Schedules III, IV, and V controlled substances for refill purposes.

(a) The transfer of original paper prescription information for a Schedule III, IV, or V controlled substance for the purpose of refill dispensing is permissible between pharmacies on a one-time basis only. However, pharmacies electronically sharing a real-time, online database may transfer up to the maximum refills permitted by law and the prescriber's authorization.

(b) Electronic prescriptions may be transferred up to the maximum refills

permitted by law and the prescriber's authorization.

(c) Transfers of paper prescriptions are subject to the following requirements:

(1) The transfer must be communicated directly between two licensed pharmacists.

(2) The transferring pharmacist must do the following:

(i) Write the word ''VOID'' on the face of the invalidated prescription.

(ii) Record on the reverse of the invalidated prescription the name, address, and DEA registration number of the pharmacy to which it was transferred and the name of the pharmacist receiving the prescription information.

(iii) Record the date of the transfer and the name of the pharmacist transferring the information.

(3) The pharmacist receiving the transferred paper prescription information must write the word ''transfer'' on the face of the transferred prescription and reduce to writing all information required to be on a prescription under § 1306.05 and include:

(i) Date of issuance of original prescription.

(ii) Original number of refills authorized on original prescription.

(iii) Date of original dispensing.

(iv) Number of valid refills remaining and date(s) and locations of previous refill(s).

(v) Pharmacy's name, address, DEA registration number, and prescription number from which the prescription information was transferred.

(vi) Name of pharmacist who transferred the prescription.

(vii) Pharmacy's name, address, DEA registration number, and prescription number from which the prescription was originally filled.

(d) For electronic prescriptions, the transferring pharmacist must do the following:

(1) Add information to the record of the original prescription that indicates the following:

(i) That the prescription has been transferred.

(ii) The name, address, and DEA registration number of the pharmacy to which it was transferred.

(iii) The date of the transfer and the name of the pharmacist transferring the information.

(2) Provide the receiving pharmacy with the following information in addition to the original electronic prescription data:

(i) The date of the original dispensing.

(ii) The number of refills remaining and the dates and location of previous refills.

(iii) The transferring pharmacy's name, address, DEA registration number, and prescription number.

(iv) The name of pharmacist transferring the prescription.

(v) The name, address, DEA registration number, and prescription number from the pharmacy that originally filled the prescription, if different.

(e) The pharmacist receiving a transferred electronic prescription must create an electronic record for the prescription that includes the receiving pharmacist's name and all of the information transferred with the prescription under paragraph (d)(2) of this section.

(f) A transferred electronic prescription may be transferred multiple times, as long as there are refills remaining and as long as the dispensing occurs within six months of the date of issue of the prescription.

(g) The original and transferred prescription(s) must be maintained for a period of two years from the date of last refill.

(h) Pharmacies electronically accessing the same prescription record must satisfy all information requirements of a manual mode for prescription transferal.

(i) The procedure allowing the transfer of prescription information for refill purposes is permissible only if allowable under existing State or other applicable law.

14. Section 1306.28 is added to read as follows:

§ 1306.28 Recordkeeping.

(a) All prescription records required by this part must be maintained as provided in § 1304.04(h) of this chapter.

(b) In addition to any other information required under this part, a pharmacy must retain the following information for each controlled substance prescription filled:

(1) Prescriber's name.

(2) Patient's name and address.

(3) The name and dosage form of the controlled substance.

(4) The quantity dispensed.

(5) The date filled.

(6) The written or typewritten name or initials of the dispensing pharmacist.

(7) The date refilled (Schedule III and IV only).

(8) The total number of refills for the prescription (Schedule III and IV only).

(9) In addition to the requirements of this paragraph, practitioners dispensing gamma-hydroxybutyric acid under a prescription must also comply with § 1304.26 of this chapter.

PART 1311—REQUIREMENTS FOR ELECTRONIC ORDERS AND PRESCRIPTIONS

15. The authority citation for part 1311 continues to read as follows:

Authority: 21 U.S.C. 821, 828, 829, 871(b), 958(e), 965, unless otherwise noted.

16. The heading for part 1311 is revised to read as set forth above.

17. Section 1311.01 is revised to read as follows:

§ 1311.01 Scope.

This part sets forth the rules governing the creation, transmission, and storage of electronic orders and prescriptions.

18. Section 1311.02 is revised to read as follows:

§ 1311.02 Definitions.

Any term contained in this part shall have the definition set forth in section 102 of the Controlled Substance Act (21 U.S.C. 802) or part 1300 of this chapter.

19. In § 1311.08, paragraph (a) is amended by adding paragraph (a)(4) to read as follows:

§ 1311.08 Incorporation by reference.

(a) * * *

(4) NIST SP 800–63, Electronic Authentication Guideline, April 2006.

* * * * *

20. Subpart C, consisting of §§ 1311.100 through 1311.180, is added to read as follows:

Subpart C—Electronic Prescriptions

Sec.

§ 1311.100 Eligibility to issue electronic prescriptions.

(a) A practitioner may issue a controlled substance prescription electronically if both of the following conditions are met:

(1) The practitioner is registered as an individual practitioner or exempt from registration under part 1301 of this chapter and is authorized under the registration or exemption to dispense the controlled substance.

(2) The practitioner uses an electronic prescription system that meets all of the applicable requirements of this subpart.

(b) An electronic prescription created and transmitted using an electronic prescription system that does not meet the requirements of this subpart is not a valid prescription.

(c) The practitioner issuing an electronic controlled substance prescription is responsible if a prescription does not conform in all essential respects to the law and regulations.

§ 1311.105 Electronic prescription system requirements: Identity proofing.

(a) Before permitting access to the electronic prescription system for signing controlled substance prescriptions, the service provider must receive a document prepared by an entity permitted to conduct in-person identity proofing listed in paragraph (b) of this section. If a practitioner wishes to electronically prescribe controlled substances in more than one State, the service provider must receive a document prepared by an entity permitted to conduct in-person identity proofing that indicates each of the State licenses and DEA Certificates of Registration. Such document shall be prepared either on the identity proofing entity's letterhead or other official form of correspondence, or the service provider may design a form for use by the identity proofing entity. Regardless of the format of the document, the document must contain all of the following information:

(1) The name and DEA registration number, where applicable, of the entity which conducted the in-person identity proofing of the practitioner;

(2) The name of the person within the entity who conducted the in-person identity proofing of the practitioner;

(3) The name and address of the principal place of business of the practitioner whose identity is being verified;

(4)(i) For each State in which the practitioner wishes to prescribe controlled substances electronically, the name of the State licensing authority and State license number of the practitioner whose identity is being verified, or

(ii) If the individual practitioner is an employee of a health care facility that is operated by the Department of Veterans Affairs, confirm that the individual practitioner has been duly appointed to practice at that facility by the Secretary of the Department of Veterans Affairs pursuant to 38 U.S.C. 7401–7408, or

(iii) If the individual practitioner is working at a health care facility operated by the Department of Veterans Affairs on a contractual basis pursuant to 38 U.S.C. 8153 and, in the performance of his duties, prescribes controlled substances, confirm that the individual practitioner meets the criteria for eligibility for appointment under 38 U.S.C. 7401–7408 and is prescribing controlled substances under the registration of such facility;

(5) Except as provided in paragraph (a)(6) of this section, for each State in which the practitioner wishes to prescribe controlled substances electronically, the DEA registration number and date of expiration of DEA registration of the practitioner whose identity is being verified;

(6) For individual practitioners who prescribe controlled substances using the DEA registration of the institutional practitioner, a statement by the institutional practitioner acknowledging the authority of the individual practitioner to prescribe controlled substances using the institution's DEA registration, and the specific internal code number assigned to the individual practitioner;

(7) The type of government-issued photographic identification checked (e.g., the practitioner's driver's license, passport) and a statement that the photograph on the identification matched the person presenting the photographic identification;

(8) The date on which the practitioner's in-person identity proofing was conducted;

(9) The signature of the person within the entity who conducted the in-person identity proofing;

(10) The signature of the practitioner who is the subject of the in-person identity proofing.

(b) The following entities are permitted to conduct in-person identity proofing as described in paragraph (a) of this section:

(1) The entity within a DEA-registered hospital that has previously granted that practitioner privileges at the hospital (e.g., a hospital credentialing office). The practitioner's privileges must be active and in good standing;

(2) The State professional or licensing board or State controlled substances authority that currently authorizes the practitioner to prescribe controlled substances;

(3) A State or local law enforcement agency.

(c) For each practitioner seeking to issue electronic controlled substances prescriptions, the service provider shall do the following:

(1) Check with each State to determine that the practitioner's State license to practice medicine is current and in good standing. If the individual practitioner is an employee of a health care facility that is operated by the Department of Veterans Affairs, the service provider shall confirm that the individual practitioner has been duly appointed to practice at that facility by the Secretary of the Department of Veterans Affairs pursuant to 38 U.S.C. 7401–7408. If the individual practitioner is working at a health care facility operated by the Department of Veterans Affairs on a contractual basis pursuant to 38 U.S.C. 8153 and, in the performance of his duties, prescribes controlled substances, the service provider shall confirm that the individual practitioner meets the criteria for eligibility for appointment under 38 U.S.C. 7401–7408 and is prescribing controlled substances under the registration of such facility.

(2) In those States in which a separate controlled substance registration is required to prescribe controlled substances, check with the appropriate State authority to determine that the practitioner's State license is current and in good standing.

(3) Except for individual practitioners referred to in paragraph (a)(6) of this section, check the DEA CSA database to determine that the DEA registration for each State is current and in good standing;

(4) Ensure that the service provider has an accurate list of the schedules the practitioner is authorized to prescribe;

(5) Contact the prescribing practitioner at the practitioner's registered location by telephone to confirm the practitioner's intent to apply to prescribe controlled substances using the service provider's system. The service provider must obtain the telephone number from a public source other than the application received from the practitioner. Alternatively, the service provider may confirm the practitioner's intent in person at the practitioner's registered location.

(d) The service provider must retain the document referred to in paragraph (a) of this section prepared by the entity that conducted the in-person identity proofing for each practitioner prescribing controlled substances electronically using the service provider's system in the manner specified in § 1311.180 of this part.

§ 1311.110 Electronic prescription system requirements: Authentication.

(a) The system must require that practitioners eligible to issue controlled substance prescriptions use two-factor authentication that meets the requirements of NIST SP 800–63 Level 4 authentication to access the system to sign and transmit controlled substances prescriptions.

(b) The hard token needed to meet NIST SP 800–63 Level 4 authentication must require the entry of a password or biometric to activate the authentication key and must not be able to export the authentication key. The hard token may be a PDA or other handheld device, smart card, thumb drive, etc. The token must be FIPS 140–2 validated as follows:

(1) Overall validation at Level 2 or higher.

(2) Physical security at Level 3 or higher.

(c) The system must require reauthentication if the practitioner does not use the system for more than 2 minutes.

(d) The system must provide a separate authentication protocol for separate DEA registrations. At a minimum, a practitioner must have a separate authentication protocol for each State in which the practitioner holds a DEA registration to dispense controlled substances. The practitioner may store multiple authentication protocols on a single hard token.

(e) The system access authentication protocol must expire no later than the expiration date of the practitioner's DEA registration with which it is associated.

§ 1311.115 Electronic prescription system requirements: Prescription contents.

(a) An electronic prescription for a controlled substance created by the system must include all of the data elements required under paragraph (b) of this section and part 1306 of this chapter.

(b) An electronic prescription for a controlled substance must include all of the following information:

(1) The full name and address of the issuing practitioner.

(2) The DEA registration number of the issuing practitioner. For practitioners issuing prescriptions under a hospital or clinic registration number, the prescription must include the registration number and registrant-assigned extension identifier. For military or Public Health Service practitioners exempt from registration, the prescription must include the practitioner's service identification number or Social Security number as required in § 1306.05(h) of this chapter.

(3) The full name and address of the patient for whom the prescription is written.

(4) The drug name, strength, dosage form, quantity prescribed, and directions for use.

(5) The time and date that the prescription was signed.

(c) An electronic prescription for a controlled substance must have the practitioner name, address, and DEA registration number for only the practitioner issuing the prescription. Multiple DEA registration numbers may not be associated with a prescription.

§ 1311.120 Electronic prescription system requirements: Creating a controlled substance prescription.

(a) The system may allow the registrant or his agent to enter data for a controlled substance prescription.

(b) After the practitioner or his agent has entered the prescription information into the system, the system must display the following information related to the controlled substance prescription:

(1) The patient's name and address.

(2) The name of the drug being prescribed;

(3) The dosage strength and form, quantity, and directions for use.

(4) The DEA registration number under which the prescription will be authorized.

(c) Where more than one controlled substance prescription has been prepared, the practitioner must positively indicate those prescriptions that are to be signed. Any prescription not indicated to be signed shall not be transmitted.

§ 1311.125 Electronic prescription system requirements: Signing the prescription.

(a) The practitioner must authenticate himself to the system using two-factor authentication immediately before signing the prescription. The system may allow a practitioner to sign multiple prescriptions at the same time.

(b) After a practitioner has authenticated to the system but prior to signing the controlled substance prescription, the system must display for the practitioner's review the information required by § 1311.120(b) for all prescriptions that are to be transmitted in connection with that signature. While such information is displayed, the practitioner must be presented with the following statement (or its substantial equivalent): ''I, the prescribing practitioner whose name and DEA registration number appear on the controlled substance prescription(s) being transmitted, have reviewed all of the prescription information listed above and have confirmed that the information for each prescription is accurate. I further declare that by transmitting the prescription(s) information, I am indicating my intent to sign and legally authorize the prescription(s).'' The practitioner must positively indicate agreement with this statement. If the practitioner does not indicate agreement to this statement, the controlled substances prescriptions shall not be transmitted.

(c) The service provider must ensure that its prescription-writing system permits practitioners to sign controlled substance prescriptions only if they have the appropriate State authorization and DEA registration to prescribe the schedule of controlled substances being prescribed.

(d) The system must require that the DEA registrant whose DEA number is listed on the prescription sign the prescription. The system must not allow any other person to sign the prescription.

(e) The signing function may take different names depending on the system and the terms used. Regardless of the system labels, signing is the practitioner's attestation that the prescription is accurate and being issued by the practitioner for a legitimate medical purpose in the usual course of professional practice.

(f) The system must include in the data file transmitted an indication that the prescription was signed by the issuing practitioner.

§ 1311.130 Electronic prescription system requirements: Transmission of electronic prescriptions.

(a) The electronic prescription system must transmit the electronic prescription immediately upon signature by the practitioner.

(b) The electronic prescription system must not allow the printing of an electronic prescription that has been transmitted.

(c) The electronic prescription system must not allow the transmission of an electronic prescription if the prescription has been printed.

(d) The service provider must ensure that the service provider or the first processor of the signed prescription digitally signs a copy of the prescription

as received and archives the digitally signed prescription.

(e) The system must retain the archived digitally signed prescription for five years from the date of issuance by the practitioner.

(f) The contents of the prescription listed in § 1311.115(b) must not be altered during transmission. Any change to the content during transmission will render the prescription invalid. The data may be reformatted.

(g) An electronic prescription must be transmitted from the practitioner to the pharmacy in its electronic form. At no time may an electronic prescription be converted to another form for transmission.

§ 1311.135 Electronic prescription system requirements: Revocation of access authorization.

(a) The service provider must revoke the authentication protocol used to sign controlled substance prescriptions immediately upon receiving notification from the practitioner that a password or token has been compromised, lost, or stolen.

(b) The service provider must revoke the authentication protocol used to sign controlled substance prescriptions on the expiration date of the practitioner's DEA registration unless the service provider determines that the registration has been renewed.

(c) The service provider must check the DEA CSA database at least once a week and revoke the authentication protocol used to sign controlled substance prescriptions for each practitioner using the system whose registration has been terminated, revoked, or suspended.

§ 1311.140 Electronic prescription system requirements: Providing log of prescriptions to practitioner.

(a) The electronic prescription system must, on a monthly basis, automatically provide the practitioner with an electronic log (which is readily viewable by the practitioner using the system) of all electronic prescriptions for controlled substances that were issued by the practitioner during the previous month using that system.

(b) The electronic prescription system must provide a means for the practitioner to indicate that he has received and reviewed the log.

(c) The electronic prescription system must retain the log provided to the practitioner and a record of the practitioner's indication of the log review for five years.

(d) The electronic prescription system must make available, on the request of the practitioner, a log of all controlled substance prescriptions that the practitioner has transmitted for the previous five years.

§ 1311.145 Electronic prescription system requirements: Security incidents.

(a) The service provider must audit its records and system at least once a day in a manner sufficient to meet the requirements of paragraph (b) of this section.

(b) The service provider must notify the Administration within one business day of any security incidents that indicate that any of the following may have occurred:

(1) An individual who is not a DEA registrant has been granted access to issue controlled substance prescriptions.

(2) An individual has been granted access to issue controlled substance prescriptions without identity proofing that meets the requirements of § 1311.105 of this part.

(3) Access to issue controlled substance prescriptions has been granted to a person using another person's identity.

(4) Prescription records have been created or altered by a service provider employee.

(5) There have been one or more successful attempts to penetrate the service provider's system from the outside.

(6) The service provider has identified any other incident that may indicate that the integrity of the system in regard to controlled substance prescriptions has been compromised.

§ 1311.150 Electronic prescription system requirements: Third-party audits of service provider systems.

(a) The service provider must have a qualified third party conduct an audit that meets the requirements of a WebTrust or SysTrust audit for system security and processing integrity prior to accepting any controlled substances prescriptions for transmission and annually thereafter.

(b) The audit must determine whether the electronic prescription system and the service provider meet the requirements of this part.

(c) The service provider must make the audit report available to any practitioner who uses the system or is considering use of the system. The service provider must retain each annual audit report for the last five years.

(d) If the third-party audit finds that the system does not meet one or more of the requirements of this part or does not provide adequate security against insider and outsider threats, the service provider must not accept for transmission any controlled substance prescription. The service provider must notify practitioners that they should not use the system to generate and transmit controlled substance prescriptions. The service provider must also notify the Administration of the adverse audit report and provide the report to the Administration.

(e) For service providers that install the prescription-writing system on a practitioner's computers and that are not involved in the subsequent transmission of the prescription, the service provider must notify its DEA registrant customers of the results of any third-party audit that finds that the system does not meet one or more of the requirements of this part. The service provider must also notify the Administration of the adverse audit report and provide the report to the Administration.

§ 1311.155 Practitioner responsibilities.

(a) The practitioner shall provide, or cause to be provided, to the service provider a document from an entity permitted to conduct in-person identity proofing that meets the requirements of § 1311.105 of this part.

(b) The practitioner must retain sole possession of the hard token and must not share the password with any other person. The practitioner must not allow any other person to use the token or enter the password or other identification means to sign prescriptions for controlled substances. Failure by the practitioner to secure the hard token or password may provide a basis for revocation or suspension of registration pursuant to section 304(a)(4) of the Act (21 U.S.C. 824(a)(4)).

(c) The practitioner must notify the service provider within 12 hours of discovery that the hard token has been lost, stolen, or compromised. A practitioner who fails to notify the service provider of the loss, theft, or compromise of the hard token will be held responsible for any controlled substance prescriptions written using the hard token.

(d) The practitioner must review the monthly log to determine whether the prescriptions issued under his DEA registration number were, in fact, issued by him and whether any prescriptions appear to be unusual based on the practitioner's known prescribing pattern. The practitioner must indicate on the log that he has reviewed it. Practitioners are not required to check the log against patient records.

(e) The practitioner must notify both the service provider and the Administration within 12 hours of

discovery that one or more prescriptions that were issued under his DEA registration were prescriptions he had not signed or were not consistent with the prescription he signed.

(f) The practitioner must determine initially and at least annually thereafter that the third-party audit report of the service provider indicates that the system and service provider meet the requirements of this part. If the third-party audit report indicates that the system or the service provider does not meet the requirements of this part, or the service provider notifies the practitioner that the system does not meet the requirements of this part, the practitioner must immediately cease to issue electronic controlled substance prescriptions using the system.

(g) The practitioner has the same responsibilities when issuing prescriptions for controlled substances via electronic means as when issuing a paper or oral prescription. Nothing in this part relieves a practitioner of his responsibility to dispense controlled substances only for a legitimate medical purpose while acting in the usual course of his professional practice. If an agent enters information at the practitioner's direction prior to the practitioner reviewing and approving the information and signing and authorizing the transmission of that information, the practitioner is responsible in case the prescription does not conform in all essential respects to the law and regulations.

§ 1311.160 Pharmacy system requirements: Archiving the initial record.

(a) A copy of each electronic controlled substance prescription record that a pharmacy receives must be digitally signed by one of the following:

(1) The last intermediary transmitting the record to the pharmacy immediately prior to transmission to the pharmacy.

(2) The first pharmacy system that receives the electronic prescription immediately on receipt.

(b) If the last intermediary digitally signs the record, it must forward the digitally signed copy to the pharmacy.

(c) The pharmacy system must archive and retain the digitally signed prescription as received for five years from the date of receipt.

§ 1311.165 Pharmacy system requirements: Prescription processing.

(a) The pharmacy system must verify that the practitioner's DEA registration was valid at the time the prescription was signed. The pharmacy system may do this by checking the DEA CSA database or by having the prescribing practitioner's service provider or one of the intermediaries check the DEA CSA database during transmission and indicate on the record that the check has occurred and the registration is valid. The CSA database may be cached for one week from the date of issuance.

(b) The pharmacy system must verify that the practitioner signed the prescription by checking the data field that indicates the prescription was signed.

(c) The pharmacy system must reject any of the following controlled substance prescriptions:

(1) A prescription that was not signed.

(2) A prescription that was signed by a practitioner without a valid DEA registration.

(3) A prescription that does not include all of the information required under § 1306.05 of this chapter.

(d) The pharmacy system must be capable of reading and retaining the full DEA registration number, including any extensions, or other identification numbers used under § 1306.05(c) of this chapter. The full number including extensions must be retained in the prescription record.

(e) The pharmacy system must provide for the following information to be added or linked to each controlled substance prescription record for each dispensing, as required in §§ 1304.22(c) and 1306.22 of this chapter:

(1) The number of units or volume of the controlled substance dispensed.

(2) The date of the dispensing.

(3) The full name of the person who dispensed the prescription.

(4) The number of refills allowed.

(f) The pharmacy system must be capable of retrieving information on controlled substance prescriptions by the following data:

(1) Prescriber name.

(2) Patient name.

(3) Drug dispensed.

(4) Date dispensed.

(g) The pharmacy prescription system must be capable of downloading an electronic copy of controlled substance prescription records into a database or spreadsheet format that is readily readable and can be easily sorted by the data elements listed in paragraph (f) of this section. Such database or spreadsheet must be able to be printed or provided electronically without the need for additional specialized software.

§ 1311.170 Pharmacy system requirements: Security.

(a) The pharmacy system must create and maintain a backup copy of all controlled substance prescriptions at an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards. A copy of each digitally signed controlled substance prescription and all linked dispensing records must be transferred to the backup storage site at least once every 24 hours. Backup copies must be maintained for five years from the date of the record creation.

(b) The pharmacy system must create and maintain an internal audit trail that indicates each time a controlled substance prescription file is opened, annotated, altered, or deleted and the identity of the person taking the action. The audit trail records must be maintained for five years.

(c) The pharmacy or the service provider must establish and implement a list of auditable events. The auditable events must, at a minimum, include attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in the prescription system.

(d) The system must analyze the audit logs at least once every 24 hours and generate an incident report that identifies each auditable event.

(e) The pharmacy must determine whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescription records. Any such incidents must be reported to the service provider and the Administration within one business day.

(f) The pharmacy system must have a qualified third party conduct an audit that meets the requirements of a SysTrust or SAS 70 audit for system security and processing integrity prior to accepting any controlled substances prescriptions for processing and annually thereafter.

(g) The third-party audit must determine whether the system for processing controlled substance prescriptions and the service provider meet the requirements of this part. The service provider must make the audit report available to any pharmacy who uses the system. The service provider must retain each annual audit report for the last five years.

(h) If the third-party audit finds that the system does not meet one or more of the requirements of this part or does not provide adequate security against insider and outsider threats, the system must not accept or process any electronic controlled substance prescription. The service provider must notify pharmacies that they should not use the system to accept and process controlled substance prescriptions. The service provider must also notify the Administration of the adverse audit

report and provide the report to the Administration.

(i) For service providers that install the prescription-processing system on a pharmacy's computers and that are not involved in the subsequent acceptance and processing of the prescription, the service provider must notify its DEA registrant customers of the results of any third-party audit that finds that the system does not meet one or more of the requirements of this part. The service provider must also notify the Administration of the adverse audit report and provide the report to the Administration.

§ 1311.175 Pharmacy responsibilities.

(a) A pharmacy must not dispense controlled substances in response to electronic controlled substance prescriptions if its pharmacy system or service provider does not meet the requirements of this part.

(b) A pharmacy must not process electronic controlled substance prescriptions if the DEA registration of the prescriber was not valid at the time the prescription was signed or if the system rejected the prescription for any other reason.

(c) When a pharmacist fills a prescription in a manner that would require, under part 1306 of this chapter, the pharmacist to make a notation on the prescription if the prescription were a paper prescription, the pharmacist must make such notation electronically when filling an electronic prescription.

(d) Nothing in this part relieves a pharmacy of its responsibility to dispense controlled substances only pursuant to a prescription issued for a legitimate medical purpose by a practitioner acting in the usual course of professional practice.

§ 1311.180 Recordkeeping.

(a) A practitioner, pharmacy, or service provider must maintain records required by this part for electronic prescriptions for five years from their creation. Records may be maintained electronically. Records regarding controlled substances prescriptions that are maintained electronically must be readily retrievable from all other records.

(b) This record retention requirement shall not pre-empt any longer period of retention which may be required now or in the future, by any other Federal or State law or regulation, applicable to practitioners, pharmacists, or pharmacies.

(c) Electronic records must be easily readable or easily rendered into a format that a person can read. They must be made available to the Administration upon request.

21. Subpart D, consisting of §§ 1311.200 through 1311.280, is added to read as follows:

Subpart D—Electronic Prescriptions for Federal Agencies

Sec.

§ 1311.200 Eligibility to digitally sign electronic prescriptions.

(a) As an optional alternative to issuing electronic prescriptions for controlled substances under the conditions set forth in Subpart C of this part, a practitioner prescribing controlled substances at a Federal health care facility in the course of their official duties may issue a controlled substance prescription electronically under the conditions set forth in this subpart if both of the following conditions are met:

(1) The practitioner is registered as an individual practitioner or exempt from registration under part 1301 of this chapter and is authorized under the registration or exemption to dispense the controlled substance.

(2) The practitioner uses an electronic prescription system that meets all of the applicable requirements of this subpart.

(b) For purposes of this section, the term ''Federal health care facility'' means a hospital or other institution that is operated by an agency of the United States (including the U.S. Army, Navy, Marine Corps, Air Force, Coast Guard, Department of Veterans Affairs, Public Health Service, or Bureau of Prisons).

(c) An electronic prescription created and transmitted using an electronic prescription system that does not meet the requirements of this subpart is not a valid prescription.

(d) The practitioner issuing an electronic controlled substance prescription is responsible if a prescription does not conform in all essential respects to the law and regulations.

§ 1311.205 Issuance and storage of digital certificates.

(a) Only Federal Certification Authorities or Certification Authorities cross-certified with a Certification Authority operated by the Federal Public Key Infrastructure Policy Authority may issue digital certificates to practitioners prescribing controlled substances at a Federal health care facility in the course of their official duties to sign electronic controlled substance prescriptions.

(b) The digital certificate must be stored on a hardware token that meets the requirements of NIST SP 800–63 Level 4.

§ 1311.210 Digitally signed prescription system requirements: Prescription-writing system requirements.

(a) Any system may be used to digitally sign electronic prescriptions for controlled substances provided that the system has been enabled to accept digitally signed documents and that it meets the following requirements:

(1) The cryptographic module must be FIPS 140–2 level 1 validated.

(2) The digital signature system and hash function must comply with FIPS 186–2 and FIPS 180–1.

(3) The private key must be stored encrypted on a FIPS 140–2 level 1 validated cryptographic module using a FIPS-approved encryption algorithm.

(4) For software implementations, when the signing module is deactivated, the system must clear the plain text password from the system memory to prevent the unauthorized access to, or use of, the private key.

(5) The system must have a time system that is within five minutes of the official National Institute of Standards and Technology time source.

(b) The system must require that practitioners eligible to issue controlled substance prescriptions use two-factor authentication that meets the requirements of NIST SP 800–63 Level

4 authentication to access the system to sign and transmit controlled substances prescriptions.

(c) The hard token needed to meet NIST SP 800–63 Level 4 authentication must require the entry of a password or biometric to activate the authentication key and must not be able to export the authentication key. The token must be FIPS 140–2 validated as follows:

(1) Overall validation at Level 2 or higher.

(2) Physical security at Level 3 or higher.

(d) The system must require reauthentication if the practitioner does not use the system for more than 2 minutes.

§ 1311.215 Digitally signed prescription system requirements: Prescription contents.

A digitally signed electronic prescription for a controlled substance created by the system must include all of the data elements required under part 1306 of this chapter.

§ 1311.220 Digitally signed prescription system requirements: Creating a controlled substance prescription.

(a) The system may allow the registrant or his agent to enter data for a controlled substance prescription.

(b) After the practitioner or his agent has entered the prescription information into the system, the system must display the following information related to the controlled substance prescription:

(1) The patient's name and address;

(2) The name of the drug being prescribed;

(3) The dosage strength and form, quantity, and directions for use;

(4) The DEA registration number under which the prescription will be authorized.

(c) Where more than one controlled substance prescription has been prepared, the practitioner must positively indicate those prescriptions that are to be signed. Any prescription not indicated to be signed shall not be transmitted.

§ 1311.225 Digitally signed prescription system requirements: Signing the prescription.

(a) The practitioner must authenticate himself to the system using two-factor authentication immediately before signing the prescription. The system may allow a practitioner to sign multiple prescriptions at the same time.

(b) After a practitioner has authenticated to the system but prior to signing the controlled substance prescription, the system must display for the practitioner's review the information required by § 1311.220(b) for all prescriptions that are to be transmitted in connection with that signature. While such information is displayed, the practitioner must be presented with the following statement (or its substantial equivalent): ''I, the prescribing practitioner whose name and DEA registration number appear on the controlled substance prescription(s) being transmitted, have reviewed all of the prescription information listed above and have confirmed that the information for each prescription is accurate. I further declare that by transmitting the prescription(s) information, I am indicating my intent to sign and legally authorize the prescription(s).'' The practitioner must positively indicate agreement with this statement. If the practitioner does not indicate agreement to this statement, the controlled substances prescriptions shall not be transmitted.

(c) The Federal agency must ensure that its prescription-writing system permits practitioners to digitally sign controlled substance prescriptions only if they have the appropriate authorization to prescribe the schedule of controlled substances being prescribed.

(d) The system must require that the DEA registrant whose DEA number is listed on the prescription digitally sign the prescription. The system must not allow any other person to sign the prescription.

(e) The system must check the certificate revocation list of the Certification Authority that issued the digital certificate of the practitioner who digitally signed the controlled substance prescription. If the certificate is not valid, the system must not transmit the prescription. The certificate revocation list may be cached until the Certification Authority issues a new certificate revocation list.

(f) If the prescription is being transmitted to a pharmacy that does not accept digitally signed prescriptions, the system must include in the data file transmitted an indication that the prescription was signed by the issuing practitioner.

§ 1311.230 Digitally signed prescription system requirements: Transmission of electronic prescriptions.

(a) The electronic prescription system must not allow the printing of an electronic prescription that has been transmitted.

(b) The electronic prescription system must not allow the transmission of an electronic prescription if the prescription has been printed.

(c) The system must retain the archived digitally signed prescription for five years from the date of issuance by the practitioner.

(d) The data elements required under part 1306 of this chapter must not be altered during transmission. Any change to the content during transmission will render the prescription invalid. The data may be reformatted.

(e) An electronic prescription must be transmitted from the practitioner to the pharmacy in its electronic form. At no time may an electronic prescription be converted to another form for transmission.

§ 1311.235 Digitally signed prescription system requirements: Revocation of access authorization.

(a) The system must revoke access to sign controlled substance prescriptions on the expiration date of the practitioner's DEA registration, if applicable, unless the Federal agency determines that the registration or Federal agency authorization has been renewed.

(b) The system must check the DEA CSA database at least once a week and revoke access to signing controlled substance prescriptions for any practitioner using the system whose registration or Federal agency authorization has been terminated, revoked, or suspended.

§ 1311.245 Digitally signed prescription system requirements: Security incidents.

(a) The Federal agency must audit its controlled substance prescription electronic records and system at least once a day in a manner sufficient to meet the requirements of paragraph (b) of this section.

(b) The Federal agency must notify the Administration within one business day of any security incidents that indicate that any of the following may have occurred:

(1) An individual who is not a DEA registrant authorized by the Federal agency to prescribe controlled substances in the course of their official duties at the Federal agency has been granted access to issue controlled substance prescriptions.

(2) Access to issue controlled substance prescriptions has been granted to a person using another person's identity.

(3) Prescription records have been created or altered by an employee not authorized to create or annotate a controlled substance record.

(4) There have been one or more successful attempts to penetrate the system from the outside.

(5) The Federal agency has identified any other incident that may indicate that the integrity of the system in regard

to controlled substance prescriptions has been compromised.

§ 1311.250 Digitally signed prescription system requirements: Third-party audits of systems.

(a) The Federal agency must have a third-party audit to verify that the system used to create and transmit controlled substance prescriptions meets the requirements of this subpart prior to accepting any controlled substances prescriptions for transmission and annually thereafter.

(b) The Federal agency must retain each annual audit report for the last five years.

(c) If the third-party audit finds that the system does not meet one or more of the requirements of this part, the system must not accept for transmission any controlled substance prescription. The Federal agency must also notify the Administration of the adverse audit report and provide the report to the Administration.

§ 1311.255 Practitioner responsibilities.

(a) The practitioner must retain sole possession of the hard token and must not share the password with any other person. The practitioner must not allow any other person to use the token or enter the password or other identification means to sign prescriptions for controlled substances. Failure by the practitioner to secure the hard token or password may provide a basis for revocation or suspension of registration pursuant to section 304(a)(4) of the Act (21 U.S.C. 824(a)(4)).

(b) The practitioner must notify the Certification Authority within 12 hours of discovery that the hard token has been lost, stolen, or compromised. A practitioner who fails to notify the Certification Authority of the loss, theft, or compromise of the hard token will be held responsible for any controlled substance prescriptions written using the hard token.

(c) The practitioner has the same responsibilities when issuing prescriptions for controlled substances via electronic means as when issuing a paper or oral prescription. Nothing in this part relieves a practitioner of his responsibility to dispense controlled substances only for a legitimate medical purpose while acting in the usual course of his professional practice. If an agent enters information at the practitioner's direction prior to the practitioner reviewing and approving the information and signing and authorizing the transmission of that information, the practitioner is responsible in case the prescription does not conform in all essential respects to the law and regulations.

§ 1311.260 Pharmacy system requirements: Archiving the initial record.

(a) If a pharmacy receives a controlled substance prescription from a Federal agency system that is not transmitted with its digital signature, either the pharmacy must digitally sign the prescription immediately upon receipt, or the last intermediary transmitting the record to the pharmacy must digitally sign the prescription immediately prior to transmission and transmit to the pharmacy the prescription and the digitally signed record. The pharmacy must archive the record as received and the digitally signed copy.

(b) If a Federal pharmacy receives a digitally signed prescription that includes the digital signature, the pharmacy must validate the prescription and archive the digitally signed record. The pharmacy record must retain an indication that the prescription was validated upon receipt. No additional digital signature is required.

(c) The pharmacy system must retain the digitally signed prescription as received for five years from the date of receipt.

§ 1311.265 Pharmacy system requirements: Prescription processing.

(a) The pharmacy system must verify that the practitioner's DEA registration was valid at the time the prescription was signed. The pharmacy system may do this by checking the DEA CSA database or by having the prescribing practitioner's system or one of the intermediaries check the DEA CSA database during transmission and indicate on the record that the check has occurred and the registration is valid. The CSA database may be cached for one week from the date of issuance.

(b) If the digital signature is not part of the record, the pharmacy system must verify that the practitioner signed the prescription by checking the data field that indicates the prescription was signed.

(c) The pharmacy system must reject any of the following controlled substance prescriptions:

(1) A prescription that was signed by a practitioner without a valid DEA registration.

(2) A prescription that does not include all of the information required under § 1306.05 of this chapter.

(3) If the digital signature is received, a prescription that is not validated.

(d) The pharmacy system must be capable of reading and retaining the full DEA registration number, including any extensions, or other identification numbers used under § 1306.05(c) of this chapter. The full number including extensions must be retained in the prescription record.

(e) The pharmacy system must provide for the following information to be added or linked to each controlled substance prescription record for each dispensing, as required in §§ 1304.22(c) and 1306.22 of this chapter:

(1) The number of units or volume of the controlled substance dispensed.

(2) The date of the dispensing.

(3) The full name of the person who dispensed the prescription.

(4) The number of refills allowed.

(f) The pharmacy system must be capable of retrieving information on controlled substance prescriptions by the following data:

(1) Prescriber name.

(2) Patient name.

(3) Drug dispensed.

(4) Date dispensed.

(g) The pharmacy prescription system must be capable of downloading an electronic copy of controlled substance prescription records into a database or spreadsheet format that is readily readable and can be easily sorted by the data elements listed in paragraph (f) of this section. Such database or spreadsheet must be able to be printed or provided electronically without the need for additional specialized software.

§ 1311.270 Pharmacy system requirements: Security.

(a) The pharmacy system must create and maintain a backup copy of all controlled substance prescriptions at an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards. A copy of each digitally signed controlled substance prescription and all linked dispensing records must be transferred to the backup storage site at least once every 24 hours. Backup copies must be maintained for five years from the date of the record creation.

(b) The pharmacy system must create and maintain an internal audit trail that indicates each time a controlled substance prescription file is opened, annotated, altered, or deleted and the identity of the person taking the action. The audit trail records must be maintained for five years.

(c) The pharmacy must establish and implement a list of auditable events. The auditable events must, at a minimum, include attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in the prescription system.

(d) The system must analyze the audit logs at least once every 24 hours and generate an incident report that identifies each auditable event.

(e) The pharmacy must determine whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescription records. Any such incidents must be reported to the Federal agency and the Administration within one business day.

(f) The Federal agency must have a qualified third party conduct an audit for processing integrity prior to accepting any controlled substances prescriptions for processing and annually thereafter.

(g) The third-party audit must determine whether the system for processing controlled substance prescriptions meets the requirements of this part. The Federal agency must retain each annual audit report for the last five years.

(h) If the third-party audit finds that the system does not meet one or more of the requirements of this part, the system must not accept or process any electronic controlled substance prescription. The Federal agency must also notify the Administration of the adverse audit report and provide the report to the Administration.

§ 1311.275 Pharmacy responsibilities.

(a) A pharmacy must not dispense controlled substances in response to electronic controlled substance prescriptions if its pharmacy system does not meet the requirements of this part.

(b) A pharmacy must not process electronic controlled substance prescriptions if the DEA registration or agency authorization of the prescriber was not valid at the time the prescription was signed or if the system rejected the prescription for any other reason.

(c) When a pharmacist fills a prescription in a manner that would require, under part 1306 of this chapter, the pharmacist to make a notation on the prescription if the prescription were a paper prescription, the pharmacist must make such notation electronically when filling an electronic prescription.

(d) Nothing in this part relieves a pharmacy of its responsibility to dispense controlled substances only pursuant to a prescription issued for a legitimate medical purpose by a practitioner acting in the usual course of professional practice.

§ 1311.280 Recordkeeping.

(a) A Federal agency or pharmacy must maintain records required by this part for electronic prescriptions for five years from their creation. Records may be maintained electronically. Records regarding controlled substances prescriptions that are maintained electronically must be readily retrievable from all other records.

(b) This record retention requirement shall not preempt any longer period of retention which may be required now or in the future, by any other federal or State law or regulation, applicable to practitioners, pharmacists, or pharmacies.

(c) Electronic records must be easily readable or easily rendered into a format that a person can read. They must be made available to the Administration upon request.

Dated: June 6, 2008.

Michele M. Leonhart,

Acting Administrator.

[FR Doc. E8–14405 Filed 6–26–08; 8:45 am]

BILLING CODE 4410–09–P