agency that there is no reasonable cause to believe that the sale of a specific chemical to a prospective bidder and end-user will result in the illegal manufacture of a controlled substance, that certification will be effective for one year from the date of issuance with respect to further sales of the same chemical to the same prospective bidder and end-user, unless the Administrator notifies the head of the Federal department or agency in writing that the certification is withdrawn. If the certification is withdrawn, DEA will also provide written notice to the bidder and end-user, which will contain a statement of the legal and factual basis for this determination.

(e) If the Administrator determines there is reasonable cause to believe the sale of the specific chemical to a specific bidder and end-user would result in the illegal manufacture of a controlled substance, DEA will provide written notice to the head of a Federal department or agency refusing to certify the proposed sale under the authority of 21 U.S.C. 890. DEA also will provide, within fifteen calendar days of receiving a request for certification from a Federal department or agency, the same written notice to the prospective bidder and end-user, and this notice also will contain a statement of the legal and factual basis for the refusal of certification. The prospective bidder and end-user may, within thirty calendar days of receipt of notification of the refusal, submit written comments or written objections to the Administrator's refusal. At the same time, the prospective bidder and end-user also may provide supporting documentation to contest the Administrator's refusal. If such written comments or written objections raise issues regarding any finding of fact or conclusion of law upon which the refusal is based, the Administrator will reconsider the refusal of the proposed sale in light of the written comments or written objections filed. Thereafter, within a reasonable time, the Administrator will withdraw or affirm the original refusal of certification as he determines appropriate. The Administrator will provide written reasons for any affirmation of the original refusal. Such affirmation of the original refusal will constitute a final decision for purposes of judicial review under 21 U.S.C. 877.

(f) If the Administrator determines there is reasonable cause to believe that an existing certification should be withdrawn, DEA will provide written notice to the head of a Federal department or agency of such withdrawal under the authority of 21 U.S.C. 890. DEA also will provide, within fifteen calendar days of withdrawal of an existing certification, the same written notice to the bidder and end-user, and this notice also will contain a statement of the legal and factual basis for the withdrawal. The bidder and end-user may, within thirty calendar days of receipt of notification of the withdrawal of the existing certification, submit written comments or written objections to the Administrator's withdrawal. At the same time, the bidder and end-user also may provide supporting documentation to contest the Administrator's withdrawal. If such written comments or written objections raise issues regarding any finding of fact or conclusion of law upon which the withdrawal of the existing certification is based, the Administrator will reconsider the withdrawal of the existing certification in light of the written comments or written objections filed. Thereafter, within a reasonable time, the Administrator will withdraw or affirm the original withdrawal of the existing certification as he determines appropriate. The Administrator will provide written reasons for any affirmation of the original withdrawal of the existing certification. Such affirmation of the original withdrawal of the existing certification will constitute a final decision for purposes of judicial review under 21 U.S.C. 877.

[68 FR 62737, Nov. 6, 2003, as amended at 75 FR 10681, Mar. 9, 2010]

PART 1311—REQUIREMENTS FOR ELECTRONIC ORDERS AND PRESCRIPTIONS

Subpart A—General

Sec.

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

SOURCE: 70 FR 16915, Apr. 1, 2005, unless otherwise noted.

Subpart A—General

§ 1311.01 Scope.

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

[75 FR 16310, Mar. 31, 2010]

§ 1311.02 Definitions.

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

[75 FR 16310, Mar. 31, 2010]

§ 1311.05 Standards for technologies for electronic transmission of orders.

(a) A registrant or a person with power of attorney to sign orders for Schedule I and II controlled substances may use any technology to sign and electronically transmit orders if the technology provides all of the following:

(1) *Authentication:* The system must enable a recipient to positively verify the signer without direct communication with the signer and subsequently demonstrate to a third party, if needed, that the sender's identity was properly verified.

(2) *Nonrepudiation:* The system must ensure that strong and substantial evidence is available to the recipient of the sender's identity, sufficient to prevent the sender from successfully denying having sent the data. This criterion includes the ability of a third party to verify the origin of the document.

(3) *Message integrity:* The system must ensure that the recipient, or a third party, can determine whether the

contents of the document have been altered during transmission or after receipt.

(b) DEA has identified the following means of electronically signing and transmitting order forms as meeting all of the standards set forth in paragraph (a) of this section.

(1) Digital signatures using Public Key Infrastructure (PKI) technology.

(2) [Reserved]

§ 1311.08 Incorporation by reference.

(a) These incorporations by reference were approved by the Director of the Federal Register in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. Copies may be inspected at the Drug Enforcement Administration, 600 Army Navy Drive, Arlington, VA 22202 or at the National Archives and Records Administration (NARA). For information on the availability of this material at the Drug Enforcement Administration, call (202) 307–1000. For information on the availability of this material at NARA, call (202) 741–6030 or go to: *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html*.

(b) These standards are available from the National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899–8930, (301) 975–6478 or TTY (301) 975–8295, *inquiries@nist.gov*, and are available at *http://csrc.nist.gov/*. The following standards are incorporated by reference:

(1) Federal Information Processing Standard Publication (FIPS PUB) 140–2, Change Notices (12–03–2002), Security Requirements for Cryptographic Modules, May 25, 2001 (FIPS 140–2) including Annexes A through D; incorporation by reference approved for §§ 1311.30(b), 1311.55(b), 1311.115(b), 1311.120(b), 1311.205(b).

(i) *Annex A:* Approved Security Functions for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, September 23, 2004.

(ii) *Annex B:* Approved Protection Profiles for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, November 4, 2004.

(iii) *Annex C:* Approved Random Number Generators for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, January 31, 2005.

(iv) *Annex D:* Approved Key Establishment Techniques for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, February 23, 2004.

(2) Federal Information Processing Standard Publication (FIPS PUB) 180–2, Secure Hash Standard, August 1, 2002, as amended by change notice 1, February 25, 2004 (FIPS 180–2); incorporation by reference approved for §§ 1311.30(b) and 1311.55(b).

(3) Federal Information Processing Standard Publication (FIPS PUB) 180–3, Secure Hash Standard (SHS), October 2008 (FIPS 180–3); incorporation by reference approved for §§ 1311.120(b) and 1311.205(b).

(4) Federal Information Processing Standard Publication (FIPS PUB) 186–2, Digital Signature Standard, January 27, 2000, as amended by Change Notice 1, October 5, 2001 (FIPS 186–2); incorporation by reference approved for §§ 1311.30(b) and 1311.55(b).

(5) Federal Information Processing Standard Publication (FIPS PUB) 186–3, Digital Signature Standard (DSS), June 2009 (FIPS 186–3); incorporation by reference approved for §§ 1311.120(b), 1311.205(b), and 1311.210(c).

(6) Draft NIST Special Publication 800–63–1, Electronic Authentication Guideline, December 8, 2008 (NIST SP 800–63–1); Burr, W. et al.; incorporation by reference approved for § 1311.105(a).

(7) NIST Special Publication 800–76–1, Biometric Data Specification for Personal Identity Verification, January 2007 (NIST SP 800–76–1); Wilson, C. et al.; incorporation by reference approved for § 1311.116(d).

[75 FR 16310, Mar. 31, 2010]

Subpart B—Obtaining and Using Digital Certificates for Electronic Orders

§ 1311.10 Eligibility to obtain a CSOS digital certificate.

The following persons are eligible to obtain a CSOS digital certificate from the DEA Certification Authority to sign electronic orders for controlled substances.

(a) The person who signed the most recent DEA registration application or renewal application and a person authorized to sign a registration application.

(b) A person granted power of attorney by a DEA registrant to sign orders for one or more schedules of controlled substances.

§ 1311.15 Limitations on CSOS digital certificates.

(a) A CSOS digital certificate issued by the DEA Certification Authority will authorize the certificate holder to sign orders for only those schedules of controlled substances covered by the registration under which the certificate is issued.

(b) When a registrant, in a power of attorney letter, limits a certificate applicant to a subset of the registrant's authorized schedules, the registrant is responsible for ensuring that the certificate holder signs orders only for that subset of schedules.

§ 1311.20 Coordinators for CSOS digital certificate holders.

(a) Each registrant, regardless of number of digital certificates issued, must designate one or more responsible persons to serve as that registrant's CSOS coordinator regarding issues pertaining to issuance of, revocation of, and changes to digital certificates issued under that registrant's DEA registration. While the coordinator will be the main point of contact between one or more DEA registered locations and the CSOS Certification Authority, all digital certificate activities are the responsibility of the registrant with whom the digital certificate is associated. Even when an individual registrant, *i.e.*, an individual practitioner, is applying for a digital certificate to order controlled substances a CSOS Coordinator must be designated; though in such a case, the individual practitioner may also serve as the coordinator.

(b) Once designated, coordinators must identify themselves, on a one-time basis, to the Certification Authority. If a designated coordinator changes, the Certification Authority must be notified of the change and the new responsibilities assumed by each of the registrant's coordinators, if applicable. Coordinators must complete the application that the DEA Certification Authority provides and submit the following:

(1) Two copies of identification, one of which must be a government-issued photographic identification.

(2) A copy of each current DEA Certificate of Registration (DEA form 223) for each registered location for which the coordinator will be responsible or, if the applicant (or their employer) has not been issued a DEA registration, a copy of each application for registration of the applicant or the applicant's employer.

(3) The applicant must have the completed application notarized and forward the completed application and accompanying documentation to the DEA Certification Authority.

(c) Coordinators will communicate with the Certification Authority regarding digital certificate applications, renewals and revocations. For applicants applying for a digital certificate from the DEA Certification Authority, and for applicants applying for a power of attorney digital certificate for a DEA registrant, the registrant's Coordinator must verify the applicant's identity, review the application package, and submit the completed package to the Certification Authority.

§ 1311.25 Requirements for obtaining a CSOS digital certificate.

(a) To obtain a certificate to use for signing electronic orders for controlled substances, a registrant or person with power of attorney for a registrant must complete the application that the DEA Certification Authority provides and submit the following:

(1) Two copies of identification, one of which must be a government-issued photographic identification.

(2) A current listing of DEA registrations for which the individual has authority to sign controlled substances orders.

(3) A copy of the power of attorney from the registrant, if applicable.

(4) An acknowledgment that the applicant has read and understands the Subscriber Agreement and agrees to the statement of subscriber obligations that DEA provides.

(b) The applicant must provide the completed application to the registrant's coordinator for CSOS digital certificate holders who will review the application and submit the completed application and accompanying documentation to the DEA Certification Authority.

(c) When the Certification Authority approves the application, it will send the applicant a one-time use reference number and access code, via separate channels, and information on how to use them. Using this information, the applicant must then electronically submit a request for certification of the public digital signature key. After the request is approved, the Certification Authority will provide the applicant with the signed public key certificate.

(d) Once the applicant has generated the key pair, the Certification Authority must prove that the user has possession of the key. For public keys, the corresponding private key must be used to sign the certificate request. Verification of the signature using the public key in the request will serve as proof of possession of the private key.

§ 1311.30 Requirements for storing and using a private key for digitally signing orders.

(a) Only the certificate holder may access or use his or her digital certificate and private key.

(b) The certificate holder must provide FIPS-approved secure storage for the private key, as discussed by FIPS 140–2, 180–2, 186–2, and accompanying change notices and annexes, as incorporated by reference in § 1311.08.

(c) A certificate holder must ensure that no one else uses the private key. While the private key is activated, the certificate holder must prevent unauthorized use of that private key.

(d) A certificate holder must not make back-up copies of the private key.

(e) The certificate holder must report the loss, theft, or compromise of the private key or the password, via a revocation request, to the Certification Authority within 24 hours of substantiation of the loss, theft, or compromise. Upon receipt and verification of a signed revocation request, the Certification Authority will revoke the certificate. The certificate holder must apply for a new certificate under the requirements of § 1311.25.

§ 1311.35 Number of CSOS digital certificates needed.

A purchaser of Schedule I and II controlled substances must obtain a separate CSOS certificate for each registered location for which the purchaser will order these controlled substances.

§ 1311.40 Renewal of CSOS digital certificates.

(a) A CSOS certificate holder must generate a new key pair and obtain a new CSOS digital certificate when the registrant's DEA registration expires or whenever the information on which the certificate is based changes. This information includes the registered name and address, the subscriber's name, and the schedules the registrant is authorized to handle. A CSOS certificate will expire on the date on which the DEA registration on which the certificate is based expires.

(b) The Certification Authority will notify each CSOS certificate holder 45 days in advance of the expiration of the certificate holder's CSOS digital certificate.

(c) If a CSOS certificate holder applies for a renewal before the certificate expires, the certificate holder may renew electronically twice. For every third renewal, the CSOS certificate holder must submit a new application and documentation, as provided in § 1311.25.

(d) If a CSOS certificate expires before the holder applies for a renewal, the certificate holder must submit a new application and documentation, as provided in § 1311.25.

§ 1311.45 Requirements for registrants that allow powers of attorney to obtain CSOS digital certificates under their DEA registration.

(a) A registrant that grants power of attorney must report to the DEA Certification Authority within 6 hours of either of the following (advance notice may be provided, where applicable):

(1) The person with power of attorney has left the employ of the institution.

(2) The person with power of attorney has had his or her privileges revoked.

(b) A registrant must maintain a record that lists each person granted power of attorney to sign controlled substances orders.

§ 1311.50 Requirements for recipients of digitally signed orders.

(a) The recipient of a digitally signed order must do the following before filling the order:

(1) Verify the integrity of the signature and the order by having the system validate the order.

(2) Verify that the certificate holder's CSOS digital certificate has not expired by checking the expiration date against the date the order was signed.

(3) Check the validity of the certificate holder's certificate by checking the Certificate Revocation List.

(4) Check the certificate extension data to determine whether the sender has the authority to order the controlled substance.

(b) A recipient may cache Certificate Revocation Lists for use until they expire.

§ 1311.55 Requirements for systems used to process digitally signed orders.

(a) A CSOS certificate holder and recipient of an electronic order may use any system to write, track, or maintain orders provided that the system has been enabled to process digitally signed documents and that it meets the requirements of paragraph (b) or (c) of this section.

(b) A system used to digitally sign Schedule I or II orders must meet the following requirements:

(1) The cryptographic module must be FIPS 140–2, Level 1 validated, as incorporated by reference in § 1311.08.

(2) The digital signature system and hash function must be compliant with FIPS 186–2 and FIPS 180–2, as incorporated by reference in § 1311.08.

(3) The private key must be stored on a FIPS 140–2 Level 1 validated cryptographic module using a FIPS-approved encryption algorithm, as incorporated by reference in § 1311.08.

(4) The system must use either a user identification and password combination or biometric authentication to access the private key. Activation data must not be displayed as they are entered.

(5) The system must set a 10-minute inactivity time period after which the certificate holder must reauthenticate the password to access the private key.

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

(7) The system must be able to digitally sign and transmit an order.

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

(9) The system must archive the digitally signed orders and any other records required in part 1305 of this chapter, including any linked data.

(10) The system must create an order that includes all data fields listed under § 1305.21(b) of this chapter.

(c) A system used to receive, verify, and create linked records for orders signed with a CSOS digital certificate must meet the following requirements:

(1) The cryptographic module must be FIPS 140–2, Level 1 validated, as incorporated by reference in § 1311.08.

(2) The digital signature system and hash function must be compliant with FIPS 186–2 and FIPS 180–2, as incorporated by reference in § 1311.08.

(3) The system must determine that an order has not been altered during transmission. The system must invalidate any order that has been altered.

(4) The system must validate the digital signature using the signer's public key. The system must invalidate any order in which the digital signature cannot be validated.

(5) The system must validate that the DEA registration number contained in the body of the order corresponds to the registration number associated with the specific certificate by separately generating the hash value of the registration number and certificate subject distinguished name serial number and comparing that hash value to the hash value contained in the certificate extension for the DEA registration number. If the hash values are not

equal the system must invalidate the order.

(6) The system must check the Certificate Revocation List automatically and invalidate any order with a certificate listed on the Certificate Revocation List.

(7) The system must check the validity of the certificate and the Certification Authority certificate and invalidate any order that fails these validity checks.

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

(9) The system must check the substances ordered against the schedules that the registrant is allowed to order and invalidate any order that includes substances the registrant is not allowed to order.

(10) The system must ensure that an invalid finding cannot be bypassed or ignored and the order filled.

(11) The system must archive the order and associate with it the digital certificate received with the order.

(12) If a registrant sends reports on orders to DEA, the system must create a report in the format DEA specifies, as provided in §1305.29 of this chapter.

(d) For systems used to process CSOS orders, the system developer or vendor must have an initial independent third-party audit of the system and an additional independent third-party audit whenever the signing or verifying functionality is changed to determine whether it correctly performs the functions listed under paragraphs (b) and (c) of this section. The system developer must retain the most recent audit results and retain the results of any other audits of the software completed within the previous two years.

§1311.60 Recordkeeping.

(a) A supplier and purchaser must maintain records of CSOS electronic orders and any linked records for two years. Records may be maintained electronically. Records regarding controlled substances that are maintained electronically must be readily retrievable from all other records.

(b) 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.

(c) CSOS certificate holders must maintain a copy of the subscriber agreement that the Certification Authority provides for the life of the certificate.

Subpart C—Electronic Prescriptions

SOURCE: 75 FR 16310, Mar. 31, 2010, unless otherwise noted.

§1311.100 General.

(a) This subpart addresses the requirements that must be met to issue and process Schedule II, III, IV, and V controlled substance prescriptions electronically.

(b) A practitioner may issue a prescription for a Schedule II, III, IV, or V controlled substance electronically if all of the following conditions are met:

(1) The practitioner is registered as an individual practitioner or exempt from the requirement of 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 application that meets all of the applicable requirements of this subpart; and

(3) The prescription is otherwise in conformity with the requirements of the Act and this chapter.

(c) An electronic prescription for a Schedule II, III, IV, or V controlled substance created using an electronic prescription application that does not meet the requirements of this subpart is not a valid prescription, as that term is defined in §1300.03 of this chapter.

(d) A controlled substance prescription created using an electronic prescription application that meets the requirements of this subpart is not a valid prescription if any of the functions required under this subpart were disabled when the prescription was indicated as ready for signature and signed.

(e) A registered pharmacy may process electronic prescriptions for controlled substances only if all of the following conditions are met:

(1) The pharmacy uses a pharmacy application that meets all of the applicable requirements of this subpart; and

(2) The prescription is otherwise in conformity with the requirements of the Act and this chapter.

(f) Nothing in this part alters the responsibilities of the practitioner and pharmacy, specified in part 1306 of this chapter, to ensure the validity of a controlled substance prescription.

§ 1311.102 Practitioner responsibilities.

(a) The practitioner must retain sole possession of the hard token, where applicable, and must not share the password or other knowledge factor, or biometric information, with any other person. The practitioner must not allow any other person to use the token or enter the knowledge factor or other identification means to sign prescriptions for controlled substances. Failure by the practitioner to secure the hard token, knowledge factor, or biometric information 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 individuals designated under §1311.125 or §1311.130 within one business day of discovery that the hard token has been lost, stolen, or compromised or the authentication protocol has been otherwise compromised. A practitioner who fails to comply with this provision may be held responsible for any controlled substance prescriptions written using his two-factor authentication credential.

(c) If the practitioner is notified by an intermediary or pharmacy that an electronic prescription was not successfully delivered, as provided in §1311.170, he must ensure that any paper or oral prescription (where permitted) issued as a replacement of the original electronic prescription indicates that the prescription was originally transmitted electronically to a particular pharmacy and that the transmission failed.

(d) Before initially using an electronic prescription application to sign and transmit controlled substance prescriptions, the practitioner must determine that the third-party auditor or certification organization has found that the electronic prescription application records, stores, and transmits the following accurately and consistently:

(1) The information required for a prescription under §1306.05(a) of this chapter.

(2) The indication of signing as required by §1311.120(b)(17) or the digital signature created by the practitioner's private key.

(3) The number of refills as required by §1306.22 of this chapter.

(e) If the third-party auditor or certification organization has found that an electronic prescription application does not accurately and consistently record, store, and transmit other information required for prescriptions under this chapter, the practitioner must not create, sign, and transmit electronic prescriptions for controlled substances that are subject to the additional information requirements.

(f) The practitioner must not use the electronic prescription application to sign and transmit electronic controlled substance prescriptions if any of the functions of the application required by this subpart have been disabled or appear to be functioning improperly.

(g) If an electronic prescription application provider notifies an individual practitioner that a third-party audit or certification report indicates that the application or the application provider no longer meets the requirements of this part or notifies him that the application provider has identified an issue that makes the application non-compliant, the practitioner must do the following:

(1) Immediately cease to issue electronic controlled substance prescriptions using the application.

(2) Ensure, for an installed electronic prescription application at an individual practitioner's practice, that the individuals designated under §1311.125 terminate access for signing controlled substance prescriptions.

(h) If an electronic prescription application provider notifies an institutional practitioner that a third-party audit or certification report indicates that the application or the application provider no longer meets the requirements of this part or notifies it that

the application provider has identified an issue that makes the application non-compliant, the institutional practitioner must ensure that the individuals designated under §1311.130 terminate access for signing controlled substance prescriptions.

(i) An individual practitioner or institutional practitioner that receives a notification that the electronic prescription application is not in compliance with the requirements of this part must not use the application to issue electronic controlled substance prescriptions until it is notified that the application is again compliant and all relevant updates to the application have been installed.

(j) The practitioner must notify both the individuals designated under §1311.125 or §1311.130 and the Administration within one business day of discovery that one or more prescriptions that were issued under a DEA registration held by that practitioner were prescriptions the practitioner had not signed or were not consistent with the prescriptions he signed.

(k) 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 subpart 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.

§1311.105 Requirements for obtaining an authentication credential—Individual practitioners.

(a) An individual practitioner must obtain a two-factor authentication credential from one of the following:

(1) A credential service provider that has been approved by the General Services Administration Office of Technology Strategy/Division of Identity Management to conduct identity proofing that meets the requirements of Assurance Level 3 or above as specified in NIST SP 800–63–1 as incorporated by reference in §1311.08.

(2) For digital certificates, a certification authority that is cross-certified with the Federal Bridge certification authority and that operates at a Federal Bridge Certification Authority basic assurance level or above.

(b) The practitioner must submit identity proofing information to the credential service provider or certification authority as specified by the credential service provider or certification authority.

(c) The credential service provider or certification authority must issue the authentication credential using two channels (e.g., e-mail, mail, or telephone call). If one of the factors used in the authentication protocol is a biometric, or if the practitioner has a hard token that is being enabled to sign controlled substances prescriptions, the credential service provider or certification authority must issue two pieces of information used to generate or activate the authentication credential using two channels.

§1311.110 Requirements for obtaining an authentication credential—Individual practitioners eligible to use an electronic prescription application of an institutional practitioner.

(a) For any registrant or person exempted from the requirement of registration under §1301.22(c) of this chapter who is eligible to use the institutional practitioner's electronic prescription application to sign prescriptions for controlled substances, the entity within a DEA-registered institutional practitioner that grants that individual practitioner privileges at the institutional practitioner (e.g., a hospital credentialing office) may conduct identity proofing and authorize the issuance of the authentication credential. That entity must do the following:

(1) Ensure that photographic identification issued by the Federal Government or a State government matches the person presenting the identification.

(2) Ensure that the individual practitioner's State authorization to practice

and, where applicable, State authorization to prescribe controlled substances, is current and in good standing.

(3) Either ensure that the individual practitioner's DEA registration is current and in good standing or ensure that the institutional practitioner has granted the individual practitioner exempt from the requirement of registration under §1301.22 of this chapter privileges to prescribe controlled substances using the institutional practitioner's DEA registration number.

(4) 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.

(5) 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.

(b) An institutional practitioner that elects to conduct identity proofing must provide authorization to issue the authentication credentials to a separate entity within the institutional practitioner or to an outside credential Service provider or certification authority that meets the requirements of §1311.105(a).

(c) When an institutional practitioner is conducting identity proofing and submitting information to a credential service provider or certification authority to authorize the issuance of authentication credentials, the institutional practitioner must meet any requirements that the credential service provider or certification authority imposes on entities that serve as trusted agents.

(d) An institutional practitioner that elects to conduct identity proofing and authorize the issuance of the authentication credential as provided in paragraphs (a) through (c) of this section must do so in a manner consistent with the institutional practitioner's general obligation to maintain effective controls against diversion. Failure to meet this obligation may result in remedial action consistent with §1301.36 of this chapter.

(e) An institutional practitioner that elects to conduct identity proofing must retain a record of the identity-proofing. An institutional practitioner that elects to issue the two-factor authentication credential must retain a record of the issuance of the credential.

§1311.115 Additional requirements for two-factor authentication.

(a) To sign a controlled substance prescription, the electronic prescription application must require the practitioner to authenticate to the application using an authentication protocol that uses two of the following three factors:

(1) Something only the practitioner knows, such as a password or response to a challenge question.

(2) Something the practitioner is, biometric data such as a fingerprint or iris scan.

(3) Something the practitioner has, a device (hard token) separate from the computer to which the practitioner is gaining access.

(b) If one factor is a hard token, it must be separate from the computer to which it is gaining access and must meet at least the criteria of FIPS 140–2 Security Level 1, as incorporated by reference in §1311.08, for cryptographic modules or one-time-password devices.

(c) If one factor is a biometric, the biometric subsystem must comply with the requirements of §1311.116.

§1311.116 Additional requirements for biometrics.

(a) If one of the factors used to authenticate to the electronic prescription application is a biometric as described in §1311.115, it must comply with the following requirements.

(b) The biometric subsystem must operate at a false match rate of 0.001 or lower.

(c) The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the false

match rate described in paragraph (b) of this section, or a lower false match rate. Testing to demonstrate performance must be conducted by the National Institute of Standards and Technology or another DEA-approved government or nongovernment laboratory. Such testing must comply with the requirements of paragraph (h) of this section.

(d) The biometric subsystem must conform to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST SP 800–76–1 as incorporated by reference in §1311.08, if they exist for the biometric modality of choice.

(e) The biometric subsystem must either be co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location, or be built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances.

(f) The biometric subsystem must store device ID data at enrollment (*i.e.*, biometric registration) with the biometric data and verify the device ID at the time of authentication to the electronic prescription application.

(g) The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or nonmatch results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be:

(1) Cryptographically source authenticated;

(2) Combined with a random challenge, a nonce, or a time stamp to prevent replay;

(3) Cryptographically protected for integrity and confidentiality; and

(4) Sent only to authorized systems.

(h) Testing of the biometric subsystem must have the following characteristics:

(1) The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric.

(2) Test data are sequestered.

(3) Algorithms are provided to the testing laboratory (as opposed to scores or other information).

(4) The operating point(s) corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate, is tested so that there is at least 95% confidence that the false match and nonmatch rates are equal to or less than the observed value.

(5) Results of the testing are made publicly available.

§1311.120 Electronic prescription application requirements.

(a) A practitioner may only use an electronic prescription application that meets the requirements in paragraph (b) of this section to issue electronic controlled substance prescriptions.

(b) The electronic prescription application must meet the requirements of this subpart including the following:

(1) The electronic prescription application must do the following:

(i) Link each registrant, by name, to at least one DEA registration number.

(ii) Link each practitioner exempt from registration under §1301.22(c) of this chapter to the institutional practitioner's DEA registration number and the specific internal code number required under §1301.22(c)(5) of this chapter.

(2) The electronic prescription application must be capable of the setting of logical access controls to limit permissions for the following functions:

(i) Indication that a prescription is ready for signing and signing controlled substance prescriptions.

(ii) Creating, updating, and executing the logical access controls for the functions specified in paragraph (b)(2)(i) of this section.

(3) Logical access controls must be set by individual user name or role. If the application sets logical access control by role, it must not allow an individual to be assigned the role of registrant unless that individual is linked to at least one DEA registration number as provided in paragraph (b)(1) of this section.

(4) The application must require that the setting and changing of logical access controls specified under paragraph

(b)(2) of this section involve the actions of two individuals as specified in §§ 1311.125 or 1311.130. Except for institutional practitioners, a practitioner authorized to sign controlled substance prescriptions must approve logical access control entries.

(5) The electronic prescription application must accept two-factor authentication that meets the requirements of § 1311.115 and require its use for signing controlled substance prescriptions and for approving data that set or change logical access controls related to reviewing and signing controlled substance prescriptions.

(6) The electronic prescription application must be capable of recording all of the applicable information required in part 1306 of this chapter for the controlled substance prescription.

(7) If a practitioner has more than one DEA registration number, the electronic prescription application must require the practitioner or his agent to select the DEA registration number to be included on the prescription.

(8) The electronic prescription application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.

(9) The electronic prescription application must present for the practitioner's review and approval all of the following data for each controlled substance prescription:

(i) The date of issuance.

(ii) The full name of the patient.

(iii) The drug name.

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

(v) The number of refills authorized, if applicable, for prescriptions for Schedule III, IV, and V controlled substances.

(vi) For prescriptions written in accordance with the requirements of § 1306.12(b) of this chapter, the earliest date on which a pharmacy may fill each prescription.

(vii) The name, address, and DEA registration number of the prescribing practitioner.

(viii) The statement required under § 1311.140(a)(3).

(10) The electronic prescription application must require the prescribing practitioner to indicate that each controlled substance prescription is ready for signing. The electronic prescription application must not permit alteration of the DEA elements after the practitioner has indicated that a controlled substance prescription is ready to be signed without requiring another review and indication of readiness for signing. Any controlled substance prescription not indicated as ready to be signed shall not be signed or transmitted.

(11) While the information required by paragraph (b)(9) of this section and the statement required by § 1311.140(a)(3) remain displayed, the electronic prescription application must prompt the prescribing practitioner to authenticate to the application, using two-factor authentication, as specified in § 1311.140(a)(4), which will constitute the signing of the prescription by the practitioner for purposes of § 1306.05(a) and (e) of this chapter.

(12) The electronic prescription application must not permit a practitioner other than the prescribing practitioner whose DEA number (or institutional practitioner DEA number and extension data for the individual practitioner) is listed on the prescription as the prescribing practitioner and who has indicated that the prescription is ready to be signed to sign the prescription.

(13) Where a practitioner seeks to prescribe more than one controlled substance at one time for a particular patient, the electronic prescription application may allow the practitioner to sign multiple prescriptions for a single patient at one time using a single invocation of the two-factor authentication protocol provided the following has occurred: The practitioner has individually indicated that each controlled substance prescription is ready to be signed while the information required by paragraph (b)(9) of this section for each such prescription is displayed along with the statement required by § 1311.140(a)(3).

(14) The electronic prescription application must time and date stamp the prescription when the signing function is used.

(15) When the practitioner uses his two-factor authentication credential as specified in §1311.140(a)(4), the electronic prescription application must digitally sign at least the information required by part 1306 of this chapter and electronically archive the digitally signed record. If the practitioner signs the prescription with his own private key, as provided in §1311.145, the electronic prescription application must electronically archive a copy of the digitally signed record, but need not apply the application's digital signature to the record.

(16) The digital signature functionality must meet the following requirements:

(i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140–2 Security Level 1 validated. FIPS 140–2 is incorporated by reference in §1311.08.

(ii) The digital signature application and hash function must comply with FIPS 186–3 and FIPS 180–3, as incorporated by reference in §1311.08.

(iii) The electronic prescription application's private key must be stored encrypted on a FIPS 140–2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140–2 is incorporated by reference in §1311.08.

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

(17) Unless the digital signature created by an individual practitioner's private key is being transmitted to the pharmacy with the prescription, the electronic prescription application must include in the data file transmitted an indication that the prescription was signed by the prescribing practitioner.

(18) The electronic prescription application must not transmit a controlled substance prescription unless the signing function described in §1311.140(a)(4) has been used.

(19) The electronic prescription application must not allow alteration of any of the information required by part 1306 of this chapter after the prescription has been digitally signed. Any alteration of the information required by part 1306 of this chapter after the prescription is digitally signed must cancel the prescription.

(20) The electronic prescription application must not allow transmission of a prescription that has been printed.

(21) The electronic prescription application must allow printing of a prescription after transmission only if the printed prescription is clearly labeled as a copy not for dispensing. The electronic prescription application may allow printing of prescription information if clearly labeled as being for informational purposes. The electronic prescription application may transfer such prescription information to medical records.

(22) If the transmission of an electronic prescription fails, the electronic prescription application may print the prescription. The prescription must indicate that it was originally transmitted electronically to, and provide the name of, a specific pharmacy, the date and time of transmission, and that the electronic transmission failed.

(23) The electronic prescription application must maintain an audit trail of all actions related to the following:

(i) The creation, alteration, indication of readiness for signing, signing, transmission, or deletion of a controlled substance prescription.

(ii) Any setting or changing of logical access control permissions related to the issuance of controlled substance prescriptions.

(iii) Notification of a failed transmission.

(iv) Auditable events as specified in §1311.150.

(24) The electronic prescription application must record within each audit record the following information:

(i) The date and time of the event.

(ii) The type of event.

(iii) The identity of the person taking the action, where applicable.

(iv) The outcome of the event (success or failure).

(25) The electronic prescription application must conduct internal audits and generate reports on any of the events specified in §1311.150 in a format

that is readable by the practitioner. Such internal audits may be automated and need not require human intervention to be conducted.

(26) The electronic prescription application must protect the stored audit records from unauthorized deletion. The electronic prescription application shall prevent modifications to the audit records.

(27) The electronic prescription application must do the following:

(i) Generate a log of all controlled substance prescriptions issued by a practitioner during the previous calendar month and provide the log to the practitioner no later than seven calendar days after that month.

(ii) Be capable of generating a log of all controlled substance prescriptions issued by a practitioner for a period specified by the practitioner upon request. Prescription information available from which to generate the log must span at least the previous two years.

(iii) Archive all logs generated.

(iv) Ensure that all logs are easily readable or easily rendered into a format that a person can read.

(v) Ensure that all logs are sortable by patient name, drug name, and date of issuance of the prescription.

(28) Where the electronic prescription application is required by this part to archive or otherwise maintain records, it must retain such records electronically for two years from the date of the record's creation and comply with all other requirements of § 1311.305.

§ 1311.125 Requirements for establishing logical access control—Individual practitioner.

(a) At each registered location where one or more individual practitioners wish to use an electronic prescription application meeting the requirements of this subpart to issue controlled substance prescriptions, the registrant(s) must designate at least two individuals to manage access control to the application. At least one of the designated individuals must be a registrant who is authorized to issue controlled substance prescriptions and who has obtained a two-factor authentication credential as provided in § 1311.105.

(b) At least one of the individuals designated under paragraph (a) of this section must verify that the DEA registration and State authorization(s) to practice and, where applicable, State authorization(s) to dispense controlled substances of each registrant being granted permission to sign electronic prescriptions for controlled substances are current and in good standing.

(c) After one individual designated under paragraph (a) of this section enters data that grants permission for individual practitioners to have access to the prescription functions that indicate readiness for signature and signing or revokes such authorization, a second individual designated under paragraph (a) of this section must use his two-factor authentication credential to satisfy the logical access controls. The second individual must be a DEA registrant.

(d) A registrant's permission to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions must be revoked whenever any of the following occurs, on the date the occurrence is discovered:

(1) A hard token or any other authentication factor required by the two-factor authentication protocol is lost, stolen, or compromised. Such access must be terminated immediately upon receiving notification from the individual practitioner.

(2) The individual practitioner's DEA registration expires, unless the registration has been renewed.

(3) The individual practitioner's DEA registration is terminated, revoked, or suspended.

(4) The individual practitioner is no longer authorized to use the electronic prescription application (e.g., when the individual practitioner leaves the practice).

§ 1311.130 Requirements for establishing logical access control—Institutional practitioner.

(a) The entity within an institutional practitioner that conducts the identity proofing under § 1311.110 must develop a list of individual practitioners who are

permitted to use the institutional practitioner's electronic prescription application to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions. The list must be approved by two individuals.

(b) After the list is approved, it must be sent to a separate entity within the institutional practitioner that enters permissions for logical access controls into the application. The institutional practitioner must authorize at least two individuals or a role filled by at least two individuals to enter the logical access control data. One individual in the separate entity must authenticate to the application and enter the data to grant permissions to individual practitioners to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions. A second individual must authenticate to the application to execute the logical access controls.

(c) The institutional practitioner must retain a record of the individuals or roles that are authorized to conduct identity proofing and logical access control data entry and execution.

(d) Permission to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions must be revoked whenever any of the following occurs, on the date the occurrence is discovered:

(1) An individual practitioner's hard token or any other authentication factor required by the practitioner's two-factor authentication protocol is lost, stolen, or compromised. Such access must be terminated immediately upon receiving notification from the individual practitioner.

(2) The institutional practitioner's or, where applicable, individual practitioner's DEA registration expires, unless the registration has been renewed.

(3) The institutional practitioner's or, where applicable, individual practitioner's DEA registration is terminated, revoked, or suspended.

(4) An individual practitioner is no longer authorized to use the institutional practitioner's electronic prescription application (e.g., when the individual practitioner is no longer associated with the institutional practitioner.)

§ 1311.135 Requirements for creating a controlled substance prescription.

(a) The electronic prescription application may allow the registrant or his agent to enter data for a controlled substance prescription, provided that only the registrant may sign the prescription in accordance with §§ 1311.120(b)(11) and 1311.140.

(b) If a practitioner holds multiple DEA registrations, the practitioner or his agent must select the appropriate registration number for the prescription being issued in accordance with the requirements of § 1301.12 of this chapter.

(c) If required by State law, a supervisor's name and DEA number may be listed on a prescription, provided the prescription clearly indicates who is the supervisor and who is the prescribing practitioner.

§ 1311.140 Requirements for signing a controlled substance prescription.

(a) For a practitioner to sign an electronic prescription for a controlled substance the following must occur:

(1) The practitioner must access a list of one or more controlled substance prescriptions for a single patient. The list must display the information required by § 1311.120(b)(9).

(2) The practitioner must indicate the prescriptions that are ready to be signed.

(3) While the prescription information required in § 1311.120(b)(9) is displayed, the following statement or its substantial equivalent is displayed: ''By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing. The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear above.''

(4) While the prescription information required in § 1311.120(b)(9) and the statement required by paragraph (a)(3) of this section remain displayed, the

practitioner must be prompted to complete the two-factor authentication protocol.

(5) The completion by the practitioner of the two-factor authentication protocol in the manner provided in paragraph (a)(4) of this section will constitute the signing of the prescription by the practitioner for purposes of §1306.05(a) and (e) of this chapter.

(6) Except as provided under §1311.145, the practitioner's completion of the two-factor authentication protocol must cause the application to digitally sign and electronically archive the information required under part 1306 of this chapter.

(b) The electronic prescription application must clearly label as the signing function the function that prompts the practitioner to execute the two-factor authentication protocol using his credential.

(c) Any prescription not signed in the manner required by this section shall not be transmitted.

§1311.145 Digitally signing the prescription with the individual practitioner's private key.

(a) An individual practitioner who has obtained a digital certificate as provided in §1311.105 may digitally sign a controlled substance prescription using the private key associated with his digital certificate.

(b) The electronic prescription application must require the individual practitioner to complete a two-factor authentication protocol as specified in §1311.140(a)(4) to use his private key.

(c) The electronic prescription application must digitally sign at least all information required under part 1306 of this chapter.

(d) The electronic prescription application must electronically archive the digitally signed record.

(e) A prescription that is digitally signed with a practitioner's private key may be transmitted to a pharmacy without the digital signature.

(f) If the electronic prescription is transmitted without the digital signature, the electronic prescription application must check the certificate revocation list of the certification authority that issued the practitioner's digital certificate. If the digital certificate is not valid, the electronic prescription application must not transmit the prescription. The certificate revocation list may be cached until the certification authority issues a new certificate revocation list.

(g) When the individual practitioner digitally signs a controlled substance prescription with the private key associated with his own digital certificate obtained as provided under §1311.105, the electronic prescription application is not required to digitally sign the prescription using the application's private key.

§1311.150 Additional requirements for internal application audits.

(a) The application provider must establish and implement a list of auditable events. Auditable events must, at a minimum, include the following:

(1) Attempted unauthorized access to the electronic prescription application, or successful unauthorized access where the determination of such is feasible.

(2) Attempted unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.

(3) Interference with application operations of the prescription application.

(4) Any setting of or change to logical access controls related to the issuance of controlled substance prescriptions.

(5) Attempted or successful interference with audit trail functions.

(6) For application service providers, attempted or successful creation, modification, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider.

(b) The electronic prescription application must analyze the audit trail at least once every calendar day and generate an incident report that identifies each auditable event.

(c) Any person designated to set logical access controls under §§1311.125 or

1311.130 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 electronic prescription application provider and the Administration within one business day.

§ 1311.170 Transmission requirements.

(a) The electronic prescription application must transmit the electronic prescription as soon as possible after signature by the practitioner.

(b) The electronic prescription application may print a prescription that has been transmitted only if an intermediary or the designated pharmacy notifies a practitioner that an electronic prescription was not successfully delivered to the designated pharmacy. If this occurs, the electronic prescription application may print the prescription for the practitioner's manual signature. The printed prescription must include information noting that the prescription was originally transmitted electronically to [name of the specific pharmacy] on [date/time] and that transmission failed.

(c) The electronic prescription application may print copies of the transmitted prescription if they are clearly labeled: ''Copy only—not valid for dispensing.'' Data on the prescription may be electronically transferred to medical records, and a list of prescriptions written may be printed for patients if the list indicates that it is for informational purposes only and not for dispensing.

(d) The electronic prescription application must not allow the transmission of an electronic prescription if an original prescription was printed prior to attempted transmission.

(e) The contents of the prescription required by part 1306 of this chapter must not be altered during transmission between the practitioner and pharmacy. Any change to the content during transmission, including truncation or removal of data, will render the electronic prescription invalid. The electronic prescription data may be converted from one software version to another between the electronic prescription application and the pharmacy application; conversion includes altering the structure of fields or machine language so that the receiving pharmacy application can read the prescription and import the data.

(f) An electronic prescription must be transmitted from the practitioner to the pharmacy in its electronic form. At no time may an intermediary convert an electronic prescription to another form (e.g., facsimile) for transmission.

§ 1311.200 Pharmacy responsibilities.

(a) Before initially using a pharmacy application to process controlled substance prescriptions, the pharmacy must determine that the third-party auditor or certification organization has found that the pharmacy application does the following accurately and consistently:

(1) Import, store, and display the information required for prescriptions under § 1306.05(a) of this chapter.

(2) Import, store, and display the indication of signing as required by § 1311.120(b)(17).

(3) Import, store, and display the number of refills as required by § 1306.22 of this chapter.

(4) Import, store, and verify the practitioner's digital signature, as provided in § 1311.210(c), where applicable.

(b) If the third-party auditor or certification organization has found that a pharmacy application does not accurately and consistently import, store, and display other information required for prescriptions under this chapter, the pharmacy must not process electronic prescriptions for controlled substances that are subject to the additional information requirements.

(c) If a pharmacy application provider notifies a pharmacy that a third-party audit or certification report indicates that the application or the application provider no longer meets the requirements of this part or notifies it that the application provider has identified an issue that makes the application non-compliant, the pharmacy must immediately cease to process controlled substance prescriptions using the application.

(d) A pharmacy that receives a notification that the pharmacy application

is not in compliance with the requirements of this part must not use the application to process controlled substance prescriptions until it is notified that the application is again compliant and all relevant updates to the application have been installed.

(e) The pharmacy must determine which employees are authorized to enter information regarding the dispensing of controlled substance prescriptions and annotate or alter records of these prescriptions (to the extent such alterations are permitted under this chapter). The pharmacy must ensure that logical access controls in the pharmacy application are set so that only such employees are granted access to perform these functions.

(f) 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 the same notation electronically when filling an electronic prescription and retain the annotation electronically in the prescription record or in linked files. When a prescription is received electronically, the prescription and all required annotations must be retained electronically.

(g) When a pharmacist receives a paper or oral prescription that indicates that it was originally transmitted electronically to the pharmacy, the pharmacist must check its records to ensure that the electronic version was not received and the prescription dispensed. If both prescriptions were received, the pharmacist must mark one as void.

(h) When a pharmacist receives a paper or oral prescription that indicates that it was originally transmitted electronically to another pharmacy, the pharmacist must check with that pharmacy to determine whether the prescription was received and dispensed. If the pharmacy that received the original electronic prescription had not dispensed the prescription, that pharmacy must mark the electronic version as void or canceled. If the pharmacy that received the original electronic prescription dispensed the prescription, the pharmacy with the paper version must not dispense the paper prescription and must mark the prescription as void.

(i) Nothing in this part relieves a pharmacy and pharmacist of the 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.

§ 1311.205 Pharmacy application requirements.

(a) The pharmacy may only use a pharmacy application that meets the requirements in paragraph (b) of this section to process electronic controlled substance prescriptions.

(b) The pharmacy application must meet the following requirements:

(1) The pharmacy application must be capable of setting logical access controls to limit access for the following functions:

(i) Annotation, alteration, or deletion of prescription information.

(ii) Setting and changing the logical access controls.

(2) Logical access controls must be set by individual user name or role.

(3) The pharmacy application must digitally sign and archive a prescription on receipt or be capable of receiving and archiving a digitally signed record.

(4) For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirements:

(i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140–2 Security Level 1 validated. FIPS 140–2 is incorporated by reference in § 1311.08.

(ii) The digital signature application and hash function must comply with FIPS 186–3 and FIPS 180–3, as incorporated by reference in § 1311.08.

(iii) The pharmacy application's private key must be stored encrypted on a FIPS 140–2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140–2 is incorporated by reference in § 1311.08.

(iv) For software implementations, when the signing module is deactivated, the pharmacy application must clear the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key.

(v) The pharmacy application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.

(5) The pharmacy application must verify a practitioner's digital signature (if the pharmacy application accepts prescriptions that were digitally signed with an individual practitioner's private key and transmitted with the digital signature).

(6) If the prescription received by the pharmacy application has not been digitally signed by the practitioner and transmitted with the digital signature, the pharmacy application must either:

(i) Verify that the practitioner signed the prescription by checking the data field that indicates the prescription was signed; or

(ii) Display the field for the pharmacist's verification.

(7) The pharmacy application must read and retain the full DEA number including the specific internal code number assigned to individual practitioners authorized to prescribe controlled substances by the hospital or other institution as provided in §1301.22(c) of this chapter.

(8) The pharmacy application must read and store, and be capable of displaying, all information required by part 1306 of this chapter.

(9) The pharmacy application must read and store in full the information required under §1306.05(a) of this chapter. The pharmacy application must either verify that such information is present or must display the information for the pharmacist's verification.

(10) The pharmacy application must provide for the following information to be added or linked to each electronic controlled substance prescription record for each dispensing:

(i) Number of units or volume of drug dispensed.

(ii) Date dispensed.

(iii) Name or initials of the person who dispensed the prescription.

(11) The pharmacy application must be capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.

(12) The pharmacy application must allow downloading of prescription data into a database or spreadsheet that is readable and sortable.

(13) The pharmacy application must maintain an audit trail of all actions related to the following:

(i) The receipt, annotation, alteration, or deletion of a controlled substance prescription.

(ii) Any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions.

(iii) Auditable events as specified in §1311.215.

(14) The pharmacy application must record within each audit record the following information:

(i) The date and time of the event.

(ii) The type of event.

(iii) The identity of the person taking the action, where applicable.

(iv) The outcome of the event (success or failure).

(15) The pharmacy application must conduct internal audits and generate reports on any of the events specified in §1311.215 in a format that is readable by the pharmacist. Such an internal audit may be automated and need not require human intervention to be conducted.

(16) The pharmacy application must protect the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.

(17) The pharmacy application must back up the controlled substance prescription records daily.

(18) The pharmacy application must retain all archived records electronically for at least two years from the date of their receipt or creation and comply with all other requirements of §1311.305.

§1311.210 Archiving the initial record.

(a) Except as provided in paragraph (c) of this section, 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 must digitally sign the prescription immediately prior to transmission to the pharmacy.

(2) The first pharmacy application that receives the electronic prescription must digitally sign the prescription immediately on receipt.

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

(c) If a pharmacy receives a digitally signed prescription that includes the individual practitioner's digital signature, the pharmacy application must do the following:

(1) Verify the digital signature as provided in FIPS 186–3, as incorporated by reference in §1311.08.

(2) Check the validity of the certificate holder's digital certificate by checking the certificate revocation list. The pharmacy may cache the CRL until it expires.

(3) Archive the digitally signed record. The pharmacy record must retain an indication that the prescription was verified upon receipt. No additional digital signature is required.

§1311.215 Internal audit trail.

(a) The pharmacy application provider must establish and implement a list of auditable events. The auditable events must, at a minimum, include the following:

(1) Attempted unauthorized access to the pharmacy application, or successful unauthorized access to the pharmacy application where the determination of such is feasible.

(2) Attempted or successful unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.

(3) Interference with application operations of the pharmacy application.

(4) Any setting of or change to logical access controls related to the dispensing of controlled substance prescriptions.

(5) Attempted or successful interference with audit trail functions.

(6) For application service providers, attempted or successful annotation, alteration, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider.

(b) The pharmacy application must analyze the audit trail at least once every calendar day and generate an incident report that identifies each auditable event.

(c) 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 pharmacy application service provider, if applicable, and the Administration within one business day.

§1311.300 Application provider requirements—Third-party audits or certifications.

(a) Except as provided in paragraph (e) of this section, the application provider of an electronic prescription application or a pharmacy application must have a third-party audit of the application that determines that the application meets the requirements of this part at each of the following times:

(1) Before the application may be used to create, sign, transmit, or process controlled substance prescriptions.

(2) Whenever a functionality related to controlled substance prescription requirements is altered or every two years, whichever occurs first.

(b) The third-party audit must be conducted by one of the following:

(1) A person qualified to conduct a SysTrust, WebTrust, or SAS 70 audit.

(2) A Certified Information System Auditor who performs compliance audits as a regular ongoing business activity.

(c) An audit for installed applications must address processing integrity and determine that the application meets the requirements of this part.

(d) An audit for application service providers must address processing integrity and physical security and determine that the application meets the requirements of this part.

(e) If a certifying organization whose certification process has been approved by DEA verifies and certifies that an electronic prescription or pharmacy application meets the requirements of this part, certification by that organization may be used as an alternative to the audit requirements of paragraphs (b) through (d) of this section, provided that the certification that determines that the application meets the requirements of this part occurs at each of the following times:

(1) Before the application may be used to create, sign, transmit, or process controlled substance prescriptions.

(2) Whenever a functionality related to controlled substance prescription requirements is altered or every two years, whichever occurs first.

(f) The application provider must make the audit or certification report available to any practitioner or pharmacy that uses the application or is considering use of the application. The electronic prescription or pharmacy application provider must retain the most recent audit or certification results and retain the results of any other audits or certifications of the application completed within the previous two years.

(g) Except as provided in paragraphs (h) and (i) of this section, if the third-party auditor or certification organization finds that the application does not meet one or more of the requirements of this part, the application must not be used to create, sign, transmit, or process electronic controlled substance prescriptions. The application provider must notify registrants within five business days of the issuance of the audit or certification report that they should not use the application for controlled substance prescriptions. The application provider must also notify the Administration of the adverse audit or certification report and provide the report to the Administration within one business day of issuance.

(h) For electronic prescription applications, the third-party auditor or certification organization must make the following determinations:

(1) If the information required in §1306.05(a) of this chapter, the indication that the prescription was signed as required by §1311.120(b)(17) or the digital signature created by the practitioner's private key, if transmitted, and the number of refills as required by §1306.22 of this chapter, cannot be consistently and accurately recorded, stored, and transmitted, the third-party auditor or certification organization must indicate that the application does not meet the requirements of this part.

(2) If other information required under this chapter cannot be consistently and accurately recorded, stored, and transmitted, the third-party auditor or certification organization must indicate that the application has failed to meet the requirements for the specific information and should not be used to create, sign, and transmit prescriptions that require the additional information.

(i) For pharmacy applications, the third-party auditor or certification organization must make the following determinations:

(1) If the information required in §1306.05(a) of this chapter, the indication that the prescription was signed as required by §1311.205(b)(6), and the number of refills as required by §1306.22 of this chapter, cannot be consistently and accurately imported, stored, and displayed, the third-party auditor or certification organization must indicate that the application does not meet the requirements of this part.

(2) If the pharmacy application accepts prescriptions with the practitioner's digital signature, the third-party auditor or certification organization must indicate that the application does not meet the requirements of this part if the application does not consistently and accurately import, store, and verify the digital signature.

(3) If other information required under this chapter cannot be consistently and accurately imported, stored, and displayed, the third-party auditor or certification organization must indicate that the application has failed to meet the requirements for the specific information and should not be used to

process electronic prescriptions that require the additional information.

§ 1311.302 Additional application provider requirements.

(a) If an application provider identifies or is made aware of any issue with its application that make the application non-compliant with the requirements of this part, the application provider must notify practitioners or pharmacies that use the application as soon as feasible, but no later than five business days after discovery, that the application should not be used to issue or process electronic controlled substance prescriptions.

(b) When providing practitioners or pharmacies with updates to any issue that makes the application non-compliant with the requirements of this part, the application provider must indicate that the updates must be installed before the practitioner or pharmacy may use the application to issue or process electronic controlled substance prescriptions.

§ 1311.305 Recordkeeping.

(a) If a prescription is created, signed, transmitted, and received electronically, all records related to that prescription must be retained electronically.

(b) Records required by this subpart must be maintained electronically for two years from the date of their creation or receipt. 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) Records regarding controlled substances prescriptions must be readily retrievable from all other records. Electronic records must be easily readable or easily rendered into a format that a person can read.

(d) Records required by this part must be made available to the Administration upon request.

(e) If an application service provider ceases to provide an electronic prescription application or an electronic pharmacy application or if a registrant ceases to use an application service provider, the application service provider must transfer any records subject to this part to the registrant in a format that the registrant's applications are capable of retrieving, displaying, and printing in a readable format.

(f) If a registrant changes application providers, the registrant must ensure that any records subject to this part are migrated to the new application or are stored in a format that can be retrieved, displayed, and printed in a readable format.

(g) If a registrant transfers its electronic prescription files to another registrant, both registrants must ensure that the records are migrated to the new application or are stored in a format that can be retrieved, displayed, and printed in a readable format.

(h) Digitally signed prescription records must be transferred or migrated with the digital signature.

PART 1312—IMPORTATION AND EXPORTATION OF CONTROLLED SUBSTANCES

Sec.