PART 1311—REQUIREMENTS FOR ELECTRONIC ORDERS AND PRESCRIPTIONS

Subpart A—General

Sec.
1311.01 Scope.
1311.02 Definitions.
1311.05 Standards for technologies for electronic transmission of orders.
1311.08 Incorporation by reference.

Subpart B—Obtaining and Using Digital Certificates for Electronic Orders

1311.10 Eligibility to obtain a CSOS digital certificate.
1311.15 Limitations on CSOS digital certificates.
1311.20 Coordinators for CSOS digital certificate holders.
1311.25 Requirements for obtaining a CSOS digital certificate.
1311.30 Requirements for storing and using a private key for digitally signing orders.
1311.35 Number of CSOS digital certificates needed.
1311.40 Renewal of CSOS digital certificates.
1311.45 Requirements for registrants that allow powers of attorney to obtain CSOS digital certificates under their DEA registration.
1311.50 Requirements for recipients of digitally signed orders.
1311.55 Requirements for systems used to process digitally signed orders.
1311.60 Recordkeeping.

Subpart C—Electronic Prescriptions

1311.100 General.
1311.102 Practitioner responsibilities.
1311.105 Requirements for obtaining an authentication credential—Individual practitioners.
1311.110 Requirements for obtaining an authentication credential—Individual practitioners eligible to use an electronic prescription application of an institutional practitioner.
1311.115 Additional requirements for two-factor authentication.
1311.116 Additional requirements for biometrics.
1311.120 Electronic prescription application requirements.
1311.125 Requirements for establishing logical access control—Individual practitioner.
1311.130 Requirements for establishing logical access control—Institutional practitioner.
1311.135 Requirements for creating a controlled substance prescription.
1311.140 Requirements for signing a controlled substance prescription.
1311.145 Digitally signing the prescription with the individual practitioner's private key.
1311.150 Additional requirements for internal application audits.
1311.170 Transmission requirements.
1311.200 Pharmacy responsibilities.
1311.205 Pharmacy application requirements.
1311.210 Archiving the initial record.
1311.215 Internal audit trail.
1311.300 Application provider requirements—Third-party audits or certifications.
1311.302 Additional application provider requirements.
1311.305 Recordkeeping.

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]