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 non-match 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