Guidelines for the Electronic Prescribing of Controlled Substances: Identity Proofing, Issuing Authentication Credentials, and Configuring Logical Access Controls

Prepared by

Sujansky & Associates, LLC

On behalf of
The California HealthCare Foundation

Nov. 24, 2013

Contents

1 Introduction and Purpose

This document is intended to serve as a companion guide for healthcare organizations that wish to comply with the *Interim Final Rule on Electronic Prescriptions for Controlled Substances* (IFR)[1]. The IFR is a federal regulatory document promulgated by the U.S. Drug Enforcement Agency (DEA) that defines the specific conditions under which healthcare providers may engage in the electronic prescribing of controlled substances (EPCS). These conditions include policies, processes, technologies, and documentation practices that provider organizations conducting EPCS must implement and adhere to.

The IFR is a lengthy and complex document that includes (implicitly and explicitly) a myriad of regulatory and technical concepts, many of which may be unfamiliar to physicians and administrators at provider organizations. The purpose of this companion guide is to help clarify certain key regulatory and technical requirements of the IFR for those physicians and administrators whom the DEA will ultimately hold responsible for compliance. These requirements covered in this document pertain specifically to the manner in which provider organizations procure two-factor authentication credentials and configure the access-control privileges for those who will engage in EPCS.

Section 2 of this document provides additional background about the intent of the IFR and several key regulatory and technical concepts that pertain to the subsequent discussion. Section 3 helps to clarify the portion of the IFR that governs the procurement of two-factor authentication credentials for those who will engage in EPCS. Section 4 helps to clarify the portion of the IFR that governs the configuration of access-control privileges for those who will engage in EPCS.

***Caveat*:** This document does not comprise and should not be interpreted as a legal opinion or legal advice. The contents of the document represent a best-faith effort to interpret the meaning of the IFR by lay persons qualified in the fields of health information technology and information security practices, but not in the law or government regulation. Provider organizations, physicians, or other readers who require definitive interpretations of the IFR are strongly encouraged to seek the opinion of qualified legal counsel.

2 Relevant Background

This section provides background regarding the intent of the IFR, as well as certain general terms and concepts that are fundamental to the IFR's requirements with respect to identity proofing and issuance of authentication credentials.

2.1 Intent of the IFR

The Controlled Substances Act of 1970 mandates the DEA to establish rigorous processes to control the dispensing of controlled substances and to deter the diversion of controlled substances to illegal purposes. To fulfill this mandate, the DEA published regulatory rules governing the actions of medical providers, drug manufacturers, and pharmacies. Until recently, these rules assumed that controlled substances would be prescribed and dispensed through a paper-based authorization process.

With the advent of electronic medical records, electronic prescribing systems, and electronic networks for the transmission of digital prescriptions, the prescribing and dispensing of medications may now be accomplished entirely through software systems, without any paper-based documentation. This new environment creates new threats for diversion of controlled substances, for example by unauthorized persons gaining access to electronic prescription applications or to electronic prescriptions themselves.

[1] 21 CFR Parts 1300, 1304, 1306, and 1311 (Federal Register, March 31, 2010). See http://www.gpo.gov/fdsys/pkg/FR-2010-03-31/pdf/2010-6687.pdf.

The intent of the IFR is to amend the existing DEA regulations to minimize the potential for such diversion, while allowing the electronic prescription of controlled substances to occur. The IFR attempts to accomplish this by imposing specific requirements on the processes and technologies used for EPCS, including the credentials that prescribers use to authenticate to EPCS systems and the controls implemented within EPCS systems to limit the users that may prescribe controlled substances.

2.2 Key Terminology

Section § 1300.03 of the IFR defines many terms used throughout the regulation, but omits or inadequately describes a number of terms that are key to clearly understanding all the IFR's requirements. Table 1 includes a supplemental set of definitions that helps readers to understand the meanings of many provisions in the IFR, including those related to procuring two-factor authentication credentials and configuring logical access controls.

Table 1. Supplemental definitions important for understanding the IFR.

Term	Definition
Institutional Practitioner	A hospital, clinic, or other organization *(*specifically *not* an individual) that is licensed, registered, or otherwise permitted, by the United States or the jurisdiction in which the organization practices, to dispense a controlled substance in the course of professional practice [2]. Note that *institutional practitioner* exclude pharmacies. In the context of the IFR, an *Institutional Practitioner* may perform certain security functions required for EPCS (such as identity proofing its own healthcare providers and issuing two-factor authentication credentials to them) if it meets certain additional criteria.
Individual Practitioner	A physician, dentist, veterinarian, or other individual person (specifically excluding a pharmacist) that is licensed, registered, or otherwise permitted, by the United States or the jurisdiction in which he/she practices, to dispense a controlled substance in the course of professional practice[2]. In the context of the IFR, an individual practitioner may work either at an institutional practitioner or in a (typically smaller) practice that lacks a dedicated department for medical credentialing and managing access to the computer system used for electronic prescribing. Note that the IFR uses the more general term "Practitioner" to refer to any healthcare provider who works either in a small-office practice or at an institutional practitioner and who might prescribe controlled substances.
Registrant	An individual or an organization (institution) that is formally registered with and authorized by the DEA to prescribe or dispense controlled substances, per the regulations and processes specified in the Controlled Substances Act of 1970. In the context of the IFR, an individual practitioner that has thus been registered is an *Individual Registrant*, and an institutional practitioner that has thus been registered is an *Institutional Registrant*.
Prescriber	An individual who is authorized to approve prescriptions for controlled substances to be transmitted to and dispensed by a pharmacy. In the context of the IFR, a *Prescriber* is the user of an electronic prescribing application who approves prescriptions for controlled substances via the specific technologies and processes specified by the rule (including the execution of a two-factor authentication protocol). The *Prescriber* is also the individual to whom the password and other credentials required for two-factor authentication are issued. Note that prescribers are usually *Individual Registrants*, although prescribers may be exempted from DEA registration if they work for an *Institutional Registrant* that authorizes their prescribing activity. Note also that the terms *Prescriber* and *Practitioner* (with no prefix) are often used interchangeably in the IFR.

[2] See http://www.deadiversion.usdoj.gov/21cfr/cfr/1300/1300_01.htm

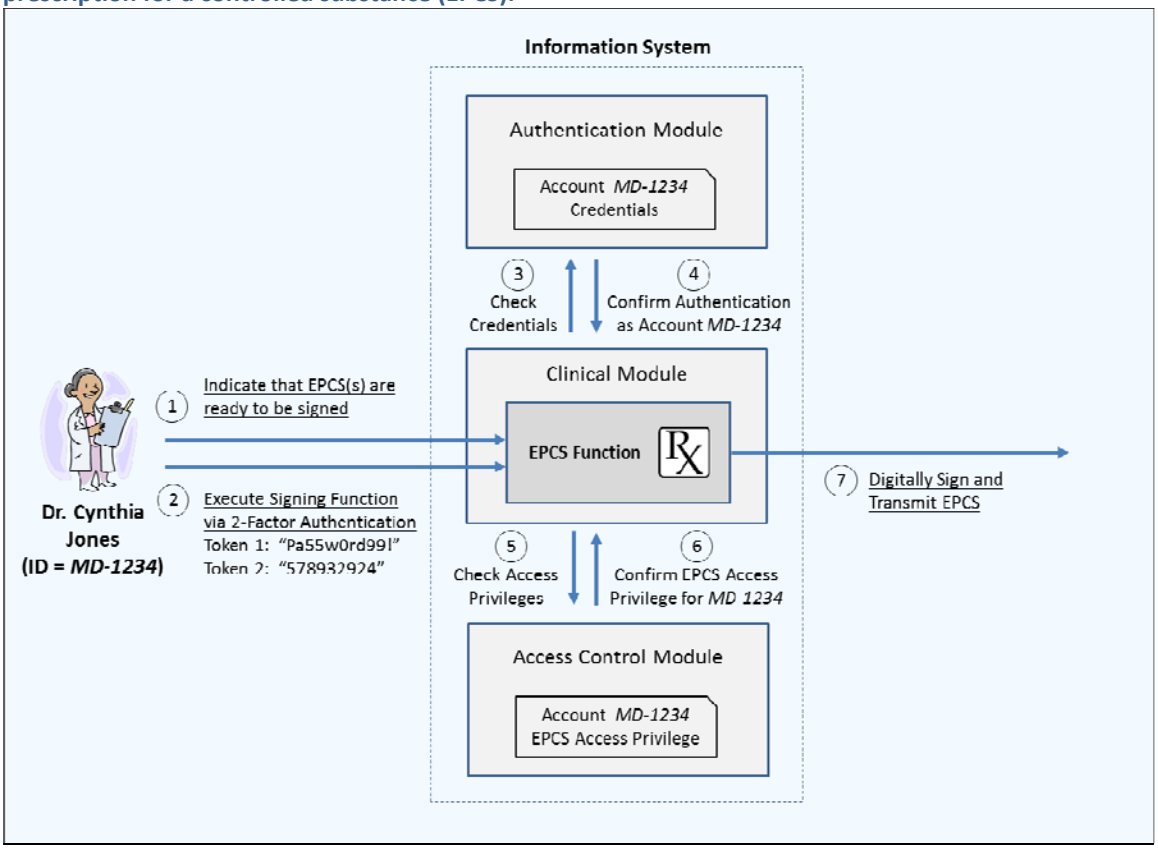
Two-factor authentication protocol	A process and set of related technologies via which the user of a computer application gains access to a specific user account (and to the functions granted to that account) by providing two separate forms of "proof" that the user owns the account. Although most computer applications, such as email or online banking, require only a password to access an account (one form of proof, or "factor"), the IFR requires an additional form of proof, such as possession of a hardware token or a biometric pattern that is uniquely associated with the account. Note that the process of *Two-factor authentication* by a user to gain access to an account is distinct from the processes of "identity proofing" and "access control" (see below).
Token	Something that a user possesses or controls (such as a key or password) that the user must demonstrate possession of to gain access to a specific account or specific function on a computer application. In the context of the IFR, two tokens (or "factors") are required to gain access to an account that allows the electronic prescribing of controlled substances.
Credential	In the context of the IFR, *Credential* is used synonymously with *Token*, as in "A practitioner who fails to [report a lost authentication token] may be held responsible for any controlled substance prescriptions written using his two-factor authentication credential." Note that *Credential*, in this sense, refers to a *security* credential, as distinct from the *medical* credentials of a healthcare provider (such as state licensure). The latter type of credentials is verified by an organization's "credentialing office" during the "credentialing process" for that provider.
Identity Proofing	The process of validating the identity of a potential user before he is granted an account or issued security credentials to access that account. *Identity Proofing* is critical to ensure that the person who is given the token(s) to access a computer account is, in fact, the person whom he claims to be, because that person will be formally associated with that account and any actions performed through that account will be ascribed to that person. *Identity proofing* prevents one person from impersonating another for purposes of accessing a computer system in the guise of that person. Note that *identity proofing* is different than *authentication*, which entails a person using the token(s) they've been given earlier to actually log into a computer system.
Access Control	*Access Control* entails limiting the specific set of functions that a particular computer account has access to, i.e. the functions that a user may perform after successfully logging into that account. *Access Control* allows different types of users of the same application to access different functions, depending on their job roles, level of authority, etc. *Access control* also allows the functions to which a user has access to change over time without requiring that the user be issued new authentication credentials. Access to specific functions may be assigned to individual user accounts, or it may be assigned to named groups of users or user roles, to which individual user accounts are then linked as appropriate.

Signing Function	The keystroke or other action used to indicate that the prescriber has authorized for transmission and dispensing a controlled substance prescription. In the context of the IFR, the *Signing Function* formally documents that a specific prescriber who was authorized to prescribe controlled substances and who authenticated his identity using a two-factor authentication protocol actually approved the prescription. Note that the *Signing Function* does not necessarily entail a "digital signature," *per* se, which involves a very specific type of digital encryption technology.
Digital Signature	The encryption of an electronic prescription after its approval and transmission in a manner that prevents the contents of the prescription and the identity of the prescriber from being later modified without authorization. Note that the *Digital Signature* of a prescription is distinct from the approval and authorization of that prescription (via the *Signing Function)*, which may precede its digital signing. The Signing function may use a different two-factor authentication methodology, and serves a different purpose with respect to securing electronic prescriptions for controlled substances.

2.3 Key Elements of the Required Two-Factor Authentication Process for EPCS

To understand the requirements of the IFR for procuring two-factor authentication credentials and configuring access controls for EPCS, it's useful to review the security procedures defined by the IFR for the signing of electronic prescriptions for controlled substances. Figure 1 shows schematically the steps required by the IFR for a prescriber to authorize such prescriptions and the technical mechanisms by which those steps are typically executed within a clinical information system.

Figure 1. Schematic of the technical steps required by the IFR for a prescriber to approve an electronic prescription for a controlled substance (EPCS).



Step 1: While using the clinical information system, a prescriber reviews one or more electronic prescriptions for controlled substances and indicates which ones are ready to be signed. All of these prescriptions must be for the same patient. After indicating the prescriptions' readiness, the prescriber is given the opportunity to electronically sign the prescriptions.

Step 2: The prescriber invokes a specific set of commands that comprise the EPCS *signing function*. This signing function must include a *two-factor authentication protocol*, i.e., the prescriber's entry of two separate authentication tokens. These tokens will typically comprise a memorized password, plus another token that is uniquely generated either by a hardware device issued to the prescriber (such as a smart card, USB device, or one-time-password device) or by a biometric characteristic of the prescriber herself (such as a fingerprint or retinal pattern).

Steps 3 and 4: The authentication module verifies that the authentication tokens the prescriber entered correspond to the credentials (tokens) associated with that prescriber's account. This correspondence was established at the time the credentials for that account were created and issued to the prescriber.

Steps 5 and 6: The access-control module verifies that the user account to which the prescriber authenticated via the two-factor protocol includes the *access privilege* for EPCS (i.e., is permitted by the information system's security controls to execute the signing function for controlled-substance prescriptions). The assignment of this access privilege was specified earlier by personnel who configure the logical access controls for user accounts on the clinical information system, based on authorization policies and processes.

Step 7: The signing function executes and the prescriptions are digitally signed and electronically transmitted to a dispensing pharmacy.

Note that steps 5 and 6 could precede steps 3 and 4, i.e., the information system could first check whether the prescriber had the required access controls to prescribe controlled substances and then confirm the prescriber's two-factor authentication credentials only if she did. The IFR does not prescribe a specific sequence, as long as both types of verification are required to sign EPCSs.

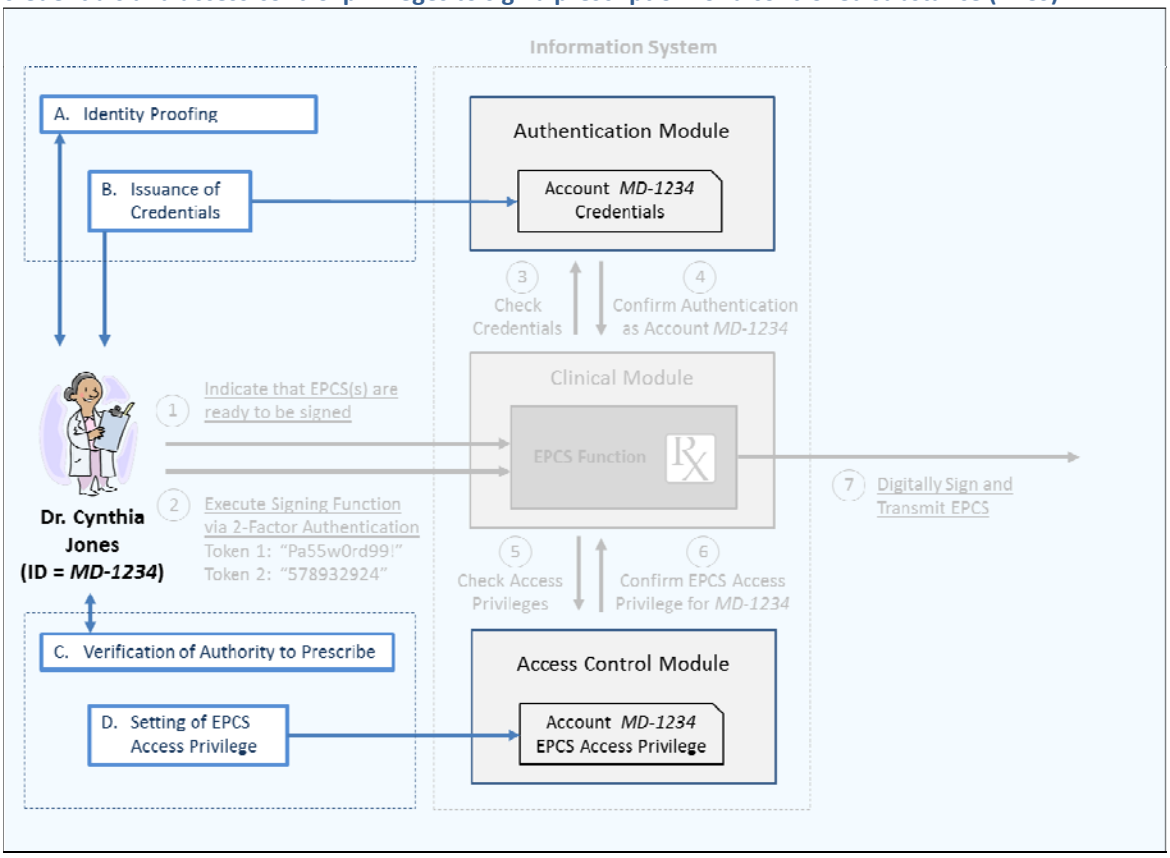
Using the example practitioner shown in Figure 1, these steps are intended to ensure that

(1) Only the real Dr. Cynthia Jones can access the computer account of Dr. Cynthia Jones (by forcing users to authenticate in a rigorous way)

(2) The computer account of Dr. Cynthia Jones includes the ability to sign prescriptions for controlled substances only if Dr. Cynthia Jones is authorized to prescribe controlled substances (by explicitly granting the EPCS signing privilege only to certain accounts)

Building on the definitions in Table 1 and the steps illustrated in Figure 1, Figure 2 illustrates the processes required by the IFR for procuring two-factor authentication credentials and configuring access controls for EPCS. The illustration and description of these processes is intended to summarize how they fit into the IFR's model for authorizing EPCSs in a manner that minimizes the risk of diversion.

Figure 2. Schematic illustrating the processes required for practitioners to gain the authentication credentials and access-control privileges to sign a prescription for a controlled substance (EPCS).



A. Identity Proofing

In general, identity proofing is the process for verifying that a person is who she claims to be. In the context of the IFR, identity proofing is the process for verifying that a person to whom two-factor authentication credentials will be issued for the electronic prescribing of controlled substances is the person she claims to be and (in certain cases – see Section 3.2.1) to also verify that this person is a licensed provider who is authorized to prescribe controlled substances. This step must be rigorously performed (e.g., involving official identification credentials issued by a trusted third party, such as the DMV or U.S. State Department), to avoid allowing a person not authorized for EPCS to gain access to the user account of a person who is authorized for EPCS, and thereby to prescribe controlled substances inappropriately in the guise of that person (i.e., to "impersonate" an authorized prescriber).

In general, identity proofing may be conducted in person (e.g., by a person presenting official identification credentials, a signature, and/or a fingerprint before a notary). Alternatively, identity proofing may be conducted remotely (e.g., by a person providing certain confidential information likely to be known only to that person via the internet, phone, or mail).

B. Issuance of Credentials

In general, "credentials" comprise a set of authentication tokens that are associated with a specific user account and that grant the possessor of the tokens access to that account or to specific functions of that

account. In the context of the IFR, credentials comprise the two-factor authentication tokens that are required to gain access to the signing function for electronic prescribing of controlled substances.

After identity proofing of a person is successfully performed, the credentials associated with that person's user account must be securely generated and securely delivered to the person (i.e., in a manner such that no interloper can gain possession of the credentials and, again, access that person's user account in her guise).

C. Verification of Authority to Prescribe

The identity proofing of a healthcare provider and the secure issuance of two-factor authentication credentials to that provider are sufficient to ensure that only that person can access the computer account that has been created for her. However, these steps are not sufficient, in the context of the IFR, to ensure that the healthcare provider is authorized to prescribe controlled substances using that computer account or any other means. The IFR requires a separate step that provider organizations must take to verify that every provider whose computer account will allow the electronic prescribing of controlled substances is, in fact, authorized to prescribe controlled substances.

D. Setting of EPCS Access Privileges

Once a provider organization has verified a practitioner's authority to prescribe controlled substances, the organization may configure the practitioner's computer account to allow the electronic prescribing of controlled substances. This step is done by setting the appropriate "access control" privileges for that account, a technical process that, itself, must be performed in a secure manner by designated and trusted personnel. In the context of the IFR, the setting of this access control requires the collective action of two separate individuals, to minimize the risk that an unauthorized practitioner's account will be inappropriately granted the ability to prescribe controlled substances (through accident or intent).

Using the example practitioner shown in Figure 2, these processes are intended to ensure that

(3) The real Dr. Cynthia Jones and only the real Dr. Cynthia Jones is provided the two-factor authentication credentials needed to access the computer account of Dr. Cynthia Jones,

(4) The real Dr. Cynthia Jones is authorized to prescribe controlled substances,

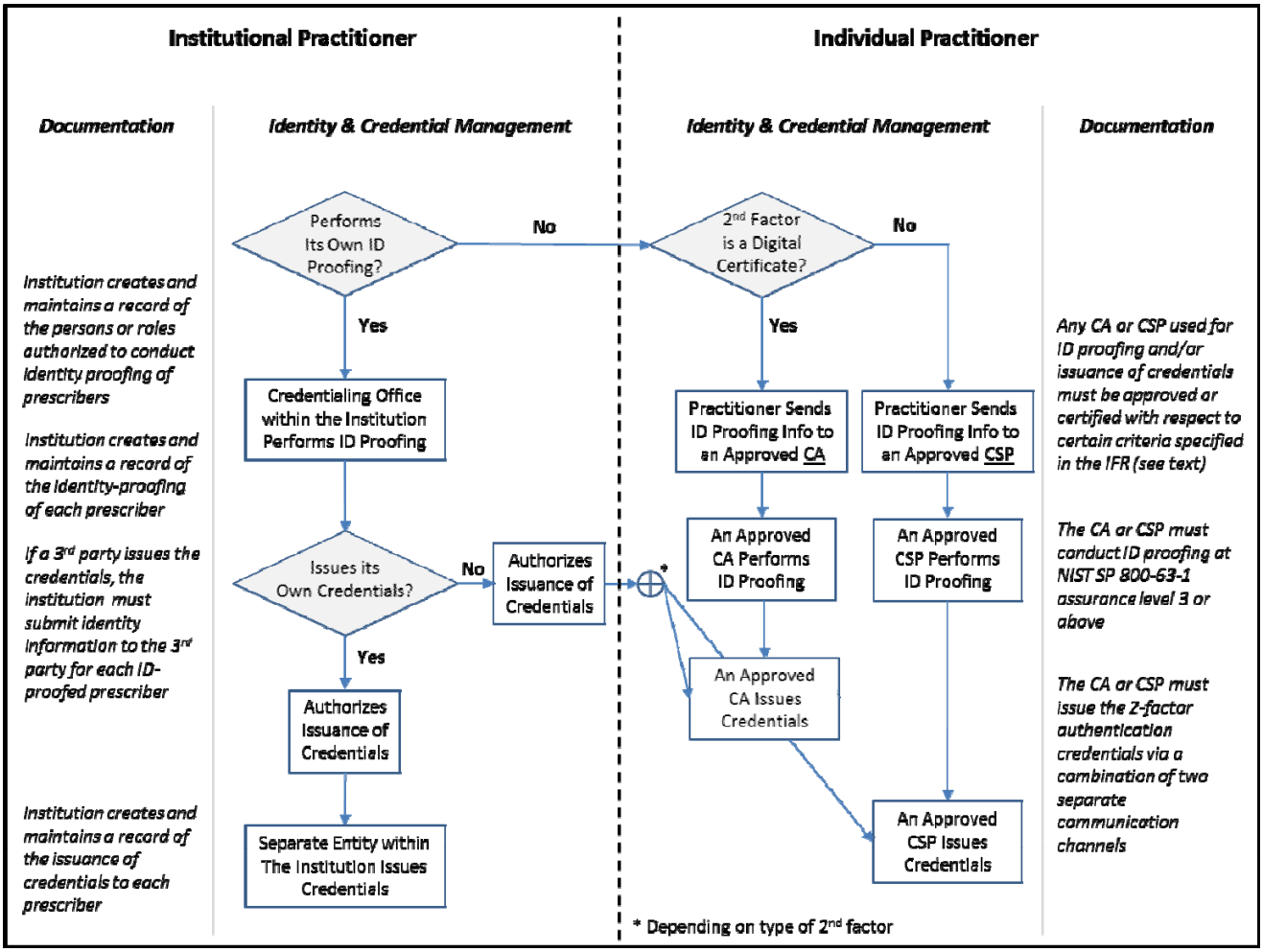
(5) Dr. Cynthia Jones' computer account is granted access to the signing function for EPCS, and

(6) The user accounts of persons NOT authorized to prescribe controlled substances are not granted access to the signing function for EPCS.

3 Providing Credentials for Two-Factor Authentication

The IFR provides several options for practitioners to obtain two-factor authentication credentials for EPCS, depending on the type of organization they practice in and the type of two-factor credentials they intend to use. Figure 3 illustrates the options and sequential steps involved in obtaining such credentials. As described in Sec. 2.3, the process in all cases involves the initial identity proofing of a practitioner, followed by the issuance of appropriate two-factor authentication credentials to that practitioner.

Figure 3. Schematic of options, steps, and documentation requirements for identity proofing and issuance of two-factor authentication credentials for EPCS.



3.1 Individual Practitioners

Individual Practitioners who are DEA registrants and who do not work within organizations that are institutional practitioners (per the definitions of these terms in Sec. 2.2) must use the services of a 3rd-party Certificate Authority (CA) or Credential Services Provider (CSP) to verify their identities and to issue their two-factor authentication credentials for purposes of EPCS.

The determination of whether a CA or a CSP should perform these functions depends on the kind of two-factor authentication credentials that the practitioners will use.

If the credentials involve the use of a X509 digital certificate and the public key infrastructure (PKI), then the identity proofing must be done and the credential issued by a CA.

If the credentials involve the use of authentication tokens other than X509 digital certificates (such as one-time password tokens, smart cards, or biometric attributes), then the identity proofing must be done and the credential issued by a CSP.

3.1.1 Identity Proofing

For individual practitioners, identity proofing for EPCS must be conducted by a federally approved CA or CSP at NIST SP 800-63-1 Assurance Level 3 or above[3] [IFR p. 16242]. In general, these requirements allow identity proofing to be conducted either in person or remotely (i.e., via internet, telephone, or U.S. mail). The specific policies of the CA or CSP will determine which identifying information must be provided by the practitioner and how the identity proofing will be specifically performed. Hence, individual practitioners may "follow the lead" of their CA or CSP, as long as the CA or CSP is aware of the specific requirements of the IFR to identity proof at NIST SP 800-63-1 Assurance Level 3 or above.

3.1.2 Issuance of Credentials

For individual practitioners, the issuance of two-factor authentication credentials must be done by a federally approved CA or CSP. Specifically, if a CA is used, it must be cross certified with the Federal Bridge Certification Authority (FBCA) and operate at a FBCA "basic" assurance level or above [IFR § 1311.105(a)(1)]. A list of such CAs may be found at http://www.idmanagement.gov/entities-cross-certified-federal-bridge.

If a CSP is used, it must meet the requirements of the NIST Electronic Authentication Guideline, Assurance Level 3 or above for identity proofing (NIST Special Publication 800–63–1) [IFR § 1311.105(a)(2)].

Note: For individual practitioners, identity proofing and the issuance of credentials are part of a single process performed by a single CA or CSP. For practitioners working at institutional providers (see below), identity proofing and the issuance of credentials may be divided into separate processes performed by separate organizations.

The IFR provides little direction regarding the exact processes that must be followed for the issuance of credentials to individual providers, deferring to the cited security guidelines and assurance levels. However, the IFR does specify the following:

- The type of two-factor credential (or token) issued by the institutional practitioner for EPCS must conform to the requirements for a "hard token" or biometric credential, as specified in IFR § 1311.115, § 1311.116, and p. 16242.
- The authentication credentials must be issued/delivered to the recipient via two channels (e.g., e-mail, mail, or telephone call). For example, a hard token could be surface mailed to the recipient's mailing address of record, and then receipt of the token confirmed by a telephone call from the recipient's phone number of record. Alternatively, a hard token could be surface mailed to the recipient's mailing address of record and a password required to use the hard token could be subsequently emailed to the recipient's email address of record.

3.2 Prescribers Working within Institutional Practitioners

Prescribers who work within organizations that are institutional practitioners may have their identities proofed and/or their two-factor authentication credentials issued directly by their organizations rather than by a third party CA or CSP. To qualify for performing identity proofing directly, the prescriber's organization must:

1. Be a DEA registrant (i.e., an *Institutional Registrant*) [IFR, p. 16246]

[3] See http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

2. Have an entity or department within the organization that grants individual practitioners privileges to practice at that organization (such as the medical credentialing office at a hospital) [IFR, § 1311.110(a)]

To qualify for performing the issuance of credentials directly, the prescriber's organization must:

1. Have secure processes in place for the creation and delivery of the types of two-factor authentication credentials required, as specified in IFR § 1311.115, § 1311.116, and p. 16242.
2. Have the ability to configure the authentication module of its information system to correctly associate the credentials it generates with the corresponding practitioners' accounts (this requirement is not explicitly specified in the IFR, but follows from the way that two-factor authentication credentials work).

If an organization does not meet these requirements, the prescribers working at the organization who wish to engage in EPCS *must* have their identities proofed and/or their credentials issued by a 3rd party, as described in Sec. 3.1.

If an organization does meet these requirements, but prefers not to perform identity proofing and/or the issuance of two-factor authentication credentials for EPCS, the individual practitioners working at the organization *may* have their identities proofed and/or their credentials issued by a 3rd-party (as described in Sec. 3.1) rather than the organization.

If an organization meets these requirements and has the ability and desire to perform identity proofing and the issuance of two-factor authentication credentials for EPCS, it may perform these functions itself, provided it does so in compliance with the specific requirements indicated in the IFR and summarized below.

Lastly, there also exists a "hybrid" option, whereby a qualified organizations may perform identity proofing itself, but outsource the issuance of two-factor authentication credentials to a 3rd-party, provided that the organization communicates the results of the identity proofing to the 3rd party in an approved manner, as described below.

3.2.1 Identity Proofing

When an institutional practitioner, itself, performs identity proofing for EPCS, it must conform to certain specific requirements, as specified in § 1311.110 of the IFR. Organizations should review these requirements carefully, but notable points include:

- Identity proofing may only be done by persons authorized in writing by the institutional practitioner to perform this function [IFR, § 1311.130(c)]. Institutional practitioners may designate individual persons to perform identity proofing or they may designate job roles within the organization (such as "credentialing manager"), which may be filled by different persons at different times.
  Note: The persons who conduct identity proofing within an institutional practitioner do not need to be DEA registrants.
- The persons or roles designated to perform identity proofing must be associated with the entity or department at the institutional practitioner that grants individual practitioners privileges to practice at that organization (e.g., the medical credentialing office at a hospital). [IFR, § 1311.110(a)]
- Identity proofing must be done in person, and cannot be done remotely [IFR, p. 16246].

- Identity proofing must include the physical matching of the practitioner to an official photographic identification issued by the Federal or State government (such as a driver's license of passport). [IFR, § 1311.110(a)(1)]
- The process must include verification that the practitioner is authorized to practice in the state where the EPCS software will be used (such as a state medical license or other state certification/accreditation/licensure for health care providers), and that the practitioner is authorized by the state where the EPCS software will be used to prescribe controlled substances, if such state authorization is required [IFR, § 1311.110(a)(2)].
- The process must include verification that the practitioner is authorized by the DEA to prescribe controlled substances (either under his/her own DEA registration number or the institutional practitioner's DEA registration number, if applicable). [IFR, § 1311.110(a)(3)]
- The organization must document and retain a record of the identity-proofing process [IFR, § 1311.110(e)]. Although the IFR does not specify the exact form or contents of such documentation, it should reasonably include:
    - The identity of the person(s) who performed the identity proofing and their signatures attesting to the validity of the process.
    - The date that the identity proofing was conducted
    - The form of photographic identification used to verify the identity of the prescriber, including the type of identification, the issuing authority, any unique identification numbers (such as a passport number), and (preferably) photocopies of the physical identification document.
    - The type of state licensure or other state certification that was verified, any unique identification numbers for this licensure, and the means by which the current validity of the licensure was verified (e.g., confirmatory documents, conversations, emails, etc.). Copies of any relevant documents are also preferred.
    - The practitioner's DEA registration number (if the practitioner will conduct EPCS under that number), or the institutional practitioner's DEA registration number (if the practitioner will conduct EPCS under that number) along with attestation by the institutional practitioner that it authorizes such use of its DEA registration.
- **NOTE:** The IFR does not require institutional practitioners to meet the requirements of NIST SP 800–63–1 for identity proofing [IFR, p. 16246]. This requirement only applies when 3rd parties conduct the identity proofing of individual practitioners.

3.2.2 Issuance of Credentials

In general, the issuance of two-factor authentication credentials for EPCS at an institutional practitioner entails five steps:

1. The preparation by the institutional practitioner of an approved list of prescribers to whom such credentials should be issued, including their identifying information and contact information
2. The communication of this list to the entity that will create the credentials and that will deliver the credentials to the respective prescribers.
3. The creation by this entity of two-factor credentials specific to each approved prescriber
4. The secure delivery of the credentials to the respective prescribers

5. The association of the credentials with the respective prescribers' accounts in the clinical information system, so that presentation of the credentials by a prescriber when logging in will provide access to that prescriber's account and only that prescriber's account.

Third-Party Issuance of Credentials

An institutional practitioner that has conducted its own identity proofing may "outsource" the issuance of two-factor authentication credentials to a third party, such as a CA or CSP. When this is done, the CA or CSP must issue the credentials in the same manner as described in Sec. 3.1.2. The hand-off of information between the institutional practitioner and the third party, however, must be done in a specific manner prescribed by the IFR ((§ 1311.110(b), (c), and (e)) and elsewhere). Organizations should review these requirements carefully, but notable points include:

- An institutional practitioner may only use a "federally approved" entity to issue two-factor authentication credentials for EPCS, i.e. either (1) a CA that is cross certified with the Federal Bridge certification authority and that operates at a Federal Bridge Certification Authority basic assurance level or above OR (2) a CSP that meets the requirements of Assurance Level 3 or above for identity proofing, as specified in NIST SP 800–63–1 [IFR ((§ 1311.105(a)(1) and (a)(2)].
- If a two-factor authentication credential entails the issuance of a digital certificate, the institutional practitioner must use a federally approved CA. If another type of two-factor authentication credential is used, the institutional practitioner must use a federally approved CSP.
- When institutional practitioners perform identity proofing in-house and then outsource the issuance of credentials to a CA or CSP, the institutional practitioner is acting as a "trusted agent" on behalf of the CA or CSP (see IFR § 1311 DEFINITIONS and pp. 16242 and 16246).
  Note: In this case, the CA or CSP must still conform to the requirements of NIST SP 800–63–1 Assurance Level 3 for identity proofing, although the institutional practitioner will be its "trusted agent" in performing the identity proofing.
- The institutional practitioner must meet any requirements that the CA or CSP imposes on entities that serve as its trusted agents regarding the specific manner in which the institutional practitioner submits identity proofing information to the CA or CSP [§ 1311.105(b)].
  Note: These requirements of CAs and CSPs may vary and are not specified by the IFR. Institutional practitioners should check with any CA or CSP that they are considering using for details.

"In-House" Issuance of Credentials

An institutional practitioner that has conducted its own identity proofing may also create and issue two-factor authentication credentials itself. The IFR provides very little direction or requirements for this process, however (unlike for the issuance of authentication credentials by a CA or CSP). All that may be gleaned from the IFR are the following requirements:

- The type of two-factor credential (or token) issued by the institutional practitioner for EPCS must conform to the requirements for a "hard token" or biometric credential, as specified in IFR § 1311.115, § 1311.116, and p. 16242.
- An institutional practitioner that issues its own two-factor authentication credentials for EPCS must retain a record of the issuance of the credential. [IFR § 1311.105(3)]. The specific contents of such a record are not specified in the IFR, but should presumably include:
  - Who issued the credentials and when

- How the credentials were delivered to the prescriber, and whether/how/when the prescriber securely acknowledged receipt and activation of the credentials (for example, by placing a phone call from a registered phone number).
- How and by whom the credentials were configured to provide access to the prescriber's user account.

However, it may be safest for institutional practitioners to assume that the process for issuing two-factor authentication credentials by institutional practitioners should parallel those required for CAs and CSPs, as specified in IFR § 1311.105(c) and p. 16242, as well as NIST SP 800–63–1 (particularly Sec. 5.3.1, Assurance Level 3). Specifically, these requirements include:

- The authentication credentials must be issued/delivered to the recipient via two channels (e.g., e-mail, mail, or telephone call). For example, a hard token could be surface mailed to the recipient's mailing address of record, and then receipt of the token confirmed by the appropriate recipient via a telephone call from the recipient's phone number of record. Alternatively, a hard token could be surface mailed to the recipient's mailing address of record and a password required to use the hard token could be emailed to the recipient's email address of record.

4 Setting Access Controls for EPCS

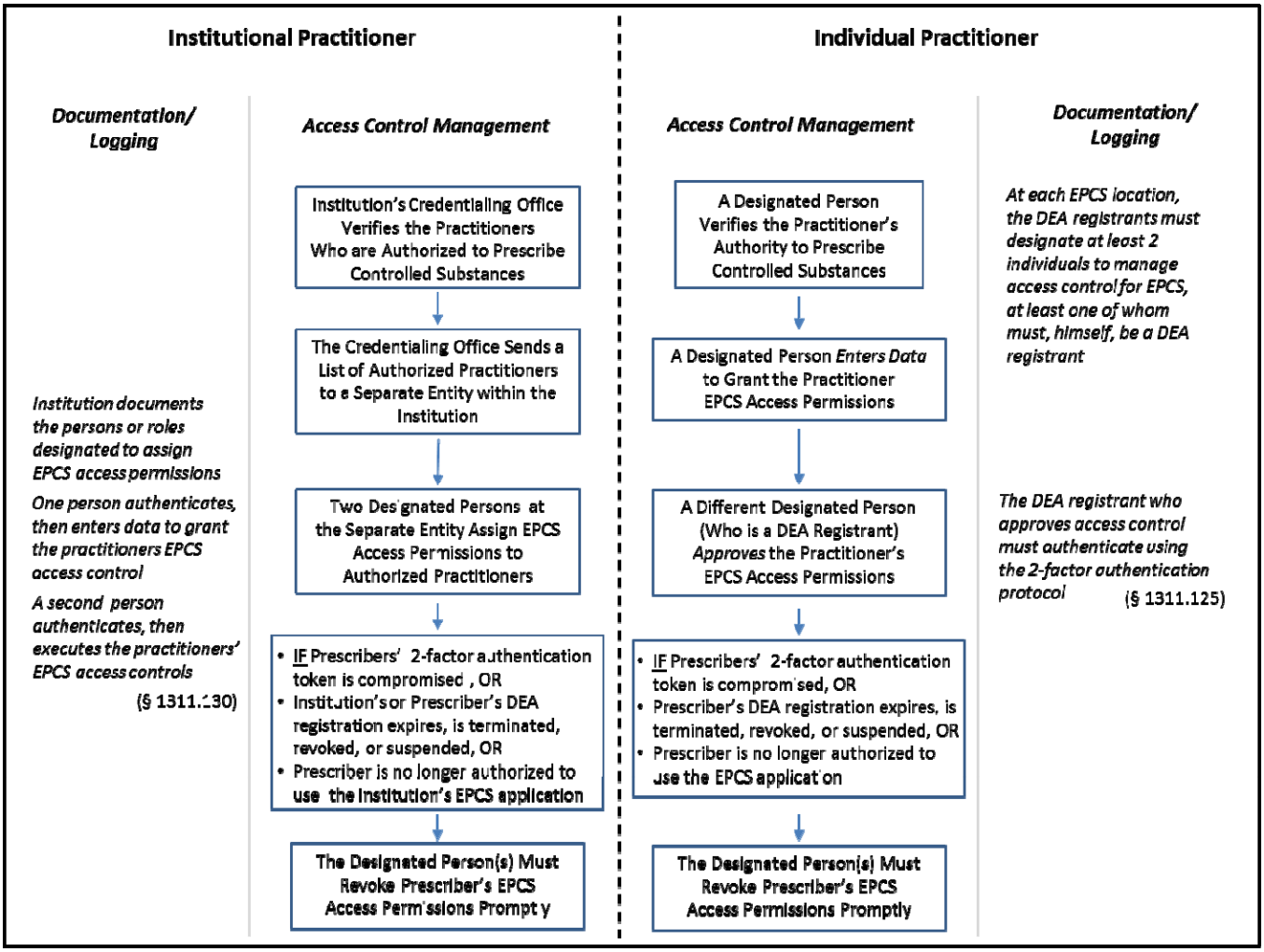
Rigorous identity proofing and issuance of two-factor authentication credentials are not sufficient to ensure that only authorized practitioners can electronically prescribe controlled substances. The IFR additionally requires that *logical access controls* allowing practitioners to approve and sign EPCSs be explicitly assigned to the user accounts of authorized practitioners. The IFR also requires that such access controls be explicitly and promptly revoked for the user accounts of practitioners who lose their authorization to prescribe controlled substances.

Logical access controls are security settings specified in an information system that determine which specific functions of the system a particular user may access. For example, logical access controls in an EHR may allow clerical users to view patients' progress notes, but only allow physicians or nurses to create or update such notes. In general, access to specific functions may be assigned to *individual user accounts* (such as "MD-1234" for Dr. Jones), or they may be assigned to *user roles* (such as "physician," "nurse," "medical assistant," or "billing clerk"), such that any individual user account later assigned that role can automatically access the function.

In the context of the IFR, the relevant system functions for EPCS are the ability to (1) indicate that electronic prescriptions for controlled substances are ready to be signed and (2) electronically sign prescriptions for controlled substances. Per the IFR, access to those two functions must be limited via logical access controls to authorized prescribers only, and the means by which the recipients of such access are determined and the access itself granted must comply with certain specific procedures. § 1311.125 and § 1311.130 of the IFR describe these procedures in detail. Sec. 4 of this document highlights and clarifies the key elements of the procedures.

As with the procedures for identity proofing and issuing authentication credentials, the procedures for setting logical access controls differ depending on whether an institutional practitioner is setting these access controls for its member practitioners or a group of individual practitioners is setting logical access controls for itself. Figure 4 graphically summarizes the required procedures in each case, and the following sections provide further details.

Figure 4. Schematic of steps and related documentation required for setting logical access controls for EPCS.



4.1 Individual Practitioners

For Individual Practitioners who are DEA registrants and who do not work within organizations that are institutional practitioners, the process for setting access controls for EPCS involves four sequential steps:

1. Designate the personnel allowed to manage access controls for EPCS
2. Verify each practitioner's authority to prescribe
3. Grant the practitioner's account access to EPCS functions
4. Promptly revoke the practitioner's access to EPCS functions if necessary

4.1.1 Designate the Personnel Allowed to Manage Access Controls for EPCS

At each location or facility where EPCS will be conducted, the individual practitioners at the facility must collectively designate and document the specific persons who are authorized to manage access controls for EPCS. At least two such persons must be designated. [IFR § 1311.125(a)]

- Although the IFR does not specify how such designations should be documented, it is presumably sufficient to maintain a paper record containing a list of the designated individuals, the date(s) on which the individuals were designated, and the name, signature, and DEA registration number of at least one DEA registrant at the facility who authorized the designations.
- At least one of these designated persons must be an individual DEA registrant who is authorized to prescribe controlled substance and has been issued two-factor authentication credentials for a user account that allows managing access controls for the facility's information system. At least one other of these persons must also have a user account that allows managing access controls for the facility's information system, although they need not be a DEA registrant nor have two-factor authentication credentials.
- **Note:** The designated DEA registrant need not already have logical access controls that enable EPCS. If such a requirement were in place, it would not be possible for the *first* practitioner at any facility to get such access controls, because no other practitioner would yet be qualified to grant such controls per the procedures below.

4.1.2 Verify each Practitioner's Authority to Prescribe

For each practitioner being granted logical access control to sign electronic prescriptions for controlled substances, at least one of the designated individuals must verify that:

1. the practitioner's DEA registration is current and in good standing, and
2. the practitioner's State authorization to practice (such as state medical license) is current and in good standing, and
3. the practitioner's State authorization to dispense controlled substances is current and in good standing (if the practitioner's state requires such authorization) [IFR § 1311.125(b)].

Note: In small practices, this verification may require nothing more than checking expiration dates on the practitioners' DEA Certificate of Registration and State license, unless there is reason to question the current validity of either [per IFR, p. 16248].

Note: The validity of DEA registrations may be checked online at DEA's Web site at https://www.deadiversion.usdoj.gov/webforms/validateLogin.jsp.

Note: Verification of a practitioner's authority to prescribe need not be done by another DEA registrant – any designated person may perform this step. However, if the DEA web site is used to validate a DEA registration, this may only be done by another DEA registrant, as only DEA registrants may log into the validation site.

4.1.3 Grant the Practitioner's Account Access to EPCS Functions

The action of granting a practitioner access control to sign electronic prescriptions must be performed by two separate persons and both must be among those designated by the DEA registrants to manage access control at the facility [IFR § 1311.125(c)]. More specifically:

- Both persons must log in (authenticate) to the information system that is used for managing access to EPCS functions. For example, both persons must have administrative privileges on the facility's EHR that allow them to manage other users' access controls.
- One person must specify which practitioner's account should be granted access to the EPCS signing function, for example by referencing that user's account and clicking a check box that indicates the EPCS signing function is allowed for that account. This person need not be a DEA

registrant, or even an employee of the practice, nor must this person authenticate to the information system using two-factor authentication. For example, an office manager or part-time I.T. consultant could perform this function.

- The other person must explicitly approve the granting of the EPCS signing function to the specified practitioner. The IFR does not specify how such approval is executed, but it is presumably done by also referencing the practitioner's user account and executing a different action (such as clicking a different check box) than that used in the step above.
- **Note:** This second person must be an individual DEA registrant and must have authenticated to the information system using a two-factor authentication protocol. Although the IFR does not specifically stipulate that this registrant's two-factor authentication credential must have been issued per the process specified in Section 3, this is presumably the intent of the IFR.
- **Note:** The processes required for granting individual practitioners' logical access control for EPCS assume that the practitioners' information system support these specific processes. Presumably, all information systems certified to be compliant with the IFR do support these processes, but practitioners are advised to confirm this functionality.

4.1.4 Promptly Revoke the Practitioner's Access to EPCS Functions if Necessary

In certain situations, the logical access controls that enable a practitioner to use the EPCS signing function must be revoked (i.e., disabled) [IFR § 1311.125(d)]. This is the case if

1. the prescriber's two-factor authentication token is lost, stolen, or compromised (e.g., secret information from the token is copied), OR
2. the prescriber's individual DEA registration expires and has not been renewed, OR
3. the prescriber's individual DEA registration is terminated or revoked, OR
4. the prescriber is no longer authorized to use the facility's EPCS application (e.g., the prescriber leaves the medical practice).

If any of these situations occur, two of the persons designated at the facility to manage access controls must disable the prescriber's access to the EPCS signing function. As with the granting of access controls, one of these persons must specify which practitioner's account should have its signing privileges disabled, and the other person (a DEA registrant who logs into the system via two-factor authentication) must approve the revocation of the privileges [IFR p. 16248].

Note: If the prescriber's two-factor authentication token is lost, stolen, or compromised, the logical access control must be disabled *immediately* after the prescriber notifies the designated persons at the practice. Otherwise, the logical access control must be disabled the *same day* as the prescriber's DEA registration is discovered to be invalid or the prescriber loses authority to use the facility's EPCS application.

4.2 Prescribers Working within Institutional Practitioners

For institutional practitioners who manage access to an EPCS application on behalf of their prescribers, the process for setting access controls for EPCS involves a somewhat different sequence of steps:

1. Designate the personnel allowed to manage access controls for EPCS
2. Provide these personnel a list of practitioners authorized to access the EPCS signing function
3. Grant the practitioner's account access to EPCS functions

4. Promptly revoke the practitioner's access to EPCS functions if necessary

4.2.1 Designate the Personnel Allowed to Manage Access Controls for EPCS

The institutional practitioner must designate and document at least two persons who are authorized to manage access controls for EPCS [IFR § 1311.130(b)].

- These persons must work within a department or entity other than that which conducts the identity proofing of practitioners for EPCS (see Section 3.1.1). For example, identity proofing may be done by persons in the medical credentialing office, and the management of access controls may be done by persons in the I.T. department.
- Although the IFR does not specify how such designations should be documented, it is presumably sufficient to maintain a paper record containing a list of the designated individuals or roles, the date(s) on which the individuals or roles were designated, and the name and signature of the representative of the institutional practitioner who authorized the designations.
- **Note:** The institutional practitioner may designate two or more *individual persons* to have this authority, or it may designate a functional *role* filled by at least two individual persons.
- **Note:** None of the persons designated to manage access controls needs to be an individual DEA registrant nor have two-factor authentication credentials. All of the persons, however, must have user accounts that allow them to manage access controls for the institutional practitioner's information system.

4.2.2 Provide a List of Practitioners Authorized to Access the EPCS Signing Function

The entity or department within an institutional practitioner that conducts the identity proofing of practitioners for EPCS (see Section 3.1.1) must also develop a list of individual practitioners who are authorized to use the signing function of the institutional practitioner's electronic prescription application. This list must be approved by two individuals. [IFR § 1311.130(a) and (c)].

- Although the IFR does not specify how this list should be documented, it is presumably sufficient to maintain a paper record containing a list of the authorized practitioners, as well as the names and signatures of the two individuals who approved the list and the date it was approved.
- The IFR also does not specify how the list should be sent or communicated to the persons who manage access controls, but presumably it is sufficient to transmit the list in the same manner as other legal documents (i.e., in paper or electronic form).
- **Note:** Neither of the individuals who approve the list needs to be a DEA registrant.
- **Note:** Verification of each practitioner's authority to prescribe controlled substances was already performed at the time the practitioner was identity proofed and granted authentication credentials, so it is not necessary to verify such authority again during the process of generating the list described here.

4.2.3 Grant the Practitioner's Account Access to EPCS Functions

The action of granting a practitioner access control to sign electronic prescriptions must be performed by two separate persons and both must be among those designated by the institutional practitioner for this function [IFR § 1311.130(b)]. The action must specifically entail:

- Both persons must log in (authenticate) to the information system that is used for managing access to EPCS functions. For example, both persons must have administrative privileges on the facility's EHR that allow them to manage other users' access controls.

- One person must specify which practitioner's account should be granted access to the EPCS signing function, for example by referencing that user's account and clicking a check box that indicates the EPCS signing function is allowed for that account.
- The other person must explicitly approve the granting of the EPCS signing function to the specified practitioner. The IFR does not specify how such approval is executed, but it is presumably done by also referencing the practitioner's user account and executing a different action (such as clicking a different check box) than that used in the step above.
- **Note:** Neither of the persons who perform this action for an institutional practitioner needs to be a DEA registrant nor log into the application using two-factor authentication credentials.
- **Note:** The processes required for granting practitioners' logical access control for EPCS assume that the institutional practitioner's information system supports these specific processes. Presumably, all information systems certified to be compliant with the IFR do support these processes, but institutional practitioners are advised to confirm this functionality.

4.2.4 Promptly Revoke the Practitioner's Access to EPCS Functions if Necessary

In certain situations, the logical access controls that enable a practitioner to use the EPCS signing function must be revoked (i.e., disabled) [IFR § 1311.130(d)]. At institutional practitioners, this is the case if

1. A prescriber's two-factor authentication token is lost, stolen, or compromised (e.g., secret information from the token is copied), OR
2. the institutional practitioner's or the individual practitioner's DEA registration expires and has not been renewed, OR
3. the institutional practitioner's or the individual practitioner's DEA registration is terminated or revoked, OR
4. the prescriber is no longer authorized to use the institutional practitioner's EPCS application (e.g., the prescriber no longer practices at the institutional practitioner).

If any of these situations occur, the persons designated by the institutional practitioner to manage access controls must disable the prescriber's access to the EPCS signing function. Although the IFR does not explicitly require that two persons revoke the prescriber's access when these situations occur at an institutional practitioner, this is likely the intent of the IFR, as two persons are required to revoke access for individual practitioners, as described above [IFR p. 16248].

Note: If the prescriber's two-factor authentication token is lost, stolen, or compromised, the logical access control must be disabled *immediately* after the prescriber notifies the designated persons at the practice. Otherwise, the logical access control must be disabled the *same day* as the relevant DEA registration is discovered to be invalid or the prescriber loses authority to use the institutional practitioner's EPCS application.