# Electronic Controlled Substance Practitioner Responsibilities

Transmission and Receipt of Electronic Controlled

Substance Prescriptions

**21 CFR 1311 Practitioner Responsibilities**

Pursuant to DEA Interim Final Rule (IFR): Electronic Prescriptions for Controlled Substances

As a Provider, participation in electronically prescribing of controlled substance is dependent on State regulations and the participating pharmacies capabilities. Although, at the time of this document, 80% of States accept EPCS, 4 States have mandated that all controlled substances be submitted electronically, or penalties could occur.

Electronic prescriptions for Schedule II-V controlled substances must meet DEA regulatory requirements.

Audit and Selection of Software Application(s)  Before being used to create, sign, transmit, or process controlled substance prescriptions, electronic prescribing applications or pharmacy applications (stand-alone or integrated Electronic Medical Record (EMR) types) must have a third-party audit of the application certifying that it meets the requirements of the DEA regulations. eazyScripts is certified by Drummond Group. The following guide will provide the instructions on how to successfully prescribe Schedule II-V controlled substances through the eazyScripts platform.

The requirements for an electronic prescription application are quite specific. The DEA rules that Providers, Pharamacies and application providers must meet specific criteria to complete a successful process of electronically prescribing controlled substances.

**Identity Proofing of Prescribers (Practitioners).** Identity proofing is the process by which a prescriber is uniquely identified, so that only that prescriber has the access necessary to authorize and sign electronic prescriptions using a software application. Identity proofing of prescriber must be done by an approved credential service provider (CSP) or certification authority (CA) [for digital certificates]. Remote identity proofing is permissible.

eazyScripts uses IdenTrust to complete the Identity Proofing of prescribers.

eazyScripts does not support Institutional Prescribers at this time.

**Two-Factor Authentication**

Once identity is verified, the prescriber is issued a two-factor authentication credential. (21 CFR § 1311.105.) The two factors must be two of the following: (1) Something the prescriber knows, such as a password or PIN; (2) A hard token separate from the computer being accessed (meeting at least FIPS 140-2 Security Level 1); or (3) A biometric, such as a fingerprint or iris scan, meeting DEA criteria.

Two-factor credentials will be used for (1) approving access controls, and (2) signing electronic prescriptions. They must always be in the exclusive control of the prescriber. (21 CFR § 1311.102.)

**§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 **Section 1311.125** or **Section 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 **Section 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 **Section 1306.05**(a) of this chapter.

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

(3) The number of refills as required by **Section 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 **Section 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 Section 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 **Section 1311.125** or **Section 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.

**Access Controls**

Access controls relate to software-based specifications and restrictions that ensure that only those individuals authorized to sign prescriptions are allowed to do so, and only those persons authorized to enter information regarding dispensing, or to annotate or alter or delete prescription information, are allowed to do so.

**§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 **Section 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).

**§1311.150 Additional requirements for internal application audits.**

(c) Any person designated to set logical access controls under Section Section 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.

**§1311.305 Recordkeeping.**

(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.

**Audit Trails and Other Requirements**

The regulations specify various events and incidents for which both prescriber and pharmacy applications must maintain an audit trail (i.e., a secure activity log that can be used to retrace those events/incidents). An "audit trail" is defined as "a record showing who has accessed an information technology application and what operations the user performed during a given period." (21 CFR § 1300.03.)

For prescribers, the application must track, among other things, the creation, alteration, indication of readiness for signing, signing, transmission, or deletion of an electronic controlled substance prescription, as well as any notification of a failed transmission. (21 CFR § 1311.120(b)(23).) For pharmacies, the application must track, among other things, all receipts, annotations, alterations, and deletions of controlled substance prescriptions. (21 CFR § 1311.205(b)(13)(i).) For both prescribers and pharmacies, the application(s) must track: the setting of, or changes to, access controls (21 CFR §§ 1311.120(b)(23)(ii), 1311.205(b)(13)(ii)); as well as other events that the application provider establishes as "auditable events," which are typically security incidents (21 CFR §§ 1311.120(b)(23)(iv), 1311.205(b)(13)(iii), 1311.150(a), 1311.215(a).)

In addition, both types of applications must conduct daily internal audits to determine whether

any “auditable events” (security incidents) have occurred on that day. (21 CFR §§ 1311.150, 1311.215.) This may be an automated function that generates a report for the prescriber or pharmacist to review. If the prescriber or pharmacist reviewing the report determines that a security incident has in fact occurred, that incident must be reported to the application provider and to the DEA within one day. (21 CFR §§ 1311.150(c), 1311.215(c).)