Billing Code 4410-09-P

DEPARTMENT OF JUSTICE

Drug Enforcement Administration

21 CFR Parts 1300, 1304, 1306, and 1311

[Docket No. DEA–218I]

RIN 1117-AA61

Electronic Prescriptions for Controlled Substances

AGENCY: Drug Enforcement Administration, Department of Justice.

ACTION: Interim final rule; reopening of comment period.

SUMMARY: The Drug Enforcement Administration (DEA) published an interim final rule in the *Federal Register* on March 31, 2010, which provides practitioners with the option of writing prescriptions for controlled substances electronically. Since publishing the interim final rule, DEA has received questions and requests for clarification on various issues concerning the implementation and technical requirements for the electronic prescribing of controlled substances. DEA is therefore reopening the March 31, 2010, interim final rule to solicit comments from the public on specific issues outlined below regarding the electronic prescribing of controlled substances in anticipation of subsequently publishing a final rule on these topics.

DATES: DEA is reopening a comment period for the interim final rule published March 31, 2010, at 75 FR 16236, which became effective June 1, 2010. Electronic comments must be submitted, and written comments must be postmarked, on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Commenters

should be aware that the electronic Federal Docket Management System will not accept comments after 11:59 p.m. Eastern Time on the last day of the comment period.

ADDRESSES: To ensure proper handling of comments, please reference "RIN 1117-AA61/Docket No. DEA-218I" on all correspondence, including any attachments.

- *Electronic comments:* DEA encourages that all comments be submitted electronically through the Federal eRulemaking Portal, which provides the ability to type short comments directly into the comment field on the Web page or to attach a file for lengthier comments. Please go to *http://www.regulations.gov* and follow the online instructions at that site for submitting comments. Upon completion of your submission, you will receive a Comment Tracking Number for your comment. Please be aware that submitted comments are not instantaneously available for public view on Regulations.gov. If you have received a Comment Tracking Number, your comment has been successfully submitted, and there is no need to resubmit the same comment.

- *Paper comments:* Paper comments that duplicate the electronic submission are not necessary and are discouraged. Should you wish to mail a paper comment in lieu of an electronic comment, it should be sent via regular or express mail to: Drug Enforcement Administration, Attn: DEA Federal Register Representative/DPW, 8701 Morrissette Drive, Springfield, VA 22152.

FOR FURTHER INFORMATION CONTACT: Scott A. Brinks, Diversion Control Division, Drug Enforcement Administration; Mailing Address: 8701 Morrissette Drive, Springfield, Virginia 22152; Telephone: (571) 362-3261.

SUPPLEMENTARY INFORMATION:

Posting of Public Comments

Please note that all comments received are considered part of the public record. They will, unless reasonable cause is given, be made available by DEA for public inspection online at *http://www.regulations.gov*. Such information includes personal identifying information (such as your name, address, etc.) voluntarily submitted by the commenter. The Freedom of Information Act applies to all comments received. If you want to submit personal identifying information (such as your name, address, etc.) as part of your comment, but do not want it to be made publicly available, you must include the phrase "PERSONAL IDENTIFYING INFORMATION" in the first paragraph of your comment. You must also place all of the personal identifying information you do not want made publicly available in the first paragraph of your comment and identify what information you want redacted.

If you want to submit confidential business information as part of your comment, but do not want it to be made publicly available, you must include the phrase "CONFIDENTIAL BUSINESS INFORMATION" in the first paragraph of your comment. You must also prominently identify the confidential business information to be redacted within the comment.

Comments containing personal identifying information and confidential business information identified as directed above will generally be made publicly available in redacted form. If a comment has so much confidential business information or personal identifying information that it cannot be effectively redacted, all or part of that comment may not be made publicly available. Comments posted to *http://www.regulations.gov* may include any personal identifying information (such as name, address, and phone number) included in the text of your electronic submission that is not identified as directed above as confidential.

An electronic copy of this document is available in its entirety under the tab "Supporting Documents" of the public docket of this action at *http://www.regulations.gov* under FDMS Docket ID: DEA-2010-0010 (RIN 1117-AA61/Docket No. DEA-218I) for easy reference.

Background

Historically, where federal law required that a prescription for a controlled substance be issued in writing, that requirement could only be satisfied through the issuance of a paper prescription. DEA, however, amended its regulations in 2010 to provide practitioners with the option of issuing electronic prescriptions for controlled substances (EPCS) in lieu of paper prescriptions. In particular, on June 27, 2008, DEA published a Notice of Proposed Rulemaking (NPRM) describing its plan to revise its regulations to allow the creation, signature, transmission, and processing of controlled substance prescriptions electronically. 73 FR 36722. After considering the comments it had received and revising its proposed rule accordingly, DEA published its Interim Final Rule (IFR) for Electronic Prescriptions for Controlled Substances on March 31, 2010. 75 FR 16236. The IFR's changes became effective June 1, 2010.[1]

The IFR is codified in DEA regulations in 21 CFR Parts 1300, 1304, 1306, and 1311. These provisions govern many different aspects of the electronic prescribing process and are explained in significant detail in the IFR. *See* 75 FR 16284–16289. Rather than repeating the IFR's explanation here, this discussion will briefly highlight several aspects of the IFR particularly germane to the issues on which DEA is seeking additional public comment.

[1] On October 19, 2011, DEA published a short clarification addressing certain EPCS topics to help ensure that industry properly implemented the requirements of the IFR. 76 FR 64813.

The Controlled Substances Act (CSA), 21 U.S.C. 801–904, prevents the diversion of controlled substances into improper channels by requiring that controlled substances only be prescribed by practitioners registered with DEA (or exempt from the registration requirement). Thus, one of DEA's primary goals in the IFR was to ensure that nonregistrants cannot improperly gain access to electronic prescription applications—*i.e.*, the computer software practitioners use to electronically issue their prescriptions. Obviously, if nonregistrants could gain access to these applications, they might be able to use them to fraudulently generate or alter electronic prescriptions for controlled substances, thereby diverting these controlled substances in violation of the CSA.

Thus, the IFR contains a number of measures designed to minimize, to the greatest extent possible, the potential for the diversion of controlled substances through such misuse of electronic prescription applications. These include the IFR's approaches to identity proofing (verifying that the user of an electronic prescription application is who he or she claims to be) and logical access control (verifying that the authenticated user has the authority to perform the requested action).

Under the IFR, a practitioner can only sign and issue an electronic prescription by using an authentication credential, and a practitioner can only receive such a credential after having his or her identity verified. For individual practitioners (as opposed to practitioners associated with an institutional practitioner registrant), such identity proofing is done by authorized third parties that, after verifying a registrant's identity, issue an authentication credential to the registrant. These third parties must be federally approved credential service providers (CSPs) or certification authorities (CAs).

Further, the IFR requires CSPs and CAs to conduct identity proofing at Assurance Level 3 of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-1, "Electronic Authentication Guideline," which allows either in-person or remote identity proofing. Since the IFR was published, changes in technology have led to the creation of new, updated NIST guidelines, NIST SP 800-63-3, "Digital Identity Guidelines." Under NIST SP 800-63-3, the relevant identity proofing assurance level is Identity Assurance Level 2. Identity Assurance Level 2 of NIST SP 800-63-3, like Assurance Level 3 of NIST SP 800-63-1, allows either in-person or remote identity proofing.

The IFR allows institutional practitioners to conduct their own in-house identity proofing as part of their credentialing process of the individual practitioners who will be using the institution's electronic prescribing application to issue prescriptions. If an institutional practitioner chooses to conduct its own internal identity proofing, that process must fulfill a number of specific requirements, such as including review of a government-issued photographic identification of the individual and ensuring that the individual's state authorization to practice is in good standing. Once this process is completed, a separate entity within the institutional practitioner (or an outside CSP or CA) can issue an authorization credential to the individual. In the alternative, rather than conducting its own identity proofing, an institutional practitioner can require individuals to obtain identity proofing and authentication credentials in the same manner as individual practitioners, *i.e.*, through a CSP or CA.

Under the IFR, authorization credentials must be two-factor. That is, a user must supply two different forms of authentication—two "factors"—to use their credential to issue an electronic prescription. These factors can take one of three forms. A factor can be

knowledge-based—something only the practitioner knows—such as a password or a response to a certain question. The factor can be biometric data, such as a fingerprint or iris scan. Or the factor can be a hard token, a cryptographic key stored on a special hardware device, such as a smart card or cellular phone, separate from the computer system containing the electronic prescribing application. Accordingly, to issue an electronic prescription under the IFR, a practitioner must first enter two different factors into the system containing the prescription application (*e.g.*, enter a password, scan a fingerprint, insert a smartcard) before the system will allow that practitioner to issue the prescription.

Identity proofing and two-factor authentication credentials are not the only controls the IFR requires. The IFR also requires electronic prescription applications to use "logical access controls." Logical access controls are controls in the application that ensure that the application only allows DEA registrants (or persons otherwise authorized under the CSA) to electronically sign controlled substance prescriptions (or indicate that prescriptions are ready to be signed). Logical access controls may be by user or role-based; that is, the application may allow permissions to be assigned to individual users or it may associate permissions with particular roles (*e.g.*, physician, nurse), and then assign each individual to the appropriate role.

In a private practice, logical access control must be handled by at least two people within the practice, one of whom must be a DEA registrant who has obtained his or her own two-factor authentication credential. Once a practitioner has received an authentication credential and wishes to use the electronic prescribing application, the two or more individuals who set the access controls first verify that the practitioner's DEA registration is valid. They then set the application's logical access controls to grant the practitioner access to those application

functions that indicate a prescription is ready to be signed and that sign controlled substance prescriptions. The individuals handling the access controls must complete this process together: one person must enter the data to grant access, and then another person (who is a DEA registrant and who has an authentication credential) must approve the entry using his or her own authentication credential before the access becomes operational.

Institutional practitioners use a similar but slightly different process to establish logical access control under the IFR. First, at least two individuals within the institution's credentialing office must approve any list of individuals who are to be permitted to use the institution's electronic prescription application to sign controlled substance prescriptions or indicate that controlled substance prescriptions are ready to be signed. After the list is approved, it must be sent to a separate entity within the institution (probably an information technology office) that actually enters the logical access control data and thereby grants the individuals on the list access to the electronic prescription application. This process also requires at least two individuals: one to enter the data to grant access and one to approve this entry.

The IFR's logical access control provisions also require that practitioners lose their permission to electronically sign controlled substance prescriptions (or to indicate that such prescriptions are ready to be signed) in certain scenarios: if the individual practitioner's hard token or other authentication factor is lost, stolen, or compromised; if the individual (or institutional) practitioner's DEA registration expires without renewal; if the individual (or institutional) practitioner's DEA registration is terminated, revoked, or suspended; or if the individual practitioner is no longer authorized to use the electronic prescription application

for whatever reason (such as a practitioner's departure from the institution using the application).

Additionally, the IFR requires that any electronic prescription application used to prescribe controlled substances create and preserve an "audit trail," a record of who accessed the application and certain operations they performed, including specified "auditable events." Among other things, such auditable events, include any setting of or change to logical access controls related to the issuance of controlled substance prescriptions. Whenever an auditable event occurs, an individual authorized to set logical access controls must review the auditable event and determine whether it was a security event that compromised or could have compromised the integrity of the electronic prescription application's prescription records. Any such security events must be reported both to the provider of the electronic prescription application and to DEA within one business day.

The IFR also contains certain provisions governing the transmission of electronic prescriptions for controlled substances. After an electronic prescription for a controlled substance has been digitally signed and issued, the electronic prescription application must transmit the prescription to a pharmacy application (software that manages the receipt and processing of electronic prescriptions) as soon as possible so that the pharmacy can fill the prescription. If the practitioner is informed that the prescription's transmission has failed, he or she may provide a paper or oral (where permitted) prescription as a replacement (including a manually signed printout of the electronic prescription), but must ensure that the replacement prescription indicates that the prescription was originally issued electronically but that transmission failed. Before filling such a replacement prescription, a pharmacist must check his or her records to ensure that the electronic prescription was not already

received and filled. If it was, the replacement prescription must be marked void. In this manner, the IFR seeks to ensure that electronic prescriptions will not be filled twice.

Finally, as discussed above, the IFR provides that biometric data, such as a fingerprint, is one of the authentication factors that a practitioner may use to issue a prescription. The IFR also provides certain requirements that an electronic prescription application using biometric data as an authentication factor must meet. On October 24, 2018, the SUPPORT for Patients and Communities Act (SUPPORT Act) was signed into law. The SUPPORT Act mandated that, "[n]ot later than 1 year after the date of enactment of this Act, the Attorney General shall update the [IFR's] requirements for the biometric component of multifactor authentication with respect to electronic prescriptions of controlled substances."[2] This requirement is part of a larger provision that amends the Social Security Act to require e-prescribing (with some exceptions) of drugs prescribed on or after January 1, 2021.[3]

Outstanding EPCS Issues and DEA's Need for Additional Comments

DEA received over 200 comments in response to its 2008 EPCS NPRM. Many of the comments received in response to the NPRM included arguments that the EPCS provisions should allow for more flexible electronic processes similar to those for handling prescriptions for non-controlled substances. DEA's 2010 IFR addressed these comments, but, in light of the complexity of the issues involved and various changes between the NPRM and IFR, also sought further comments about certain issues. *See* 75 FR 16236, 16242, 16243, 16246, 16248, 16251–16253, 16270, 16289, 16294. Since publishing the IFR, DEA has received

[2] Substance Use-Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act (SUPPORT Act), Pub. L. 115-271, sec. 2003(c), 132 Stat. 3894, 3927(2018). The Attorney General has delegated the authority to make the required updates to the Administrator of the DEA. *See* 28 CFR 0.100.

[3] SUPPORT Act, sec. 2003(a),(b). This requirement is codified at 21 U.S.C. 1395w–104(e)(7).

dozens of comments in response. Nonetheless, given the passage of time since the IFR was published and the rapid pace of technological development—in addition to the questions and requests for clarification that DEA continues to receive about the IFR's requirements—DEA has determined that it would be beneficial to reopen the IFR for comment to solicit comments from the public on specific issues, which are listed below, some of which DEA had previously raised as topics for comment in the IFR. DEA anticipates that such additional comments will prove helpful as it completes its final rule on these topics. In addition, as stated earlier, Congress has required the DEA to "update" its regulations on one of these issues, the biometric component of two-factor authentication, and comments from the public may help DEA to do so. DEA would like to remind commenters that any new approaches they are suggesting would be helpful only if DEA is able to adopt these new approaches while still ensuring the security and accountability of systems to identify fraud and prevent diversion.

Thus, DEA is now soliciting public comment on the following issues.

1. DEA currently requires that the authentication credential be two-factor to protect the practitioner from internal misuse, as well as external threats. *DEA is seeking comments in response to the following questions*:

    - Is there an alternative to two-factor authentication that would provide an equally safe, secure, and closed system for electronic prescribing of controlled substance while better encouraging adoption of EPCS? If so, please describe the alternative(s) and indicate how, specifically, it would better encourage adoption of EPCS without diminishing the safety and security of the system.

- Are practitioners using universal second factor authentication (U2F)? If so, how (*e.g.*, Near-Field Communication (NFC), Bluetooth, USB, or Passwordless)?

- Are practitioners using cellular phones as a hard token, or as part of the two-factor authentication? Is short messaging service (SMS) being used as one of the authentication factors used for signing a controlled substance prescriptions?

  Note: Authenticators using SMS and phone call verification currently fall under RESTRICTED use as outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B, "Authentication and Lifecycle Management," sections 5.1.3.3 and 5.2.10. Vulnerabilities evolve over time and implementing organizations should continually evaluate risk to determine long-term suitability.

2. As discussed, the IFR requires that a CSP or CA conduct identity proofing at Assurance Level 3 of the NIST SP 800-63-1, "Electronic Authentication Guideline." As noted, because of updates in technology, NIST SP 800-63-3, "Digital Identity Guidelines," now provides the most current relevant identity proofing guidelines. And, under NIST SP 800-63-3, the relevant assurance level is Identity Assurance Level 2. DEA believes that the ability to conduct remote identity proofing allowed

for in Assurance Level 3 of NIST SP 800-63-1 and Identity Assurance Level 2 of NIST SP 800-63-3 ensures that practitioners in rural areas are able to obtain an authentication credential without the need for travel. DEA further believes that application providers work with CSPs or CAs to direct practitioners to one or more sources of two-factor authentication credentials that will be interoperable with their applications. Additionally, an IFR provision, 21 CFR 1311.105, requires that a CSP providing EPCS authentication credentials be approved by the General Services Administration Office of Technology Strategy/Division of Identify Management to conduct identity proofing at Assurance Level 3 or above of NIST SP 800-63-1 (*i.e.*, Identity Assurance Level 2 or above of NIST SP 800-63-3). DEA has received questions asking for clarification of this requirement. *DEA is seeking comment on this approach to identity proofing, as well as any more comments about whether clarification of the language regarding CSP approval would be helpful.*

3. DEA emphasizes that institutional practitioners are allowed, but not required, to conduct identity proofing. If an institutional practitioner decides to have each practitioner obtain identity proofing and the two-factor authentication credential on his or her own, as other individual practitioners do, that is permissible under the rule. *DEA is seeking comment on this approach to identity proofing by institutional practitioners.*

- DEA is also seeking comment on the methods institutional practitioners are using to validate the identity of practitioners remotely. For example, are institutions viewing practitioners' driver's licenses or other forms of identification remotely using video?

4. The IFR requires that any setting of or change to logical access controls related to the issuance of controlled substance prescriptions be defined as an auditable event and that a record of the changes be retained as part of the internal audit trail. *DEA is seeking comment on this approach to logical access control for individual practitioners. In particular, DEA is seeking comment on whether there are any adjustments that DEA could make to this requirement that would reduce its burden on practitioners while still protecting the integrity of EPCS.*

5. As explained above, the IFR sets requirements for how institutional practitioners must establish logical access control for their electronic prescription applications. Among other things, the IFR requires that at least two individuals from the institution's credentialing office provide the part of the institution that controls the computer applications with the names of practitioners authorized to issue controlled substance prescriptions. The entry of the data that grant access to practitioners also requires the involvement of at least two individuals, one to enter the data and another to approve the entry. The institutional registrant is responsible for designating and documenting individuals or roles that can perform these functions. And a practitioner's access

must be revoked whenever any of the following occurs: the institutional practitioner's or, where applicable, individual practitioner's DEA registration expires without renewal, or is terminated, revoked, or suspended; the practitioner reports that a token or other factor associated with the two-factor authentication credential has been lost or compromised; or the individual practitioner is no longer authorized to use the institutional practitioner's application. *DEA is seeking comment on this approach to logical access control for institutional practitioners.*

6. The IFR requires that security events—auditable events that compromise or could compromise the integrity of the prescription records of an electronic prescription application—be reported to both the application's provider and DEA within one business day. *DEA is seeking comment from EPCS application users on whether they have experienced a security incident and, if so, whether they have experienced any difficulties reporting it.*

7. *DEA is generally seeking comment on any aspects of the IFR or other EPCS areas where further clarification would be helpful. For example:*

    - What types of issues have registrants encountered during the adoption and implementation of EPCS into their workflow, particularly where a prescriber uses an electronic health record (electronic medical record)?

- What types of devices are currently being used to create, sign, transmit, and process controlled substances electronically? For example, are practitioners using iOS or Android mobile devices, Chromebooks, Windows Laptop/Desktops, Mac OS, or others?

- Are there problems using two-factor authentication due to the method used to complete verification (*e.g.,* prohibited or limited cellular service, restriction on external USB devices, offline system access)?

- Has two-factor authentication caused barriers to efficient workflows?

- Have staff workflows at long-term and post-acute care facilities faced barriers during the adoption and implementation of EPCS?

8. Many institutions have implemented biometrics as part of their authentication credentialing for electronic applications. *DEA is seeking comments in response to the following questions:*

- What types of biometric authentication credentials are currently being utilized (*e.g.*, fingerprint, iris scan, handprint)?

- How has the implementation of biometrics, as an option for meeting the two-factor authentication requirement, benefited the EPCS program?

- Are there alternatives to biometrics that could result in a greater adoption rate for EPCS while continuing to meet the authentication requirements? If so, please describe the alternative(s) and indicate how, specifically, it would be an improvement on the authentication requirements in the IFR.

9. Previous commenters have expressed concern regarding failed transmissions of electronic prescriptions. *DEA is seeking comment in response to the following questions:*

- Have any entities experienced failed transmissions (*e.g.*, an EPCS being sent to the wrong pharmacy, an incorrectly filled out EPCS, an EPCS fails to send, the pharmacy does not have the prescribed controlled substance in stock, or the pharmacy rejects the EPCS)?

- If any failed transmissions have occurred, what alternative means of submitting the prescription to the pharmacy have been used?

_____

Uttam Dhillon,
Acting Administrator.

[FR Doc. 2020-07085 Filed: 4/20/2020 8:45 am; Publication Date: 4/21/2020]