Submitted via electronic submission to www.regulations.gov

June 22, 2020

Drug Enforcement Administration
Attn: DEA Federal Register/DPW
8701 Morrissette Drive
Springfield, VA 22152

Re: RIN 1117-AA61/Docket No. DEA-218I; Reopening of Comment Period for Interim Final Rule

Mr. Scott A. Brinks:

DrFirst.com, Inc. ("DrFirst") provides electronic prescribing software to thousands of health care entities and providers across the United States. DrFirst is a pioneer in electronic prescribing of controlled substances (EPCS), releasing the industry's first DEA-approved electronic prescribing application to securely transmit controlled substance prescriptions. Today, thousands of prescribers across the United States use DrFirst's EPCS Gold application to prescribe controlled substances. For that reason, DrFirst is exceedingly aware of the burdens and workflow issues prescribers face when electronically prescribing controlled substances. Given the significant advancements in technology since the 2010 Interim Final Rule (IFR) was published, DrFirst submits the following comments for your consideration.

I. Two-Factor Authentication

A. *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.*

Yes, DrFirst recommends that the DEA consider two alternative authentication solutions that would provide an equally safe, secure, and closed system for electronic prescribing of controlled substances and will also encourage adoption of EPCS. In the IFR, the DEA confirmed that single-factor was an insufficient security measure because it could not ensure that a practitioner would not be able to repudiate a prescription that he signed. This was based on the DEA's belief at the time that single-factor authentication only meant passwords alone or in combination with user IDs. This is not the case today. Though not traditional single-factor authentication, single gesture authentication does not require use of a password and is more safe and secure than multi-factor authentication. Single gesture authentication comprises of an on-device biometric match as the first factor and a private cryptographic key as the second factor. The DEA made the strong case for biometrics in the IFR, stating that they were less burdensome and can last for years. This combination of an

on-device biometric match and the private cryptographic key supports both the DEA's case for biometrics and addresses the DEA's security concerns. Another alternative authentication method that the DEA should consider in the future is continuous authentication. Continuous authentication can use behavioral analytics to validate a practitioner's identity based on the practitioner's prescribing behavior and how the practitioner interacts with an electronic prescribing application. Data can be gathered on the type of medications a practitioner prescribes, the amount of prescriptions signed during a specific period of time, and the time of day the practitioner usually accesses the application. If a practitioner's prescription transaction deviates from his or her historical behavior, it would result in a "red flag" for the transaction. While there is an argument that continuous authentication could replace multi-factor authentication, DrFirst recommends using it has a tool to supplement multi-factor authentication similar to how banks and credit card companies leverage it to verify irregular purchase transactions. Further, NIST has identified continuous authentication as a valid method of identity verification and plans to recognize it in its upcoming revision to the SP 800-63 publication.

Additionally, there are ways to improve the current DEA standards for two-factor authentication that would provide not only an equally safe, secure, and closed system for EPCS, but also a safer and more secure option than what is currently required under the existing regulations. The DEA expressed in the IFR that the goal of requiring a two-factor authentication protocol is to prevent a non-registrant from using a registrant's credential to create and sign a controlled substance prescription. The DEA relied on the then-established NIST standards in 2010 to form its basis for mandating the authentication protocol when prescribing and signing controlled substances. The standards established in the NIST SP 800-63-1 publication are outdated and do not reflect the evolving trends in technology and security. The DEA's requirements have not only discouraged the adoption of EPCS, but have stifled innovation of two-factor authentication solutions that are just as if not more safe and secure than what is currently required. The following recommendations can achieve DEA's goal of ensuring that controlled substances are prescribed safely and securely, while also encouraging the adoption of EPCS:

1) Allow Two Authentication Factors on the Same Device

Currently, the DEA requires a practitioner to authenticate to the electronic prescribing application using an authentication protocol that uses two of the following three factors: something the practitioner knows, something the practitioner has, and something the practitioner is. If one factor is a hard token, it must be separate from the computer system containing the electronic prescribing application and it must meet Federal Information Processing Standard (FIPS) 140-2 Security Level 1. DrFirst understands the DEA's reasoning in the IFR for requiring the hard token to be separate from the device used to issue controlled substance prescriptions. However, over the past decade, technological developments evidence that a separate hard token is not the only method to ensure the safe and secure transmittal of controlled substance prescriptions. The need for a separate hardware token is not only outdated from a security perspective, but also a barrier to EPCS adoption. Innovative technologies provide an equally safe option of having two independent authentication factors in a single device. Existing security architectures are capable of verifying that the individual accessing the application and electronically signing a controlled substance prescription is indeed a DEA registrant.

Allowing two authentication factors in the same device should also apply to the use of mobile devices for EPCS. In August 2018, the DEA issued guidance on the use of mobile devices in the issuance of electronic prescriptions for controlled substances.[1] In the guidance, the DEA stated that the device used to create the prescription cannot be the same device that serves as the hard token in the two-factor authentication protocol. This reflected the DEA's interpretation of the requirements under 21 C.F.R. §§ 1311.115 and 1311.116. However, the DEA did not provide evidence supporting the conclusion that allowing both authentication factors to be on the same mobile device is less safe and less secure than requiring the hard token to be separate from the mobile device. Despite the lack of compelling evidence, this requirement has resulted in significant workflow barriers for providers who desire to prescribe using a mobile device. Practitioners' prescribing workflows are heavily disrupted by having to enter a password on the mobile device used to issue the controlled substance prescription, and then using a separate hard token to complete two-factor authentication. Further, practitioners often forget and misplace their hard tokens and they typically carry other hard tokens such as smart cards or tap keys in practice. For these reasons, it is burdensome, impractical, and inconvenient for practitioners to continue to carry a separate hard token device at all times.

The DEA should consider that two-factor authentication on the same mobile device is just as secure as long as the application generating the OTP code or authentication credential is FIPS 140-2 validated. Note that authentication applications that have been FIPS 140-2 validated require that the mobile device running the application is also FIPS 140-2 validated. For example, Apple and Google undergo the FIPS 140-2 validation process for their operating systems. A potential security concern might arise if Apple or Google introduces a new operating system that has yet to undergo FIPS 140-2 validation, which would cause the practitioner to be running an authentication application on a device not yet FIPS 140-2 validated. However, this concern was specifically addressed by NIST in 2017. In its 800-63-3 publication, NIST affirmed that the requirement of both the authentication application and the smartphone itself be validated at FIPS 140-2 is solely applicable to authenticators that are procured by a government agency.[2] Moreover, because mobile devices automatically update operating systems for security updates, the security risk of a practitioner using a mobile device that is not yet FIPS 140-2 validated is relatively low. Allowing a practitioner to authenticate to the electronic prescribing application using two factors on the same device does not compromise the security and safety of issuing controlled substance prescriptions. The focus should be a two-factor authentication protocol that ensures optimum security, and not a rigid protocol solely focused on two separate factors. Therefore, DrFirst strongly recommends that the DEA revise the regulations to allow prescribers to authenticate on the same device, provided that the encryption used on the device and the authentication method meets FIPS 140-2 and other applicable NIST and industry standards.

---

[1] "*Use of Mobile Devices in the Issuance of EPCS*" DRUG ENFORCEMENT ADMINISTRATION (August 16, 2018).
[2] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf, Section 4.2.2.

2) Allow Use of More FIPS 140-2 Validated Hard Tokens for EPCS

DrFirst recommends that the DEA allow use of more two-factor authentication credentials that are FIPS 140-2 validated according to NIST standards. In the IFR, the DEA prohibited the use of some two-factor combinations based on the DEA's belief that these methods were impractical because they required more time for each authentication than other options deemed acceptable at the time. For example, the DEA currently prohibits out-of-band tokens for EPCS. Yet, push notification authentication is an out-of-band token that provides comparable security to OTP authentication. OTP authentication, once an industry standard, is now more vulnerable to security threats than push notification authentication. Push notification authentication delivers an out-of-band authentication mechanism over a mutually-authenticated secure transport layer. The transaction details are presented to the user, in this case the DEA registrant, for verification. Tapping a button unlocks a cryptographic key stored securely in the user's smartphone device, which would operate as the second factor in authentication protocol for signing a controlled substance prescription. If there is an unauthorized log-in attempt, the user can flag the transaction and tap a button. Push notifications are a practical method of authentication and are widely used and accepted in other industries. There are authentication options that are now safer than what the current regulations authorize. As technology has evolved since the IFR was issued in 2010, security threats have evolved as well. As long as hard tokens have been FIPS 140-2 validated, the DEA should allow practitioners to use them in the authentication protocol.

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

Yes, practitioners are using universal second factor authentication and it is increasingly becoming industry standard. Universal second factor authentication provides an additional layer of security that allows the application provider to verify that the application being accessed by the practitioner is secure. Many practitioners use Near-Field Communication (NFC) devices, tap badges, and other password-less devices. Nearly all practitioners use a mobile device. USB devices are not widely used among practitioners.

The current process of obtaining FIPS 140-2 validation prevents practitioners from utilizing industry standard hard tokens that exceed DEA requirements, such as universal second factor authentication tokens. There are hardware security keys on the market that have not received FIPS 140-2 validation, but offer secure methods of authentication due to their reliance on public key cryptography. Entities such as the FIDO Alliance develop security standards and certification programs to certify vendors that manufacture innovative hardware tokens. For example, NFC keys meet FIDO Alliance standards and are operable on a wide range of mobile devices and operating systems. They are more efficient for practitioners because they replace OTP codes and allow practitioners to simply tap their key, but they do not sacrifice security and safety. Other multi-factor authentication solutions exist on the market that are widely-accepted in finance and technology industries and meet the FIDO Alliance standards as well, but are not FIPS 140-2 validated.

For the above reasons, DrFirst strongly urges the DEA to implement requirements that allow DEA registrants to use two-factor authentication tokens that have been certified using industry validation standards such as those developed by the FIDO Alliance.

C. *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 prescription?*

Yes, as discussed in detail above, practitioners are using cellular phones as hard tokens and as part of the two-factor authentication protocol. Many practitioners use OTP codes generated on an application downloaded on a mobile device that is separate from the computer running the EPCS application. Practitioners not only use mobile devices as hard tokens, but are also using mobile devices to electronically prescribe controlled substances.

Short messaging service (SMS) is not currently being used for EPCS; however, it could be utilized in other areas of the process. Currently, practitioners who download a soft token on their mobile device to generate an OTP code as part of the two-factor authentication application are required to undergo an extensive identity-proofing validation process prior to utilizing the application. SMS could be used to assist practitioners when they are locked out of their accounts, such as when they purchase a new phone and download the same soft token authentication application on the new device. In such circumstances, utilizing SMS as an authentication verification as a replacement to requiring practitioners to undergo identity-proofing again is a more efficient option that does not compromise safety and security.

II. Identity-Proofing Requirements

A. *DEA is seeking comment on how CSPs and CA conduct identity proofing at Assurance Level , as well as any more comments about whether clarification of the language regarding CSP approval.*

DrFirst recommends that the DEA clarify identity proofing requirements under § 1311. The current regulations under § 1311.105 require that a credential service provider conduct identity proofing that meets the requirements of Assurance Level 3 or above as specified in NIST SP 800-63-1. NIST 800-63-1 Assurance Level 3 requires possession of a valid government ID number and a financial utility account number for remote identity proofing and possession of a verified government picture ID and an address or nationality of record for in-person identity proofing. NIST 800-63-3 IAL2 permits a broader range of evidence. DEA should clarify the specific pieces of identity evidence required to confirm a practitioner's identity. Furthermore, the requirements should not be based on the categories specified in the current NIST standards and should be broad enough to encompass and accommodate future standards published by NIST.

Alternatively, the DEA should require that practitioners undergo identity proofing in a manner that thoroughly confirms the real-life identity of the practitioner as specified by the CSP or CA. CSPs and CAs approved by a federal authority should be permitted to conduct identity proofing according to their own standards and issue credentials upon successful verification. This approach allows CSPs and CAs to confirm the identities of practitioners and also meets the DEA's objective of ensuring that identity proofing is conducted by a third party not involved in any other part of the electronic prescribing process. Hospitals and application providers are capable of selecting CSPs and CAs to adequately verify practitioners' identities and issue credentials. In addition, under NIST 800-63-version 2, health care and professional organizations that accept federal government reimbursement for treating Medicare beneficiaries must have credentialing committees to

carry out identity proofing consistent with NIST standards. This is spelled out in the "Conditions of Participations" documents every health care institution or organization that treats Medicare beneficiaries must sign.

Lastly, if the DEA should update its requirements for identity proofing by CSPs and CAs, practitioners who have previously undergone identity proofing under the old approach should not be required to undergo identity proofing under the new criteria. The DEA should ensure that these practitioners are grandfathered in under the old criteria once the practitioner's DEA status is verified as still active.

B. ***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.***

Practitioners who are using the institutional practitioner's DEA number to prescribe should not be required to undergo identity proofing a second time. This provision is envisioned already in the "Federation of Identities" in NIST 800-63-3 Section 7. Practitioners are typically identity-proofed as a condition to being hired at the hospital, whether or not they will prescribe controlled substances. In circumstances where practitioners were previously identity-proofed prior to accessing an electronic prescription application as a condition of employment, hospitals can confirm that they have kept up with identity-proofing and credentialing of the practitioner. This approach meets the DEA security concerns of ensuring that each practitioner is who he or she claims to be while easing unnecessary burdens on institutional practitioners.

III. General Aspects of the IFR and EPCS requirements

A. ***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?***

Practitioners are using iOS and Android devices, Chromebooks, Windows laptops and desktops, and MAC OS to create, sign, transmit, and process controlled substance prescriptions electronically.

B. ***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)?***

Yes, connectivity issues can occur for practitioners using OTP codes for authentication. Application providers must rely on external companies to validate the token value. Therefore, if the online system goes down, practitioners are unable to prescribe controlled substance prescriptions. Because the current regulations mandate that a CSP or CA must perform identity proofing and issue authentication tokens, application providers do not have a back-up method to validate authentication once the CSP's or CA's system goes down. Application providers have no control over how long a system outage may last. The DEA should permit application providers that are not CSPs or CAs, but have the capability of producing credentials, to provide temporary authentication codes as a backup option when connectivity issues occur.

C. *Has two-factor authentication caused barriers to efficient workflows?*

Yes. The requirement that the hard token be separate from the computer to which the practitioner is gaining access has created a significant barrier to workflow. As expressed by stakeholders ten years ago in the IFR, the use of hard tokens is "inconvenient, impractical, easily lost or shared, and generally not secure enough" (75 *Fed. Reg.* 16236, 16252). The same holds true today. Many providers perceive hard tokens to be unduly burdensome and unnecessary. Providers do not want to carry an additional device. In addition to carrying a hard token to sign controlled substance prescriptions, providers may also carry other tokens such as proximity cards to access their electronic health record or electronic medical system. Further, providers have to wait thirty seconds to receive a new OTP code when prescribing each controlled substance prescription. This causes a delay in the prescribing workflow.

Moreover, the process to replace a lost token is burdensome. If a practitioner loses the only token he or she possesses, the practitioner must undergo identity proofing again to obtain another token. Additionally, if a practitioner purchases a new mobile device, the authentication application must be downloaded again on the new phone. This results in the practitioner undergoing identity proofing once again. This process can take an upwards of at least fifteen minutes, which is a taxing process for many practitioners. Practitioners should be able to answer a series of challenge questions to verify their identity in order to receive a replacement token, as leveraged in other industries. A series of knowledge-based factors are a sufficient and secure method of identity verification for the purpose of assisting with a lockout or lost token.

IV. BIOMETRICS

A. ***What type 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, benefitted 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.***

Institutions have generally implemented biometric fingerprint scans. The implementation of biometrics has not significantly benefitted the EPCS program due to the infeasibility of vendors to meet the current DEA requirements for biometrics. Therefore, DrFirst strongly suggests that the DEA provide more flexible solutions for biometrics that create a simple and secure biometric pathway for practitioners.

The current requirements developed by the DEA in consultation with NIST are rigid and not easily adoptable by institutions and practitioners. The DEA relied on NIST SP 800-76-1 specifications at the time, which are outdated and have been updated over the past decade. When the current requirements were implemented, high-performance biometric sensors for fingerprint and face were not integrated in smart phones and other devices commonly used today. Technology companies now manufacture devices and operating systems that allow use of biometric sensors instead of passwords. Biometric sensors are also used as an initial authentication factor to unlock cryptographic keys for authentication. The current NIST SP 800-76-1 specifications are heavily focused on technical requirements for capturing biometrics for inclusion on a government issued Personal Identity Verification (PIV) smart card. These requirements are not aligned with how technology companies integrate on-device biometric systems in smartphones and other commercial devices. Further, the biometric system market has evolved and can now support high security models. These biometric systems exceed the existing DEA requirement that biometric subsystems operate at a false match

rate of 0.001 or lower. Commercial biometrics now have the capability to operate at a false match rate of 0.0001. The current regulations do not reflect modern security tools and standards.

Therefore, the DEA should update the requirements for biometrics to be consistent with current NIST standards and prevailing industry standards for biometric systems. When updating the requirements, the DEA should propose flexible solutions that provide for the use of lower-cost biometrics. If DEA requirements for biometric systems are too stringent, it will create a disincentive for companies to develop biometric devices that practitioners can use. Proposed solutions should also consider practitioners who are unable to prescribe locally in their practices and institutions. Practitioners should be able to have a back-up authentication method, such as a series of challenge questions or similar knowledge-based factors when prescribing off-site.

V. CONCLUSION

Since issuance of the 2010 Interim Final Rule, technology has drastically advanced. The security industry, including NIST, have adjusted to account for this evolution of technology. The DEA's primary goal is to ensure that non-registrants cannot improperly gain access to electronic prescription applications. This goal can be achieved without implementing unnecessary requirements that compromise security and increase electronic prescribing workflow burdens on practitioners. Going forward, the DEA should rely on up to date NIST standards and also embrace standards developed by the security industry to ensure that EPCS requirements are not technologically "stuck in time." This will also ensure that requirements proposed under the new rule do not become outdated and become less safe and less secure than what is currently available on the market.

Thank you for the opportunity to provide comments on the Interim Final Rule and recommend ways to improve electronic prescribing of controlled substances. Should you have any additional questions, please contact me at (301)231-9510 Ext. 2678 or edlee@drfirst.com.

Sincerely,

Edward C. Lee
Chief Administrative Officer
DrFirst.com, Inc.