American College of Emergency Physicians®
ADVANCING EMERGENCY CARE

June 22, 2020

RE: Docket No. DEA–218I

The Honorable Timothy J. Shea
Acting Administrator
Drug Enforcement Administration
8701 Morrissette Drive
Springfield, VA 22152

Re: Electronic Prescriptions for Controlled Substances Interim Final Rule, Reopening of Comment Period

Dear Acting Administrator Shea:

On behalf of our 40,000 members, the American College of Emergency Physicians (ACEP) appreciates the opportunity to provide feedback on the Electronic Prescriptions for Controlled Substances Interim Final Rule (IRF), which the Drug Enforcement Administration (DEA) has reopened for comments. While many of the questions the DEA now poses are targeted towards facilities and electronic health record (EHR) vendors, our responses are limited to those that impact emergency physicians and the patients we serve.

In the ten years since the Electronic Prescriptions for Controlled Substances IFR was published, the world of information technology (IT) has fundamentally changed. EHR adoption, electronic prescribing, and prescription drug monitoring programs (PDMPs) have become more widespread, and smartphones with robust security features, including biometric identification, are ubiquitous. The manner in which two-factor authentication is required for electronic prescriptions for controlled substances (EPCS) is slightly more cumbersome than other forms of two-factor authentication in other hospital-based applications as well as the consumer realm (electronic financial transactions, password reset, and others). However, the real challenge is less with two-factor authentication or e-prescribing controlled substances to pharmacies that may not stock the drugs, but rather, interfacing with PDMPs and integrating their information into EHRs. Important benefits to patient care and health care efficiency could be achieved if the DEA worked with the Office of the National Coordinator (ONC) of Health IT and other stakeholders like EHR vendors and state PDMPs to improve interoperability.

We also note that the way policies described in the IFR have been implemented vary depending on the type of health care facility. Going forward, ACEP recommends that the DEA not institute a "one size-fits-all" approach towards enforcing electronic prescribing requirements.

Please find our answers to your specific questions below:

WASHINGTON, DC OFFICE
2121 K Street NW, Suite 325
Washington, DC 20037-1886

202-728-0610
800-320-0610
www.acep.org

DEA Questions

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.*

Biometric identification, if implemented properly, could be a safe, secure, and closed system that would do more to encourage EPCS. However, third-party facial recognition and fingerprint readers are of variable quality and consistency and in some cases have been more frustrating and error-prone.

In all, most prescribing for institutional practitioners occurs via an EHR. Such applications are already required to comply with sufficient security standards without being overly burdensome to practitioners. Prescriptions transmitted via this method should be considered the most reliable and least likely to be subject to misuse. As such, additional barriers to use, such a two-factor authentication with each use may at times be unnecessary and perhaps superfluous in these settings. Overly burdensome security procedures create a barrier to the adoption of EHRs and other health IT platforms.

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

Various methods for automated login have been marketed for many years. However, having a username and password log-in system continues to be the dominant method for access to EHRs. Some EHRs may require additional secure passwords for certain actions, one of which may be EPCS. However, in hospitals and other facilities, this may be an unnecessary additional burden that does not truly provide heightened security. Username and password security policies and procedures should be sufficient for all aspects of EHR utilization. Biometrics are promising-- however in the clinical setting, they face several barriers such as the use of gloves, face masks, goggles, and face shields.

- *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?*

Many emergency physicians are using an institution-approved application from a credential service providers (CSP) installed on their smartphone for two-factor authentication. The health care practitioner's credentials (government-issued ID or hospital ID) are reviewed in-person with an authorized representative from the institution's IT or human resources (HR) departments, and credentials are assigned for the CSP app and further tied to the EHR. So long as that practitioner has the same phone, they will be able to generate a token (updated every 30 seconds) to serve as a second factor for authentication (the first factor being their EHR login and password). ACEP is not aware of SMS being used for EPCS authentication, though it is common in other industries. We believe the vast majority of hospitals would prefer not to utilize these technologies for a variety of reasons—mainly because it is burdensome on hospital IT systems to implement and manage.

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.***

Overall, ACEP believes that these are considerations to be addressed by healthcare application software vendors. For EHRs, such authentication must be automatic and performed in the background without additional user input. We appreciate issues that may be relevant to remote and rural practitioners not using standard EHRs, which is our premise for noting the challenges with one-size-fits-all policies. Nevertheless, in such circumstances, when an EHR is not available, additional authentication may be warranted. However, as noted previously, this situation does not apply to the vast majority of our specialty.

One enhancement would be the automated access of the Controlled Substance Prescription Monitoring Program (CSPMP) with an automated report of relevant prescriptions, which would occur during the e-prescribing process and before final initiation of the prescription. Such a process must be integrated into the EHR and seamless to the health care practitioner.

Finally, ACEP believes clarifying language on this approach may be helpful. For instance, instead of requiring in-person validation of credentials, a two-way audio and video session where the practitioner appears on camera with the institution's credentialing office, and displays their government-issued IDs, seems satisfactory for security while improving practitioner (and credentialing office) convenience.

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?***

This approach to allow institutions to decide for themselves whether to conduct identity proofing may benefit smaller and more rural institutions without necessarily compromising security. However, it is important for the DEA to emphasize that for institutional practitioners, "identity proofing" is optional. We are concerned that even making this statement may cause some institutional practitioners to force its use due to liability concerns, even though this is not required. It is our preference that the DEA modify this wording to state simply that institutional practitioners must use reasonable care in instituting identity proofing, such as is already common in EHRs.

The issue of remote validation (example logging into the EHR from home) is a valid concern. However, we do not believe undue emphasis needs to be placed on such access. Two-factor authentication for initial device registration (e.g. IP address) and subsequent username and password authentication (as is currently used in most banking transactions) is more than sufficient.

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***

ACEP is not aware of any adjustments the DEA could make to this requirement, as we believe it is already accomplished by most EHRs.

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.***

This is where the type of "institutional practitioner" may vary. The described procedure is probably not overly burdensome for hospitals, and it may be common practice. Other types of institutions may not have as robust of staff and some may only have one individual serving in the role described. These are considerations for the DEA to address, but do not typically impact our specialty of emergency medicine.

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.***

Emergency physicians do not have experience with this issue.

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)?***

Many emergency physicians experience hurdles getting registered and implementing EPCS into our workflows. For example, when we purchase a new smartphone, we are required to visit the credentialing office and obtain a new help-desk ticket and a new credentialing of the CSP app. Then, that credential must be tied to the EHR for two-factor authentication for EPCS. Further, if we lose a smartphone, we have to re-enroll—and since that process takes time, often we cannot e-prescribe for days to weeks afterwards.

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)?***

Fingerprint and facial recognition are used for some authentication processes (e.g. signing of death certificates). However, these require either third-party fingerprint scanners or in-app facial recognition algorithms that are cumbersome to set up and seem prone to mis-reads and frequent failures to recognize the credentialed user. These biometric solutions generally seem less convenient than system-level smartphone biometric authentication. Replacing the current two-factor authentication with biometrics runs a significant risk of disrupting workflows.

8. ***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)?***

It is important for the DEA to understand the unique nature of emergency medicine. For emergency medicine, the majority of our visits fall outside of "business hours," and some of our patients are not familiar with a regular pharmacy. Thus, many e-prescriptions are prone to "failure" - meaning, the pharmacy hours are not convenient for the patient, or the prescribed drug may not be in stock. This usually requires the patient to return to the emergency department or call the prescriber to cancel the original prescription and re-issue it to a new pharmacy. If the original prescriber's emergency department shift has ended, a new prescriber must be recruited. This is a limitation of e-prescribing protocols in general and not EPCS in particular, though the additional authentication for EPCS makes this more cumbersome, and the nature of emergency medicine means this scenario is all too common. Additional state requirements for PDMP logins and checks, and the separate authentication requirements for PDMP, further complicate these scenarios.

If you have any questions, please contact Jeffrey Davis, ACEP's Director of Regulatory Affairs, at jdavis@acep.org.

Sincerely,

William Jaquis

William P. Jaquis, MD, MSHQS, FACEP

ACEP President