AMA
AMERICAN MEDICAL ASSOCIATION

JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

ama-assn.org
t (312) 464-5000

June 22, 2020

Timothy Shea
Acting Administrator
U.S. Drug Enforcement Administration
U.S. Department of Justice
8701 Morrissette Drive
Springfield, VA 22152

RE: RIN 1117-AA61/Docket No. DEA-218I Electronic Prescriptions for Controlled Substances

Dear Acting Administrator Shea:

On behalf of the physician and medical student members of the American Medical Association (AMA), I am writing to respond to the opportunity that the U.S. Drug Enforcement Administration (DEA) has provided to submit comments on the 2010 interim final rule establishing regulations for electronic prescribing of controlled substances (EPCS). The AMA commends the DEA for reopening the comment period on the EPCS rules and urges the agency to move rapidly to update these regulations. It is critically important for the DEA to modernize its EPCS rules in order to increase the number of DEA registered physicians utilizing EPCS. By significantly reducing drug diversion and fraudulent prescriptions for opioid analgesics and other controlled substances, increased adoption of EPCS by physicians could contribute to the AMA's and others' ongoing efforts to end the nationwide epidemic of opioid-related deaths. Revising the EPCS regulations was required by the Support for Patients and Communities Act in order to facilitate new EPCS requirements for Medicare prescriptions. It is also consistent with President Trump's Executive Order 13777 seeking to identify regulatory actions that are outdated or ineffective, as well as the recommendations of the President's Commission on Combating Drug Addiction and the Opioid Crisis. The EPCS regulations have not kept up with advances in technology and the much-needed revisions would reduce regulatory burdens that deter physicians from adopting EPCS.

Modernization of the EPCS rules has taken on heightened urgency this year as the country faces not one but two nationwide public health emergencies. The need for patients and physicians to replace paper with electronic prescriptions has never been greater as physicians and pharmacies work to adopt stringent infection control practices, including avoiding physical contact and maintaining social distancing.

Why the EPCS Regulations Need to be Updated

EPCS is important to support high-quality patient care and to reduce fraud, tampering, and diversion of prescriptions for controlled substances. According to a 2019 report from the Office of the National Coordinator for Health Information Technology (ONC), in 2017 only 32 percent of physicians who prescribed controlled substances did so electronically, and a similar percentage of physicians who had computerized systems for prescribing other medications were prescribing controlled substances electronically. Earlier this year, in a new ONC report outlining its strategy for reducing regulatory and administrative burden, ONC pointed specifically to the EPCS requirement for two-factor authentication, noting that it can be burdensome for prescribing clinicians to integrate into their workflow and has had the effect of slowing adoption of EPCS nationally.

By highlighting the effect of the two-factor authentication requirements in decelerating EPCS adoption, the ONC reports reinforce the role that the interim EPCS regulations have played in the low rate of adoption of EPCS compared to other electronic prescribing. The truth of the matter is that adoption of electronic prescribing for other medications that are not controlled substances is one of the few examples of technological changes promoted for physician practices that works well and is seamlessly integrated into medical practice workflows. Most physicians also want to adopt EPCS and have it integrated into their practice workflows. Physicians have expressed great frustration that they can prescribe other medications this way, but do not have the capability to adopt EPCS systems that will be integrated with their other electronic prescriptions, electronic health record (EHR) systems, state prescription drug monitoring programs (PDMPs), and practice workflows. They are also concerned that EPCS adoption would require them to absorb significant additional costs.

Changes Needed in Biometrics Regulations

A particular concern is the DEA standards for the biometric component of multifactor authentication. The AMA agrees that requiring multifactor authentication increases EPCS security, but the rigid and burdensome requirements for biometrics included in the 2010 regulations preclude physicians from deploying user-friendly devices already found in their practices to satisfy these requirements. Instead of using laptop computers and smartphones with fingerprint scanners, facial recognition, or other biometric technology, they must utilize separate biometric technology that has been reviewed by the DEA or a DEA-approved certifying organization for specific compliance with EPCS requirements. These requirements state, for example, that the "biometric subsystem must operate at a false match rate of 0.001 or lower." Yet even though Apple products, for example, have a biometric error rate of less than one in 50,000 and are validated for compliance with U.S. Federal Information Processing Standards (FIPS) 140-2 Level 1,[1] Apple products have not been certified to meet the DEA requirements and cannot be used for EPCS. The biometric scanners found on consumer devices commonly employed in medical practices are used for secure access to other sensitive information, like banking and EHRs, but typically do not comport with the rigid and outdated rules for EPCS.

The regulations further require that the biometric device either be co-located with or built into the computer that is being used for EPCS. This rule has led to the development of a niche market for EPCS products, such as Imprivata's Confirm ID, which have been certified to comply with DEA regulations for EPCS. The fingerprint reader or facial scanner on a smartphone could not be used by a physician for EPCS because, even if it had been reviewed by the DEA, the smartphone would be separate from and work independently of the EPCS software and hardware being used in the practice. The existence of this niche market allows health information technology (health IT) vendors to charge high prices to physician practices to add the technology needed for EPCS and, even after assuming these costs, EPCS technology is still likely to disrupt workflows because it is not integrated with physicians' other systems.

During the COVID-19 public health emergency, these problems have been exacerbated. Quarantine and social distancing guidance has led many physicians to work from their homes or in alternative locations away from the technology in their regular medical offices. Whereas many physicians could have

[1] https://support.apple.com/guide/security/touch-id-face-id-passcodes-and-passwords-sec9479035f1/web.

successfully used widely available consumer devices in their homes or other sites to provide telehealth services, access their EHRs, and prescribe non-controlled medications, this rule would have prevented them from using these devices for EPCS. It is ironic that the accelerated adoption of telehealth technology that has resulted from the COVID-19 pandemic could lead instead to further setbacks in EPCS adoption.

The volume of controlled substance prescriptions for a subset of physician practices makes compliance with two-factor authentication, particularly as a distinct process from electronic prescribing of non-controlled substances, onerous and a significant strain on practice workflows. On top of the fact that few health IT vendors support EPCS, and the cost of add-on modules and separate monthly service fees, the methods and processes that vendors utilize for EPCS are often not well-aligned with normal electronic prescribing workflows. In most instances, physicians must initiate an entirely new set of computer programs and windows each time they use EPCS. Separate workflows and authentication requirements for EHRs, PDMPs, and EPCS have become a major impediment to greater physician EPCS uptake. These barriers should be addressed by the DEA in concert with health IT designers and implementers. Ultimately, the prescribing workflow should combine controlled substances and other medications seamlessly.

<u>How the EPCS Regulations Should be Revised</u>

The AMA recommends several modifications to the DEA’s EPCS biometric regulations, which are shown in “tracked changes” in a document attached to this letter. The changes may be summarized as follows:

1. Under §1311.116 *Additional requirements for biometrics*, EPCS service developers should have several options for complying with the biometric subsystem requirements. One of these options could be the current requirement for testing by a DEA-approved certifying body, but developers should also be able to provide a combination of attestation and supporting documentation that a biometric subsystem’s matching software meets the DEA’s biometric requirements for EPCS. For instance, a developer seeking DEA approval could assert that its EPCS service comports to necessary technical requirements while also providing to the DEA documentation verifying its product’s testing and conformance to said technical requirements. This would lower the barrier to entry for smaller software developers while still providing the DEA oversight and developers accountability for product performance.

2. Also, under §1311.116 *Additional requirements for biometrics*, besides the option of being co-located or built into the device used for issuing electronic prescriptions, the biometric reader should be able to work independently of the physician’s computer, smartphone or tablet that is used to issue electronic prescriptions for controlled substances.

<u>Impact of Regulations on Innovation</u>

The AMA has extensive experience with the impact of regulation on health IT design, development, and use. Over-regulation, or regulation that is too prescriptive, contributes to many of the issues that physicians identify as detracting from their effective use of health IT to care for patients. A prime example of this imbalance is the unintended consequences resulting from the Centers for Medicare & Medicaid Services (CMS) EHR Incentive Program and the ONC Health IT Certification Requirements. While well intentioned, the combination of these two programs has negatively influenced the usability and interoperability of EHRs. Regulations stipulating how EHRs must perform and how physicians must use them have driven EHR vendors to create technology focused on federal reporting requirements rather than the needs of physicians and their patients (see March 2018 *Wall Street Journal* article).

Only recently, through a mixture of congressional actions and this administration's focus on regulatory relief, are we starting to see opportunities for user-centered innovation in the EHR space. While much more work remains, the continued relaxation of regulation and flexibility in the use of technology will ultimately provide far more voluntary uptake of health IT, including EPCS, than has occurred over the past ten years. Furthermore, this approach will enable a more competitive marketplace—allowing health IT vendors to compete for business based on user satisfaction and demand for functionality and workflow integration. Notably, technical advancements can improve the confidentiality, integrity, and appropriate accessibility of electronic prescribing, and will promote greater fraud and abuse detection. The AMA strongly urges the DEA to learn from this historical perspective and to examine methods to reduce regulatory complexity that detracts from health IT innovation.

The AMA appreciates the DEA's consideration of these recommended updates to the EPCS regulations, which would encourage the development of less expensive and more usable EPCS software and hardware solutions and strike a more appropriate balance between software/hardware performance assurances and EPCS regulatory flexibility. If you have any questions or want to discuss this issue further, please contact Margaret Garikes, Vice President for Federal Affairs, at margaret.garikes@ama-assn.org or by calling 202-789-7409.

Sincerely,

James L. Madara, MD

Attachment

§1311.115 Additional requirements for two-factor authentication.

(a) To sign a controlled substance prescription, the electronic prescription application must require the practitioner to authenticate to the application using an authentication protocol that uses two of the following three factors:

(1) Something only the practitioner knows, such as a password or response to a challenge question.

(2) Something the practitioner is, biometric data such as a fingerprint or iris scan.

(3) Something the practitioner has, a device (hard token) separate from the computer to which the practitioner is gaining access.

(b) If one factor is a hard token, it must be separate from the computer to which it is gaining access and must meet at least the criteria of FIPS 140-2 Security Level 1, as incorporated by reference in §1311.08, for cryptographic modules or one-time-password devices.

(c) If one factor is a biometric, the biometric subsystem must comply with the requirements of §1311.116.

§1311.116 Additional requirements for biometrics.

(a) If one of the factors used to authenticate to the electronic prescription application is a biometric as described in §1311.115, it must comply with the following requirements.

(b) The biometric subsystem must operate at a false match rate of 0.001 or lower.

(c) The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate.

(d) Compliance with the requirements of paragraph (c) of this section may be demonstrated through one of the following methods.

(1) Testing to demonstrate performance must be conducted by the National Institute of Standards and Technology or another DEA-approved government or nongovernment laboratory. Such testing must comply with the requirements of paragraph (i~~h~~) of this section; or

(2) A combination of attestation and supporting documentation that a biometric subsystem’s matching software meets the requirements of paragraph (c) of this section.

(i) This method must comply with the requirements of paragraph (i)(4)-(5) of this subsection.

(ii) This method may only be utilized if the electronic prescription application will provide to the practitioner, at no cost to the practitioner, an alternative factor in the event that the biometric subsystem fails to comply with the requirements of this section.

(iii) This method must relieve the practitioner of liability in the event that the biometric subsystem does not conform to the requirements of paragraph (c) of this section through no fault of the practitioner.

(iv) The DEA must establish a process for DEA registrants to report potential non-conformities to the DEA, with particular attention to minimizing practitioner burden.

(e~~d~~) The biometric subsystem must conform to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST SP 800-76-1 as incorporated by reference in §1311.08, if they exist for the biometric modality of choice.

(f~~e~~) The biometric subsystem must comply with one of the following: ~~either~~

(1) be co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location;

(2) ~~, or~~ be built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances; or

(3) work independently of the practitioner’s computer or PDA that he uses to issue electronic prescriptions for controlled substances.

(g~~f~~) The biometric subsystem must store device ID data at enrollment (*i.e.*, biometric registration) with the biometric data and verify the device ID at the time of authentication to the electronic prescription application.

(~~g~~h) The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be:

(1) Cryptographically source authenticated;

(2) Combined with a random challenge, a nonce, or a time stamp to prevent replay;

(3) Cryptographically protected for integrity and confidentiality; and

(4) Sent only to authorized systems.

(~~h~~i) ~~Testing of t~~The biometric subsystem must have the following characteristics:

(1) The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric.

(2) Test data are sequestered.

(3) Algorithms are provided to the testing laboratory (as opposed to scores or other information).

(4) The operating point(s) corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate, is tested so that there is at least 95% confidence that the false match and non-match rates are equal to or less than the observed value.

(5) Results of the testing are made publicly available.

Back to Top