TEXAS MEDICAL ASSOCIATION

Physicians Caring for Texans

June 22, 2020

Scott A. Brinks, Diversion Control Division
Drug Enforcement Administration
8701 Morrissette Dr.
Springfield, VA 22152

RE: Electronic Prescriptions for Controlled Substances; RIN 11117-AA61

Comments submitted via Federal Register: *www.federalregister.gov/documents/2020/04/21/2020-07085/electronic-prescriptions-for-controlled-substances*

Dear Mr. Brinks,

The Texas Medical Association (TMA) is the largest state medical society in the nation and is the voice of more than 53,000 physician and medical student members. TMA is committed to improving the health of all Texans. It is the mission of TMA to stand up for Texas physicians by providing distinctive solutions to the challenges they encounter in the care of patients. TMA thanks you for the opportunity to comment on the above-referenced interim final rule (IFR) specific to electronic prescriptions for controlled substances (EPCS).

TMA applauds the Drug Enforcement Administration for its progression in the use of EPCS. To date, physicians generally have reported that EPCS work well and they understand the extra layer of security required when prescribing controlled substances electronically. In Texas, it is generally required that physicians check the state's Prescription Monitoring Program (PMP) database when prescribing opioids, benzodiazepines, barbiturates, or carisoprodol. Having patient-specific information available at the point of care when prescribing has proven to be an effective clinical tool for physicians working to curb the opioid epidemic that has gripped our country. Additionally, Texas will require EPCS effective Jan. 1, 2021, to align with the Centers for Medicare & Medicaid Services requirements effective the same date.

Overarching comments:

TMA respectfully requests that physician workflow be considered when exploring any changes to the use of EPCS. The process must be easy to implement and the technology inexpensive for physicians. Given the current paradigm where the prescription must be sent to a specific pharmacy, it is important that systems used at the point of care provide (1) prescription availability at the patient's desired pharmacy and (2) information concerning the patient's out-of-pocket cost. It is extremely frustrating to physicians and patients when the patient goes to a pharmacy and the medication is out of stock or the patient finds the medication costs more than he or she can afford. Ideally, patients should have the ability to comparison shop electronically for their medications and have the prescription directed to their chosen pharmacy after they have evaluated factors such as price, availability, and distance. TMA realizes DEA has little to no control of these factors and that strides are

being made to deliver this information, but this is mentioned for awareness so that any advances in EPCS can be made in a way that supports these goals.

Specific comments:

In addition to the overarching comments above, TMA offers the following responses to the specific questions within the IFR.

DEA Q: 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?

TMA Comment: TMA recognizes the need for two-factor authentication but encourages DEA to consider the use of systems that minimize the number of times physicians needs to enter their two factors. Some electronic health records, for example, require entry of the two factors with each controlled substance prescription. Physicians should be able to enter their two-factor authentication periodically (ideally once or twice a day) rather than with each prescription or each patient.

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

TMA Comment: The range of second-factor tools is significant. Perhaps the most important point from a physician efficiency standpoint is that physicians should have the ability to use a single authentication method across all the organizations where they practice. Physicians who practice in multiple institutions need to carry all sorts of devices, apps, and other tools because each organization has chosen a different and incompatible approach. As a potential solution, local medical societies should be empowered to designate what two-factor tools would be used in their communities to minimize physician burden.

DEA Q: 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?

TMA Comment: Many physicians, especially those in small practice settings that don't have the advanced technology of large institutions, must rely on cellular technology and short messaging service. DEA should retain cellular phones as an option.

DEA Q: 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.

TMA Comment: Identity proofing takes time and can cost money. The cost and value of the time required for authentication should be reimbursed to physicians by any institution that outsources authentication. These institutions are placing an unfair burden on physicians by not providing identity proofing.

DEA Q: 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)?

TMA Comment: Physicians are being required to pay more for EPCS – typically $50 to $75 a month – and there is absolutely no ability to recover this cost. This is particularly unfair to small and solo practitioners. It is one of the many small burdens that, in the aggregate, generate frustration and burnout. Physicians should not have to pay extra for EPCS capabilities. Either that, or there should be a special payment that reimburses physicians for these costs.

DEA Q: 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?

TMA Comment: The devices used vary greatly, and TMA recommends that DEA not limit the types of allowable devices for EPCS.

DEA Q: 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)?

TMA Comment: When the two-factor system requires external communication, the system can fail. As an uncommon but good example, a physician cannot do EPCS on an airplane if the second factor (e.g., a token on a device) cannot be received. This speaks to allowing physicians to enter their two factors when they have access to them, which might be at a different time from when the prescription is generated.

DEA Q: Has two-factor authentication caused barriers to efficient workflows?

TMA Comment: Absolutely yes. It is an extra step is a process that can ill-afford additional steps. TMA recognizes the importance of two-factor authentication but encourages DEA to reduce the number of times two factors are required.

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

TMA Comment: Many different methods are being used, and each organization is generally doing something different from its neighbors. This means physicians are being iris-scanned in one place, hand-printed in another, and so forth.

DEA Q: 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.

TMA Comment: Biometrics is not a panacea, and TMA encourages DEA to continue to allow alternatives. Aside from the burden of having to undergo personal scans, biometrics require storage of personal information that, if compromised, could have significant negative consequences for physicians. Strict reporting and penalties that compensate physicians for damages should be in place for breaches. Some health care organizations have demonstrated their inability to keep patient information secure. Biometric databases potentially are a much richer target.

DEA Q: 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)?

TMA Comment: These are real issues and frustrations that contribute to patient and physician burden. TMA suggests the solution to many of these problems is to allow the patient to "move" the prescription to another pharmacy where it can be filled. The physician may have chosen the wrong pharmacy, the patient may have changed his or her mind about where to have the prescription filled, the pharmacy may be out of stock. There are many reasons to give control over the movement of prescriptions to patients, rather than requiring physicians or their staff to do further uncompensated work.

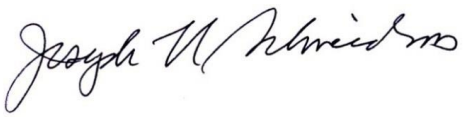
In the cases of rejected EPCS prescriptions, a national database of these should be supported by DEA so the root causes can be identified and eliminated. Systems that lack quality measurement cannot be improved, and it is highly unlikely the private market can create such a quality improvement system.

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

TMA Comment: It is not unusual for physicians to maintain secure prescription pads as a backup to EPCS failure. This alternative should remain as a viable option in the event of technical failures that could impede patient treatment. These are also necessary in the case of downtime, power failures, and other emergencies.

If you have questions about TMA's recommendations, please do not hesitate to contact Shannon Vogel by calling (512) 370-1411 or emailing shannon.vogel@texmed.org.

Sincerely,



Joseph H. Schneider, MD, MBA
Chair, Committee on Health Information Technology
Texas Medical Association