33 W Monroe, Suite 1700
Chicago, IL 60603
knicholoff@ehra.org
Phone: 517-930-1198
Twitter: @EHRAssociation

June 22, 2020

Mr. Timothy Shea
Acting Administrator
Drug Enforcement Administration
8701 Morrissette Drive
Springfield, VA 22152

RE: RIN 1117-AA61/Docket No. DEA-218I

Dear Acting Administrator Shea,

On behalf of the 30 members of the Electronic Health Record (EHR) Administration, we are pleased to submit our comments on the "Electronic Prescriptions for Controlled Substances" (EPCS) Interim Final Rule, which was published in the *Federal Register* on April 21, 2020. We appreciate that the DEA has reopened the rule for public comment, as there have been many advancements in healthcare technology and adoption since the rule was first proposed in 2010.

The EHR Association's member companies serve the vast majority of hospitals, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs across the United States. Our core objectives focus on collaborative efforts to accelerate health information and technology adoption, advance information exchange between interoperable systems, and improve the quality and efficiency of care through the use of these important technologies.

Security is a critical component to prescribing controlled substances. However, there must also be consideration of the right balance between security and the prescriber's experience, since overly restrictive security may encourage the prescriber to seek out less secure workarounds. The adoption of electronic prescribing in general has been largely successful in recent years -- and particularly in certain geographies where it is mandated -- but because EPCS comes with an added cost, supplemental security requirements, and workflow implications, adoption figures are not where they could be for greater healthcare industry benefit.

While we support the DEA's efforts to reduce provider burden while maintaining

necessary security, in our experience EPCS is but one part of a larger, more complex picture of managing controlled substances. Unfortunately, this rule does not address inconsistencies in Prescription Drug Monitoring Programs (PDMP) and EPCS reporting across states, which not only creates a usability burden for physicians, but is also reflected in the latest discouraging opioid statistics: people are getting around the system, likely due to inconsistencies of implementation and not whether providers are using two-factor authentication or other security protocols. The EHR Association recommends that the DEA work with ONC and the CDC on development of a national framework for DMP and EPCS data and policies.

Thank you for this opportunity to provide comments on this important regulation. Below, in our specific responses to the questions posed in the IFR, we discuss the importance of security, including multi-factor authentication (MFA) and identity proofing, as well as new alternatives that focus on solving the problem of controlled substance abuse while easing clinician and practice burden. We welcome the opportunity to answer any questions or provide clarification on any points made herein.

Sincerely,

Cherie Holmes-Henry
Chair, EHR Association
NextGen Healthcare

Hans J. Buitendijk
Vice Chair, EHR Association
Cerner Corporation

HIMSS EHR Association Executive Committee

David J. Bucciferro
Foothold Technology

Barbara Hobbs
MEDITECH, Inc.

Rick Reeves, RPh
CPSI

Emily Richmond, MPH
Practice Fusion Inc., a subsidiary of Allscripts

Sasha TerMaat
Epic

Courtney E. Tesvich, RN
Nextech

About the HIMSS EHR Association

Established in 2004, the Electronic Health Record (EHR) Association is comprised of more than 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.

1. Two-Factor Authentication

Two-factor authentication (2FA) is the industry standard for security. There are few, if any, commercial authentication alternatives to multi-factor authentication (MFA) that provide equally safe, secure, and closed systems. Additional factors themselves can vary: cellphones/SMS, Bluetooth, key generators, tokens, fingerprint readers, face ID, and badges. The ultimate goal in the use of MFA is to improve usability without compromising security.

Accordingly, the EHR Association recommends the DEA work with ONC both on standards evolution and usability. ONC has experience in working with the private sector to evaluate, understand, and drive standards forward as appropriate. This investigation can be supplemented through HITAC feedback and the Interoperability Standards Advisory annual process to inform the DEA on your decisions.

We also recommend that the DEA partner with NIST to continue to evolve the DEA requirements for improved usability and security as described in the latest NIST 800-63-3 special publication. Specifically, we request that the DEA work with NIST to provide clear guidance on the use of particular authentication technologies on the market today, including mobile device biometrics (iOS and Android) and FIDO-based authenticators (including the relevant FIPS compliance requirements). Establishing an authentication methodology security framework (or referencing an existing option) would help EHR developers, physician practices, hospitals, and clinicians ensure they are selecting appropriately secure and compliant options for use in EPCS software and solutions.

An area that has proven to be problematic is the re-registration process, such as when an individual practitioner replaces one factor of their two-factor authentication modalities and does not have another valid authentication factor available, thereby causing the practitioner to have to go through identity proofing again. (Example: A practitioner is identity-proofed and registered with pass-phrase and mobile phone-based one-time password (OTP) and then the practitioner replaces that mobile phone.) We suggest the DEA addresses streamlining of the identity proofing process when the only one of the factors needs to be replaced and validated.

2. Additional Usability Challenges

Current regulation requires the provider to indicate that the prescription is ready to be signed before signing it. In practice, this results in an extra click that appears to serve no added security benefit. We recommend the DEA remove this requirement.

When the IFR was first issued, EPCS technology was often separate from or bolted on to existing prescribing technology in the EHR, if such EHR technology was used at all. However, as EHRs have become ubiquitous, many EHR developers including EHRA's members have begun to integrate ECPS functionality directly within their certified EHR technology (CEHRT). However, the current regulations do not contemplate integration, resulting in burden as providers are often asked to re-authenticate when ordering controlled substances to comply with DEA's requirements. Certification for EHR technology also includes security criteria, and we recommend the DEA investigate whether there are opportunities to avoid a second authentication step in certain scenarios when ECPS is integrated into CEHRT.

Considering these usability challenges, it would be interesting for DEA to investigate if there are methods where one could sufficiently rely on analytics based on pattern-based monitoring of controlled substance prescribing to identify abuse while providing a more usable solution for the majority of prescribers. For instance, the provider who regularly prescribes fewer than 10 controlled substances a month may not require the same surveillance and oversight as the provider issuing 200+ controlled prescriptions a month. When a prescribing pattern is out of the norm, it could trigger an additional real-time review of the transaction, in addition to a prescribing requirement that still includes MFA and non-repudiation. Dynamic MFA policy decisions could reduce burden and may contribute to addressing the problem the DEA is seeking to solve.

3. Identity Proofing

The EHR Association agrees that identity proofing is an important factor in EPCS (and other healthcare scenarios). Individually, private medical information, demographics, and financial data are at risk for attack, and collectively, healthcare represents an enormous target for cybersecurity attacks and crime. While new technologies and requirements are often viewed as a burden by end users, identity verification is critical to overall solution security. Analogous to the identity verification requirements in other regulations (GDPR and CCPA), healthcare and access to healthcare data cannot and should not be provided anonymously.

Compared to when the IFR was first issued more than 10 years ago, the success rate and usability of credential service provider (CSP) identity proofing technologies have greatly improved, and the impact to end-users has also greatly decreased. With the improvements to identity proofing process standards and associated issuance of credentials that can be communicated using a combination of standards such as SAML, OAuth, and OpenID, ensuring the correct person is provided access has greatly improved. There is also a broader industry of identity verification vendors in the space.

We request clarification around the use of certified and approved CSPs for identity proofing. Validation of CSPs against NIST 800-63-3 should remain a requirement, if not simply to assist the healthcare market and EHR developers with selecting compliant, robust, and secure solutions. Otherwise, assertions of compliance become less meaningful. We also encourage DEA to update the EPCS regulations to incorporate best practices from the latest NIST 800-63-3 version of the "Digital Identity Guidelines" special publication.

The EHR Association also requests additional guidance from the DEA around the ability to source MFA credentials separately from the CSP that conducts the identity proofing. In many cases, institutions have existing compliant MFA options that they have purchased and simply need to attach a verified identity to each account. Such an ability would create greater flexibility in the market and support EPCS adoption, while reducing the burden on institutions and users associated with managing multiple credentials.

Providing a crosswalk for providers to easily assess a 2FA solution's ability to support the applicable standards and to mitigate the risks in scope of the DEA framework would help guide the end users towards choosing amongst compliant vendors.

Additionally, we would appreciate updates to the General Services Administration (GSA) website, specifically the list of approved vendors on this page: [https://www.idmanagement.gov/buy/trust-services/#identity-services]. The GSA does not appear to regularly update the list of approved vendors on their website, which means there are occasionally vendors that are "compliant" but not yet listed on that site. This results in either less choice for customers or customers inadvertently buying non-official or non-compliant solutions for their EPCS needs. Anything the DEA can do to encourage the GSA to provide updates and more detail would help.

Lastly, we recommend that flexibility for remote identity proofing be codified in the DEA's final regulation. Factors such as IP address to establish location or a photo from a camera stream may be effective alternative means of remotely establishing identity, particularly during crises like the current pandemic.

3. Identity Proofing by Institutional Practitioners

Institutional practitioners frequently require in-person validation of identification, which can be practical when coupled with other security measures like issuing the credential (token) or registering the practitioner's fingerprint for biometric authentication.

Additionally, the EHR Association is in favor of the DEA advancing shared identity proofing and credential concepts and a supporting ecosystem for "bring-your-trusted-credential" (BYTC) concepts that will enable portability and interoperability of digital credentials outside a single ecosystem or workflow concern. As identity proofing requirements continue to emerge in other healthcare programs, as well as other industries, providers should be able to verify their identity once and use that identity (and linked credentials) across a variety of programs, including EPCS.

Further, critical to credential portability is standardization around identity proofing models (for example, the "Identity Assertion Level," as defined in NIST 800-63-3). We encourage the DEA to consider steps to advance such a BYTC ecosystem, to reduce the burden on individuals and institutions.

4. Logical Access Control for Individual Practitioners

The EHR Association requests clarification from the DEA as to whether all permissions need to be reassigned in the event of a temporarily lost MFA credential or replaced MFA credential. Additionally, the DEA should also clarify what is expected to be included in daily incident reports. Standardization is key to monitoring for and detecting diversion of controlled substances across products, vendors, and solutions. Doing so would also enable better inputs to PDMP systems that are aggregating patient use of controlled substances.

As mentioned above, the monitoring and reporting on prescribing patterns, rather than sending a daily incident report, has the potential to identify bad actors more efficiently. The DEA should encourage use of the modern technologies in addressing the intent of the regulation, while reducing the burden on users and individuals to monitor large audit reports for malicious activities. This specifically relates to section §1311.150(b). In large institutions, it is highly unlikely that any human will uncover malicious activity by reviewing daily incident reports across hundreds of providers. While we agree that audit trails can be helpful, we question the effectiveness of the use of daily reports to monitor for and detect malicious activity and note that they should be overseen and monitored by operational owners rather than providers.

5. Logical Access Control for Institutional Practitioners

We support this provision. Two individuals should approve a user's access for something as sensitive as controlled substance prescriptions. The number of approvers appears to be two for both the "Individual" and "Institutional" practitioner models, but the language in the current IFR is a bit complicated and leaves too much to the auditor's interpretation. Clarification in the final rule for this requirement will be helpful.

6. Reporting Security Events

We sincerely appreciate the DEA's requirement that application providers be notified of security incidents. However, the one-day requirement as suggested presumes that events are detected in real-time. The daily incident report requirement does not mandate review of reports, though, which means that events are likely to go unnoticed in day-to-day operations unless someone in the healthcare organization is reviewing the reports at the end of every single day -- which is not reflective of reality in most institutions. Further, we note that a single day is not enough time to meaningfully assess whether an event merits further investigation and follow up. The wording should instead be updated to say something akin to "within one day of event discovery." Notification to the provider regarding such events, as well as the developer of the underlying software that was known or suspected to be involved, would seem to enable the affected parties to address anything necessary.

As noted above, large institutions also struggle to meaningfully review their incident reports because of the large numbers of providers in their practices and the sheer volume of EPCS activities (enrollments, logical access, and prescribing) that take place each day. Therefore, we recommend that the time allotted should be revisited after consultation with healthcare organizations and information security professionals.

Additionally, we request that the DEA clarify what constitutes an event that requires reporting.

Lastly, to improve the reporting of suspected or confirmed malicious events, the DEA should consider providing automated options (such as web service-based APIs designed in conjunction with industry stakeholders) for reporting such data.

8. Biometrics

EHRA member companies are starting to see adoption of biometrics by our clients, but the preference for biometrics over other MFA options varies widely across the healthcare space. The most common device used today is a fingerprint scanner that attaches to a laptop or desktop device, but palm scanners run less risk of spoofing and are demonstrably more reliable than iris scanners.

Current mobile biometric solutions native to iOS and Android devices don't appear to meet the DEA EPCS security requirements for biometrics and have not seen any substantial adoption. We have also received feedback from clients that it is not feasible to deploy and maintain biometrics at hundreds of sites, so they therefore choose to continue to use soft tokens and cell phones as the second factor device even where biometrics are available.

Looking ahead, we encourage the DEA and other stakeholders in the industry to further test and evaluate a variety of biometric modalities, such as voice, spoken pass-phrases, palm prints, facial recognition, and behavioral pattern readers. We believe there is potential for some or all of those options to be useful in the future if the issues above are addressed.

FIDO/2/WebAuthn solutions are alternatives to biometrics that could result in a greater adoption rate for EPCS. Locally-processed biometrics (e.g. iPhone fingerprint) would be better alternatives to central biometric storage. Such local biometric options also may be compatible with FIDO-based workflows, supporting greater interoperability with identity provider offerings. Many new MFA options exist in the market, including device attestations that appear promising.

We note, too, that biometrics are not suited to every medical scenario. For example, gloved clinicians currently serving COVID-19 patients with a need for strong PPE are unable to safely rely on a fingerprint as a biometric option. Additionally, with many providers currently working from home, while they may have home computers, mobile phones or tablets, they often don't have access to the same technological hardware and software they would have in the office or hospital that offers them greater choice as to how to satisfy 2FA requirements. We encourage DEA to creatively consider methods for separating EPCS requirements from physical locations.

9. Failed Transmissions

We are aware of failed transmissions of ePrescriptions, such as instances where the prescription has been sent to the wrong destination pharmacy. Even when pharmacies are part of the same organization (eg CVS or Walgreens), transferring misdirected prescriptions from one location to another can be

difficult or impossible. In these cases, the prescriber normally resubmits or provides a paper prescription.

The EHR Association recommends the DEA provide greater detail around the expected workflows and options for failure scenarios that allow the end-user to remain in compliance and still issue the prescription to the patient. Official workflow diagrams and visual aids depicting approved options for these workflows would help clarify the market's understanding of preferred approaches.