imprivata®

Five common misconceptions about electronic prescribing of controlled substances (EPCS)

Disclaimer: This document and the materials herein shall not be interpreted and/or used as legal advice for your company to be used in complying with Federal and State EPCS Laws and/or the DEA requirements for EPCS. Alternatively, it provides background information to help you understand the DEA requirements and achieve EPCS success. This legal information is not the same as legal advice, where an attorney would apply the law to your specific circumstances, so we insist that you consult an attorney if you'd like advice on your interpretation of this information or its accuracy. In summary, you may not rely on the information in the materials herein as legal advice, nor as a recommendation of any particular legal understanding.

Electronic prescribing of controlled substances (EPCS) is gaining swift adoption across healthcare as organizations look to improve prescribing workflows, meet Meaningful Use e-prescribing targets, increase patient safety and satisfaction, and combat prescription fraud, drug diversion, and "doctor shopping" for pills.

To enable EPCS, however, organizations must comply with the specific requirements outlined in the DEA IFR, the complexity of which has led to some confusion and misunderstanding about the requirements.

The following are five common misconceptions about EPCS, the debunking of which is critical to ensuring organizations implement processes and technologies that are fully compliant with the DEA requirements for EPCS:

Misconception #1: EPCS is not legal in my state

The truth: The DEA introduced the IFR legalizing EPCS in 2010, and since then, every state has passed legislation to legalize EPCS for schedule II-V controlled substances. New York and Maine are the first two states to mandate electronic prescribing, including for controlled substances. EPCS regulatory status by state is available from Surescripts.

Misconception #2: Pharmacies cannot receive electronic prescriptions for controlled substances

The truth: On average, 88% of pharmacies in each state are enabled for EPCS, according to Surescripts. However, in some cases, individual pharmacies and pharmacists may not be aware that they are able to accept electronic prescriptions for controlled substances, so as a best practice, it is recommended that organizations conduct outreach to the pharmacies in their area before enabling EPCS to ensure the pharmacies are ready to receive electronic prescriptions for controlled substances.

Misconception #3: If a physician is already logged into the EHR, they have completed the first factor of the two-factor authentication process for EPCS

The truth: Although the physician will have already authenticated to access the EHR or e-prescribing application, the DEA requires two-factor authentication at the time of prescribing.

Specifically, the IFR states, “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: Something only the practitioner knows, such as a password or response to a challenge question, Something the practitioner is, biometric data such as a fingerprint or iris scan, and Something the practitioner has, a device (hard token) separate from the computer to which the practitioner is gaining access.”[1]

Something you are

FIPS-compliant fingerprint biometrics

Something you have

FIPS-compliant Hands Free Authentication or push token notification

Something you know

****

Password

Understanding this requirement is essential to comply with the DEA IFR as well as to ensure the EPCS workflow is fast and efficient for physicians. Unfortunately, much of the confusion stems from the fact that most multifactor authentication solutions can only manage the second factor of authentication for EPCS. The first factor is the physician’s password typed into the native EHR dialog.

However, because many vendors will only demonstrate the authentication step they handle (and not the complete workflow), it gives the impression that EPCS can be completed with just a single factor. This is misleading, and it is important for organizations to understand that two-factor authentication is required at the time of prescribing to complete an EPCS order in a DEA-compliant manner.

Imprivata Confirm ID™, the comprehensive identity and multifactor authentication platform for EPCS and other secure authentication workflows across the healthcare enterprise, satisfies this requirement by managing both factors of authentication in a user interface integrated directly into the EHR e-prescribing workflow. This ensures physicians have a fast, convenient, and DEA-compliant way to complete the required two-factor authentication protocol for EPCS.

This also gives organizations the flexibility to move away from passwords and enable faster, more efficient two-factor authentication (for example, fingerprint biometrics plus push token notification). This is especially beneficial in areas of the hospital where higher volumes of controlled substances are prescribed.

Misconception #4: If an organization conducts institutional identity proofing, physicians will use the organization’s institutional DEA number when prescribing controlled substances electronically

The truth: A physician’s individual DEA number will be included on an electronic prescription for a controlled substance, just as it currently appears on paper prescriptions, regardless of how the physician is identity proofed. In the case of an intern or other clinician without an individual DEA number, the organizations’ DEA number plus the individual’s suffix will be included on the prescription (again, just as it currently appears on paper prescriptions).

[1] 1 Department of Justice Drug Enforcement Administration (DEA) (2010). 21 CFR Parts 1300, 1304, 1306, and 1311 Electronic Prescriptions for Controlled Substances; Final Rule. Page 16312.

About Imprivata

Imprivata, the healthcare IT security company, enables healthcare securely by establishing trust between people, technology, and information to address critical compliance and security challenges while improving productivity and the patient experience.

For further information please contact us at

1 781 674 2700
or visit us online at
www.imprivata.com

Offices in

Lexington, MA USA
Uxbridge, UK
Melbourne, Australia
Nuremberg, Germany
The Hague, Netherlands

Effectively, the DEA is allowing organizations with an institutional DEA number to serve as a trusted agent to validate the identity of each physician and grant them EPCS permissions. However, on the prescriptions themselves, the physician's individual DEA number (or unique suffix in the case of a provider without an individual DEA number) will be included in the same way it is currently included on a paper prescription.

Misconception #5: If a physician is already credentialed at an organization, they are not required to undergo the identity proofing process for EPCS

The truth: The DEA requires that all physicians who will be enabled for EPCS undergo the identity proofing process, even if they are already credentialed at a given organization. The DEA allows two types of identity proofing: institutional and individual.

In the institutional model, DEA-registered institutional practitioners (i.e., a hospital or health system) conduct identity proofing to validate the identity of each physician to be enabled for EPCS. The institutional identity proofing must be conducted in-person, and is typically managed by the credentialing office.

In the individual model, each physician will work with a third-party DEA-approved credential service provider (CSP) to complete the identity proofing to validate their identity.

More information about the identity proofing requirements for EPCS and the differences between the institutional and individual models can be found in this whitepaper.

Conclusion

These are just a few of the common misconceptions about the requirements for EPCS outlined in the DEA IFR. Before initiating an EPCS project, it is essential for organizations to have a complete understanding of the DEA requirements.

As a trusted strategic partner with more than 100 customers using our solutions to enable EPCS, Imprivata can help you understand the DEA requirements and identify the right technologies and processes to implement a fully compliant EPCS solution that also delivers a fast, efficient workflow that your physicians will love.

For more information or to request a demo of Imprivata Confirm ID, our comprehensive authentication platform for secure authentication workflows across the healthcare enterprise, please visit: www.imprivata.com/multifactor-authentication.