Requirements for EPCS: DEA and other federal regulations

In response to the United States' national opioid abuse epidemic, electronic prescribing of controlled substances (EPCS) continues to gain momentum among federal and state lawmakers to reduce "doctor shopping" and minimize the risk of altered, stolen, or fraudulent prescriptions.

DEA interim final rule EPCS requirements

EPCS is governed by the DEA interim final rule (IFR), the goal of which is to ensure the integrity, authentication, and non-repudiation for controlled substance prescriptions to reduce the potential for diversion, and subsequent abuse, of controlled substances.

In accordance with these objectives, the DEA IFR outlines a series of specific, unique, and complex requirements that healthcare delivery organizations, providers, pharmacies, and technology vendors must meet. Some of these requirements include:

- The EHR/e-prescribing application must be certified as compliant for EPCS

- Providers must complete an identity proofing process to confirm that they are authorized to prescribe controlled substances and have been assigned the proper credentials

- A two-step logical access control process must be in place to give EPCS permissions to approved providers

- Providers must use two-factor authentication when signing an EPCS prescription

- Comprehensive and detailed reporting must be in place to demonstrate compliance and to identify auditable events and security incidents
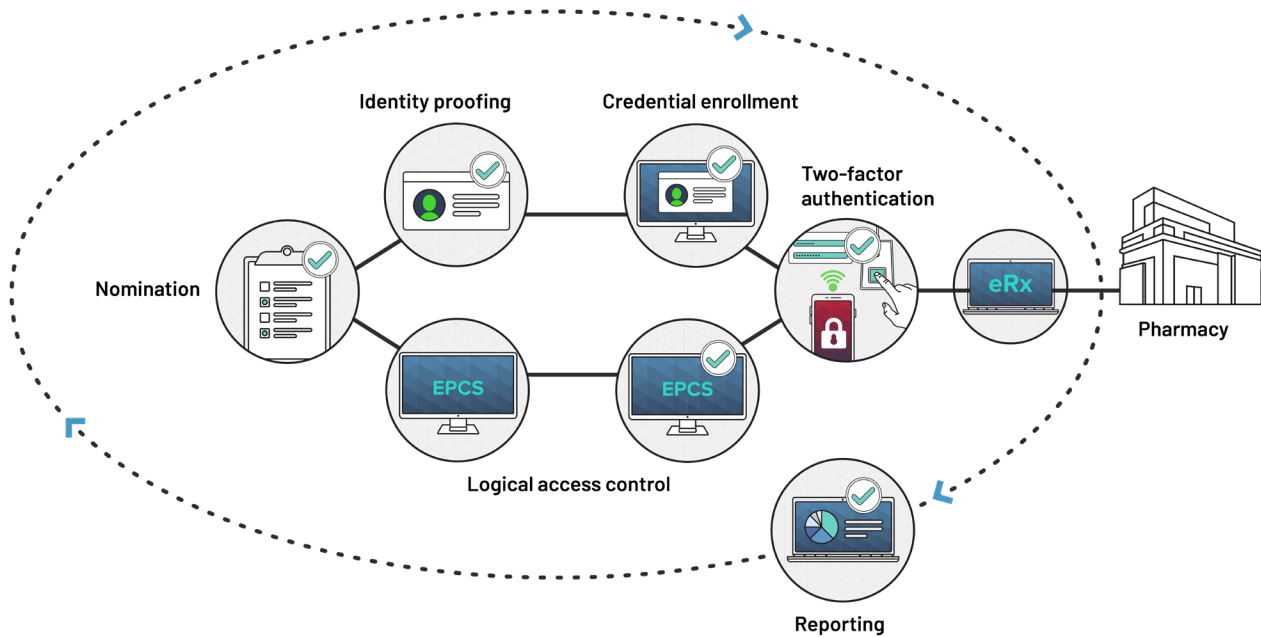
These are just a few of the requirements for EPCS, and without a complete understanding of the full DEA regulations, you are more likely to put your organization at risk of non-compliance and to leave your providers vulnerable to fraud.

Benefits for key stakeholders Complying with EPCS requirements: Tokens vs. comprehensive EPCS solutions

Because the DEA requirements are so unique and complex, authentication-only products (such as those that use only a token) are NOT sufficient for EPCS.

Relying on a token solution will leave you to develop disparate, often manual processes for meeting identity proofing, credential enrollment, logical access control approval, and additional EPCS requirements, all while making sure you can produce the records necessary to establish a complete audit trail.

And even then, a token solution leaves your providers with a sub-par workflow experience: they will have only one option for two-factor authentication (password + token), which limits flexibility and does not allow for backup.

Conversely, a true EPCS solution should be a comprehensive platform for provider identity proofing, enrollment of credentials, two-factor authentication, and auditing and reporting. It should integrate with EHRs and e-prescribing applications and should support a broad range of two-factor authentication options to ensure workflow efficiency and make EPCS as fast and convenient as possible for care providers.

SUPPORT for Patients and Communities Act

In October 2018, the "SUPPORT for Patients and Communities Act" was signed into law. This sweeping bill institutes several initiatives to address America's opioid abuse epidemic – a crisis that claimed the lives of more than 40,000 people in 2016.

Included in the bill is an electronic prescribing requirement for controlled substances, and the deadline to comply was January 1, 2022. This federal legislation followed significant momentum at the state level – where dozens of states had implemented e-prescribing and EPCS laws.

To comply with EPCS laws and mandates, healthcare delivery organizations and providers must meet the DEA requirements for EPCS, which are very specific and require a detailed, highly collaborative cross-functional project plan.

EPCS requirements for Medicare Part D

Section 2003 of the SUPPORT Act mandates that controlled substances under Medicare Part D prescription drug plans be ordered electronically in accordance with an electronic prescription drug program. This means that, for any healthcare provider prescribing controlled substances under a Medicare Part D prescription plan must be using EPCS to do so.

Enabling compliant EPCS with Imprivata Confirm ID

Imprivata Confirm ID is the fast, secure signing solution for EPCS. It is the most comprehensive platform for provider identity proofing, supervised enrollment of credentials, two-factor authentication, and auditing and reporting to help healthcare organizations meet the DEA requirements for EPCS. Imprivata Confirm ID integrates with leading EHRs and e-prescribing applications, and it supports the most complete set of two-factor authentication modalities, including Hands Free Authentication, to make EPCS as fast and convenient as possible for care providers.

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700

or visit us online at **www.imprivata.com**