Chapter 5: Electronic Prescribing of Controlled Substances (EPCS)

Background

What is a "controlled substance"? Any drug defined in the five categories of the federal Controlled Substances Act of 1970. The categories, or schedules, cover opium and its derivatives, hallucinogens, depressants and stimulants. Schedule I drugs have a high abuse potential and no approved medical uses. Drugs in Schedules II to V all have approved medical indications, with decreasing abuse and dependence liabilities as the schedule number increases. Common examples include narcotics, but also many sedatives, anxiolytics, anti-epileptics and medications for attention deficit hyperactivity disorder (ADD and ADHD).

What is EPCS? Electronic prescribing for controlled substances (EPCS), including opioids, replaces the use of paper prescriptions. When a provider uses EPCS, prescriptions are transmitted directly to the pharmacy in the same, secure manner that most prescriptions for non-controlled substances are transmitted today.

Why is it important? EPCS helps address opioid abuse in several ways.

- With EPCS, patients no longer have access to the provider's Drug Enforcement Administration (DEA) registration number, which reduces the risk of forged prescriptions. Studies show that about 10 percent of providers have had their DEA number stolen at least once.
- In addition, because electronic prescriptions are sent directly to the pharmacy, the risk of a lost, stolen or otherwise diverted prescription is significantly reduced.
- Utilizing an electronic prescribing system also provides a more comprehensive audit trail and database for analytics required to improve prescribing patterns, identify patients in need of help, help reduce overprescribing and improve operational utilization of controlled substances.

In addition to helping combat the opioid abuse epidemic, EPCS offers significant benefits to improving provider workflow efficiency and satisfaction, increasing patient satisfaction, and minimizing prescription errors and inaccuracies.

With EPCS, providers are no longer forced to manage an inefficient dual prescribing workflow—paper for controlled substances and electronic for all other medications—and instead have a single, fast, electronic method for all prescriptions. This becomes especially important as more regulations are put in place that limit how and how often certain

controlled substances can be prescribed (for example, limiting initial opioid prescriptions to just a few days).

Similarly, EPCS gives patients a single, efficient way to have all their medications sent directly to the pharmacy, and in many cases, eliminates the need for a follow-up visit for a prescription refill.

EPCS is also important for complying with the various state and federal laws—as well as industry requirements—for electronic prescribing that continue to gain momentum in response to the opioid abuse crisis:

- In May 2018, Walmart announced that it will require electronic prescriptions for controlled substances, effective Jan. 1, 2020.
- In October 2018, the SUPPORT for Patients and Communities Act was signed into federal law. Included is an electronic prescribing requirement for all controlled substance prescriptions for a covered part D drug under a prescription drug plan (or an MA–PD plan). The deadline to comply is Jan. 1, 2021.
- In addition to the federal mandate, as of early 2019, 14 states have passed laws requiring electronic prescribing of opioids and necessitating EPCS:

State	Effective Date
New York	March 27, 2016
Maine	July 1, 2017
Connecticut	January 1, 2018
Arizona	January 1, 2019 or July 1, 2019 (depending on county population)
Pennsylvania	October 24, 2019
Oklahoma	January 1, 2020
Iowa	January 1, 2020
North Carolina	January 1, 2020
Massachusetts	January 1, 2020
Rhode Island	January 1, 2020
Tennessee	July 1, 2020
Virginia	July 1, 2020
Wyoming	January 1, 2021
California	January 1, 2022

What resources /special skills will it require? Who should be included? EPCS is governed by the DEA interim final rule (IFR), one of the goals of which is to "ensure that non-registrants did not gain access to electronic prescription applications and generate or alter prescriptions for controlled substances and to ensure that a prescription record, once created, could not be repudiated."

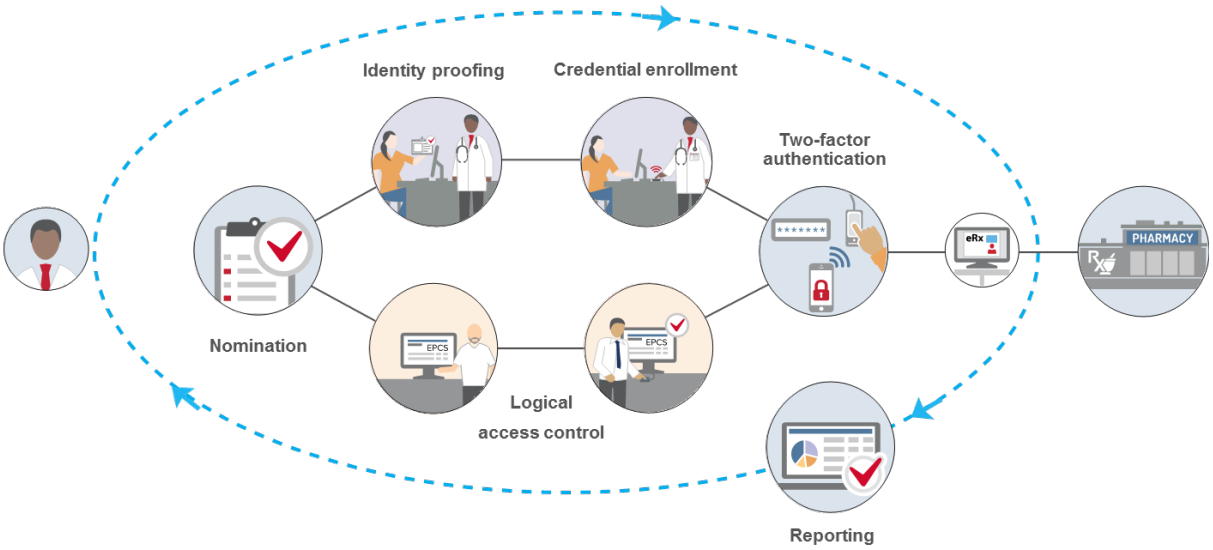
To meet this objective, the DEA IFR outlines specific requirements that healthcare delivery organizations, providers, pharmacies and technology vendors must meet. Some of these requirements include:

- The EHR or e-prescribing application must have a third-party audit that determines that the application meets the requirements of the DEA IFR.
- Providers must complete an identity proofing process to validate their identity.
- 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.

The EHR or e-prescribing application must have detailed reporting in place for "auditable events," which at a minimum includes:

- Attempted unauthorized access to the electronic prescription application, or successful unauthorized access where the determination of such is feasible.
- Attempted unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.
- Interference with application operations of the prescription application.
- Any setting of or change to logical access controls related to the issuance of controlled substance prescriptions.
- Attempted or successful interference with audit trail functions.
- The electronic prescription application must analyze the audit trail at least once every calendar day and generate an incident report that identifies each auditable event.
- Any person designated to set logical access controls must determine whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescription records. Any such incidents must be reported to the electronic prescription application provider and the DEA within one business day.

- The breadth and comprehensiveness of these and other requirements necessitate a cross-functional, collaborative project plan that involves many stakeholders across the organization. There are many strategic and tactical components that IT, clinical leadership, pharmacy, application/EHR teams, compliance/credentialing departments and others must put in place to successfully implement EPCS and realize its significant benefits.



The following are some of the important requirements that organizations and providers must meet to comply with the DEA IFR governing EPCS:

Identity Proofing - All providers must undergo identity proofing before they can be issued two-factor authentication credentials to be used for EPCS. This step is required even if providers have already been authorized to prescribe controlled substances at an organization using paper. The DEA allows two methods of identity proofing for EPCS:

- **Institutional** – Hospitals or other DEA-registered institutional practitioners can conduct in-house identity proofing (often conducted by the credentialing office or equivalent). Institutional identity proofing must be conducted in-person, and only organizations with an institutional DEA registration can use this model. At a minimum, providers must present government-issued photographic identification to complete the ID proofing process.
- **Individual** – Organizations can also elect to have providers use a third-party, DEA-approved credential service provider (CSP) or certification authority (CA) for identity proofing. This option can be done remotely, and organizations that are not DEA-registered institutional practitioners must use individual identity proofing.

Logical Access Control – All providers who are approved for EPCS must be given permissions to access the EPCS function within the EHR or e-prescribing application. At least two individuals must be involved in this step, and the DEA requires that the people responsible for setting the logical access controls be different from the individuals conducting the identity proofing (to create a separation of duties). The first individual will configure the EHR or e-prescribing application to give the approved providers permission to use EPCS, and a second individual must approve those permissions. If an organization is using the individual identity proofing model, this second individual must be a DEA registrant and use two-factor authentication to approve the access control settings.

Two-factor authentication – Providers are required to use two-factor authentication to sign EPCS orders. At the time of prescribing, they must enter two of the following three authentication methods: Something they know (i.e., a password); Something they have (i.e., a FIPS-compliant one-time password token); Something they are (i.e., biometrics).

Selecting which two-factor authentication method(s) to use for EPCS is one of the most critical elements of the project, as this will directly impact provider workflow. When selecting two-factor authentication options for EPCS, there are several key considerations, including:

- Ease-of-use – The two-factor authentication workflow for EPCS should be fast and easy for providers. If not, it could create inefficiencies that frustrate providers and impede care.

- Comprehensive options – Not every provider will be able to use all authentication methods, so an authentication solution for EPCS should offer a variety of different options to ensure every provider has access to two-factor authentication to meet DEA requirements for EPCS.

- Flexibility to adapt – Not all authentication options are viable in all prescribing scenarios, so an authentication solution for EPCS should give providers flexibility to use the best options that meet their requirements in any of these prescribing instances.

- Backup authentication options – EPCS authentication solutions should give providers backup options to complete the two-factor authentication workflow to ensure full DEA compliance. This is especially important as state and federal regulations start to mandate EPCS, which eliminates paper as a viable backup option if the provider is unable to complete two-factor authentication.

Record-keeping and reporting – The DEA IFR outline a comprehensive list of recordkeeping, reporting and auditing requirements for all aspects of the EPCS process. For example, organizations must create and retain records of the identity proofing, two-factor authentication credential issuance, and logical access control validation steps for a minimum of two years. Providers are also required to report fraudulent activity as well as lost, stolen or otherwise compromised two-factor authentication requirements. There are also reporting requirements for auditable events and possible security incidents, which organizations may need to report to the DEA. All reporting pertaining to EPCS must be easily readable and readily available to the DEA upon request.

Is there anything specific to opioids that needs to be considered? EPCS applies to all controlled substances, not just opioids. While the DEA regulations govern how controlled substances (including opioids) must be prescribed electronically, as noted above, multiple states actually mandate that EPCS systems are in place by certain dates. Of note, Prescription Drug Monitoring Programs (PMPs, or PDMPs) are not the same as EPCS. Some states require one, but not the other, so provider systems need to be aware of their own state(s)' mandates. Furthermore, hospital policies, medical boards and local care practices may also need to be accounted for. For example, some state mandates may place limitations on the number of narcotics prescribed for an acute issue, while other states may not. And some hospitals have different prescribing policies than others. In any case, EPCS is a way to leverage the safety methods, default settings, and alert systems of the e-prescribing module of the EMR, while also maintaining compliance with federal/DEA and state mandates.