imprivata®

WHITEPAPER

Electronic prescribing for controlled substances (EPCS)

A primer on the identity proofing and logical access control requirements

The Drug Enforcement Administration (DEA) interim final rule (IFR) allowing electronic prescribing for controlled substances (EPCS) was enacted in 2010, and outlines the requirements that health systems, hospitals, individual practitioners, pharmacies, and e-prescribing technology providers must meet to enable EPCS.

The requirements for EPCS are more stringent than the requirements for electronic prescribing for non-controlled substances, in part, to address what the DEA considers "existing and potential problems that exist when prescriptions are created electronically"[1] for non-controlled substances. To improve security and combat fraud, the DEA requires the use of two-factor authentication at the time of prescribing. When signing an electronic prescription for a controlled substance, practitioners must enter a combination of two of the following:

Something you are

FIPS-compliant fingerprint biometrics

Something you have

FIPS-compliant Hands Free Authentication or push token notification

Something you know

Password

But two-factor authentication is just one of the requirements outlined by the DEA. The DEA's primary goals are 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."[2]

To help meet these objectives, the DEA also requires all practitioners to complete an identity proofing process before they can prescribe controlled substances electronically. The DEA also mandates a logical access controls process to give EPCS permissions to authorized practitioners within the EHR(s) or other e-prescribing application(s).

This paper provides an overview of the identity proofing and logical access controls processes, including the methods allowed by the DEA, how credentials are issued, and requirements for setting logical access controls.

1. U.S. Department of Justice. Drug Enforcement Administration. Electronic Prescriptions for Controlled Substances; Final Rule, March 31, 2010.
2. Ibid.

Identity proofing requirements

The first step to enabling EPCS is to implement an identity proofing process to validate the identities of the individual DEA registrants seeking EPCS authorization. The two-factor authentication credentials required for signing electronic prescriptions for controlled substances can only be issued to practitioners who have been successfully identity proofed.

The DEA requires all practitioners who will be prescribing controlled substances electronically to undergo identity proofing, even if they have already been authorized to prescribe controlled substances using paper. The DEA considers this to be critical because it limits "nonregistrants to obtain an authentication credential and issue electronic controlled substance prescriptions under a practitioner's name."[3]

The DEA requires all practitioners who will be prescribing controlled substances electronically to undergo identity proofing, even if they have already been authorized to prescribe controlled substances using paper

The DEA allows two types of identity proofing for EPCS: individual and institutional. When determining which model to use, it is important to understand the role of DEA registration numbers in both the identity proofing and prescribing processes.

Individual DEA registration numbers are DEA-assigned numbers authorizing a practitioner to prescribe and dispense controlled substances. Similarly, institutional DEA registration numbers are DEA-assigned numbers authorizing hospitals, health systems, clinics, and other organizations to dispense or otherwise handle controlled substances.

To prescribe a controlled substance, an individual must have a DEA registration number, which must be included on the electronic prescription to accurately identity the practitioner (as is the case for paper prescriptions). The exception is if the practitioner does not have a DEA registration number and is authorized to prescribe controlled substances at an organization (for instance, physician interns and residents, mid-level practitioners, etc.). In this case, the electronic prescription must include the institution's DEA registration number plus extension data assigned by the organization to identify the individual writing the prescription.

3. Ibid.

For identity proofing, whether an individual has a DEA registration number or not does not dictate how they must be identity proofed. For instance, while most practitioners will use their individual DEA registration number when prescribing controlled substances electronically, they are not required to undergo individual identity proofing. Instead, as discussed in the following sections of this paper, an institutional DEA registrant may elect to conduct in-house identity proofing of individual practitioners through its credentialing office.

Understanding how DEA registration numbers are used is important to help determine which identity proofing model best fits an organization's needs.

If the hospital, clinic, private practice, or other organization at which the practitioner will be prescribing is not itself a DEA registrant, it cannot conduct institutional identity proofing and providers must undergo individual identity proofing for EPCS

Individual identity proofing

Individual identity proofing is the process by which individual practitioners undergo identity proofing through a certification authority (CA) or credential service provider (CSP) that is approved to conduct identity proofing by a federal authority.

If the hospital, clinic, private practice, or other organization at which the practitioner will be prescribing is not itself a DEA registrant, it cannot conduct institutional identity proofing and providers must undergo individual identity proofing for EPCS.

Individual identity proofing can be done in-person, but it is typically completed remotely via the online identity proofing service of the authorized CSP. The DEA does not stipulate how CSPs or CAs conduct identity proofing, as long as the process meets NIST Assurance Level 3 or above.[4] The practitioner will submit the necessary information to the CSP and, if the identity proofing process is completed successfully, the practitioner will be issued a two-factor authentication credential.

4. For remote individual identity proofing, the DEA specifies: "NIST Assurance Level 3 requires a valid government-issued identification number and a financial account number. These numbers must be confirmed via record checks with either the issuing agency or institution or through credit bureaus or similar databases. The check must confirm that the name, address, date of birth, and other personal information in the records are consistent with the application and sufficient to identify a unique individual. The address or telephone number must be confirmed by issuing the credential in a manner that confirms the ability of the applicant to receive communications at the listed address or number (ibid.)

When opting for individual identity proofing for EPCS, it is important to understand the designated CSP's process and requirements, and communicate those clearly to practitioners who will undergo individual identity proofing. The process typically requires submission of an extensive amount of personal and financial information, and there is a precise order in which each step of the process must take place. If this is not initially understood and made clear to practitioners, it may lead to challenges in the successful completion of identity proofing by some individuals and create delays in the EPCS rollout.

The DEA allows hospitals, clinics, or other DEA-registered institutional practitioners to conduct in-house identity proofing and authorize the issuance of credentials

It is also important to have a process in place to alert the organization(s) at which the practitioner will be prescribing that the individual has successfully completed identity proofing and has been issued a two-factor authentication credential. This communication is necessary to trigger the logical access controls process as the next phase of EPCS enablement (as discussed in subsequent sections of this paper), enroll the practitioner and the associated two-factor credentials, and minimize any delays between the completion of identity proofing and when the practitioner can begin prescribing controlled substances electronically.

In addition, in the individual model, there are potential downstream impacts to the EPCS workflow. The CSP conducting the identity proofing will issue the practitioner a two-factor authentication credential to be used for signing EPCS orders (most often a software or hardware OTP token). Unless the CSP has partnered with a third-party authentication solutions provider, organizations that opt for individual identity proofing will not have flexibility to leverage different two-factor authentication options.

Instead, they will exclusively use a password and the CSP-issued OTP token for EPCS, which may not meet the workflow requirements of different practitioners in different prescribing scenarios. It is important to understand the options available from the CSP or its partners to ensure the use of individual identity proofing does not have negative ramifications to EPCS workflows.

Institutional identity proofing

The DEA allows hospitals, clinics, or other DEA-registered institutional practitioners to conduct in-house identity proofing and authorize the issuance of credentials. The DEA defines an institutional practitioner as “a hospital or other person (other than an individual) licensed, registered, or otherwise permitted, by the United States or the jurisdiction in which it practices, to dispense a controlled substance in the course of professional practice, but does not include a pharmacy.” Institutional practitioners do have the option to require clinicians to undergo individual identity proofing (as described in the previous section) if they so choose, but the institutional identity proofing process is typically less time-consuming for practitioners.

The DEA allows hospitals, clinics, or other DEA-registered institutional practitioners to conduct in-house identity proofing and authorize the issuance of credentials

In this model, it is important to note that the organization’s institutional DEA registration number will only be used for identity proofing; an individual practitioner’s DEA registration number must be included on the electronic prescription itself (as is the case with paper prescriptions for controlled substances). If the organization permits, practitioners who do not have a DEA registration number can use the institution’s DEA registration number plus the necessary extension data to identity the individual prescribing the controlled substance(s).

Unlike individual identity proofing, institutional identity proofing can only be conducted in-person (not remotely). However, in the institutional model, the DEA does not require the same NIST Assurance Level 3 identity proofing criteria as for individual identity proofing.

Because hospitals and other care delivery organizations already conduct extensive background checks before credentialing clinicians, the DEA only requires that they match a government-issued photographic identification to the individual practitioner, and that they ensure that the individual is legally authorized to practice medicine and to prescribe controlled substances.

In-person identity proofing can also serve as an opportunity to supervise the enrollment of practitioners' two-factor authentication credentials that they will be using for EPCS (i.e., fingerprint biometrics or OTP tokens). Although they cannot use these credentials for EPCS until access controls are put in place, this approach minimizes the burden on practitioners, ensures they properly enroll their authentication modalities, and improves security.

Within the credentialing office, at least two people must validate the list of individuals to be granted access control for EPCS. Once approved, the list must be sent to a different department within the organization (typically IT) for the issuance of two-factor authentication credentials and to input the logical access controls to give EPCS permissions to the practitioners (as discussed in the next section of this paper).

Institutional or individual identity proofing for EPCS?

	Institutional ID proofing	Individual ID proofing
Does the organization at which practitioners will be enabled for EPCS have an institutional DEA registration number?	Yes	No
Does the organization have the ability to conduct in-person identity proofing for practitioners who will be enabled for EPCS?	Yes	No
Are there individuals without DEA registration numbers (i.e., interns or mid-level practitioners) who will be enabled for EPCS?	Yes	No
Does the organization have an IT department capable of setting logical access controls and issuing two-factor authentication credentials?	Yes	No

Setting logical access controls

After practitioners successfully complete the identity proofing process, they must be given permissions to access the EPCS function within the EHR(s) and/ or e-prescribing application(s) and sign prescriptions for controlled substances electronically.

The requirements for granting permissions differ slightly depending on whether the organization is an institutional practitioner or not, but in either case, the DEA requires that the individuals setting these logical access controls are different than the individuals conducting the identity proofing (to create a separation of duties).

For individual practices or organizations that are not DEA-registered institutional practitioners, two individuals must be assigned to manage logical access controls, one of whom must be a DEA-registrant authorized to prescribe controlled substances and who has been issued two-factor authentication credentials through the individual identity proofing process as described previously.

After the first individual gives the practitioners permission to prescribe controlled substances electronically using the assigned two-factor authentication credentials, the second individual (the DEA-registrant) must use two-factor authentication to approve the access control settings. The providers will then be ready to sign EPCS orders.

The success of an EPCS initiative depends on a complete understanding of identity proofing, logical access controls, and other aspects of the DEA IFR so the right processes are put in place to ensure compliance

Similarly, in the institutional identity proofing model, the logical access controls must also be set by individuals who are separate from those performing the identity proofing. As noted, the credentialing department creates and approves the list of practitioners to be granted access for EPCS, and sends it to a separate department within the organization (typically IT).

As with individual identity proofing, two individuals must be assigned to manage logical access control. One must authenticate to the EHR(s) and/or e-prescribing application(s) used for EPCS and grant the appropriate permissions, which the second individual must approve. Unlike the individual process, however, neither of these individuals is required to be a DEA registrant.

After the logical access controls requirements are satisfied, practitioners will be able to prescribe controlled substances electronically.

Conclusion

The success of an EPCS initiative depends on a complete understanding of identity proofing, logical access controls, and other aspects of the DEA IFR so the right processes are put in place to ensure compliance.

But the decision about which identity proofing model to implement, how to manage logical access controls, and what two-factor authentication method(s) to use must also be made from a user satisfaction perspective. If the processes and technologies to support them are cumbersome and overly complex for clinical and/or IT staff, it could stifle EPCS adoption.

Imprivata Confirm IDTM for EPCS is the most comprehensive solution for meeting DEA and state-level requirements for EPCS while giving practitioners a fast, convenient e-prescribing workflow. Imprivata Confirm ID for EPCS:

- Streamlines individual and institutional identity proofing,
- Enables supervised enrollment of practitioners' two-factor authentication credentials
- Automates logical access controls workflows
- Delivers the most extensive portfolio of innovative, convenient two- factor authentication methods—including Hands Free Authentication, push token notification, and fingerprint biometrics

Imprivata Confirm ID for EPCS is a robust, end-to-end platform for meeting the DEA requirements for EPCS and enabling a single, efficient, and consistent e-prescribing workflow for all medications, which ensures regulatory compliance and drives adoption of EPCS.

For more information, visit **https://www.imprivata.com/epcs**

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 ofinteroperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage andsecure 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

WP-CID-EPCS-Identity-Proofing-0123