Electronic Prescribing of Controlled Substances: Establishing a secure, auditable chain of trust

Imprivata Confirm ID and the DEA Interim Final Rule on EPCS

Technology requirements to comply with the DEA criteria for EPCS include:

- A method for identity proofing prescribers.

- The ability to assign different access levels to prescribers.

- Two-factor authentication for prescription signing that includes two of the following modalities: something you have, something you are, or something you know.

- Controls on prescriptions to prevent signed orders from being changed or allowing duplicate orders to be filled.

- Ongoing audit trail for all activities from identity proofing to prescription signing.

- Auditing and reporting for all discrepancies (such as unauthorized access attempts).

The primary objective of the DEA Interim Final Rule (IFR) allowing electronic prescribing of controlled substances (EPCS) is to help healthcare organizations reduce the potential for diversion, and subsequent abuse, of controlled medications. In accordance with this objective, the DEA IFR is designed to ensure that a provider is legally authorized to prescribe controlled substances and,thorough authentication credentialing, that only verified providers can order electronic prescriptions.

Imprivata Confirm ID™ helps organizations meet these requirements by establishing a secure, auditable chain of trust for the entire EPCS process. Imprivata Confirm ID streamlines provider identity proofing, supports supervised enrollment, and offers two-factor authentication for prescription signing. Imprivata Confirm ID meets regulatory requirements and gives care providers a fast, secure, and easy-to-use solution for prescribing controlled substances electronically.

This paper describes how Imprivata Confirm ID addresses the DEA authentication requirements for EPCS. Full compliance requires a combination of processes and technologies beyond the scope of this paper, however. For a more detailed discussion on the practices, see A Quick Guide to EPCS.

How Imprivata Confirm ID Creates a Secure, Auditable Chain of Trust

The DEA IFR contains a number of requirements designed to track and audit the connection between practitioners and the signatures they use to order electronic prescriptions for controlled substances. Imprivata Confirm ID helps secure, audit, and verify this end-to-end process, starting with identity proofing and extending to the act of signing prescriptions. Figure 1 shows the end-to-end EPCS process and the aspects addressed by Imprivata Confirm ID.
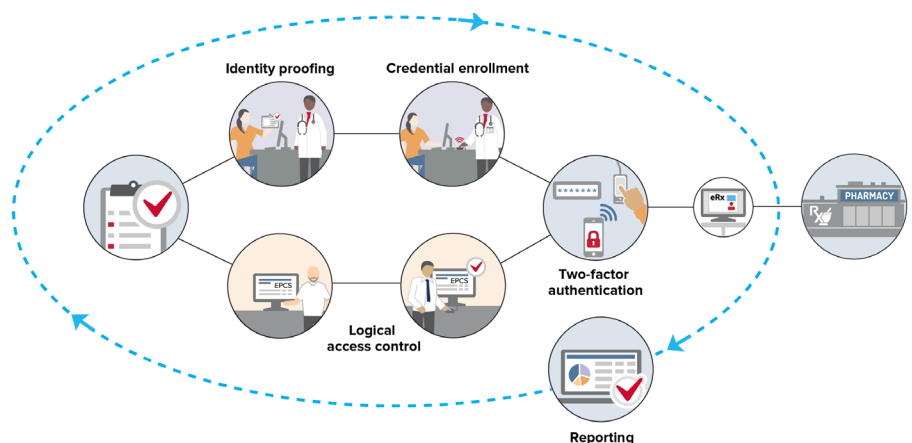

Figure 1: Imprivata Confirm ID helps organizations meet several key DEA requirements for EPCS

Imprivata Confirm ID supports each phase of this process through a combination of processes and technologies, including:

- Streamlined identify proofing (institutional and individual)

- Supervised enrollment of authorized prescribers

- Fingerprint biometrics (meeting FIPS-201 Personal Identity Verification requirements), Hands Free Authentication, and hard and soft tokens

- Comprehensive auditing and retention of permissions and authorized two-factor authentication credentials

- Complete audit reports

- Integration with leading EMR systems and e-prescribing applications

Identity Proofing

To enable EPCS, the DEA IFR requires confirmation of the identity of all providers authorized to prescribe controlled substances. The rule allows two types of identity proofing: institutional (hospitals can identity proof providers internally) or individual (providers can use a third-party credential service provider).

For institutions, Imprivata Confirm ID streamlines the identity-proofing process by enabling administrators to easily assign specific roles and responsibilities for identity proofing and retaining records for audit and reporting purposes.

For individual practitioners, Imprivata Confirm ID integrates with GSA-approved third-party credential service providers to satisfy the DEA identity-proofing requirements for EPCS.

Access Control

After identity proofing, hospitals and institutions must give practitioners appropriate access controls for e-prescribing systems, as well as two-factor authentication credentials (described in the next section). For DEA compliance, at least two separate individuals must be involved in approving or changing access controls for individual providers. Imprivata Confirm ID provides dedicated signing workflows for the approval process and audits all approval process events.

For individual practices and non-institutional registrants, the individual who receives the identity proofing and credentials from a GSA-approved third-party credential service provider uses those credentials to set access controls for other members of the practice.

Imprivata Confirm ID provides dedicated signing workflows for the approval process and audits all approval process events.

Imprivata Confirm ID helps hospitals and practices link the physical identity of authorized prescribers to their electronic prescriptions for controlled substances.

Supervised Enrollment
Imprivata Confirm ID streamlines the process of enrolling credentials for providers once they have been sufficiently identity-proofed. This includes enrolling their credentials to align with the two-factor authentication modalities they are permitted to use for EPCS. Administrators can assign individuals responsible for supervised enrollment, separating them from individuals in charge of identity proofing (as mandated by the DEA IFR). Because this process is also automated, administrators can provide a complete audit trail to demonstrate compliance.

Two-Factor Authentication
The DEA EPCS requirements mandate that two of the following approved authentication modalities be used when signing a prescription:

- Something the prescriber knows (such as a password or knowledge question)

- Something the prescriber has (such as a token or phone)

- Something the prescriber is (a biometric, such as a fingerprint scan)

Imprivata Confirm ID supports the broadest range of two-factor authentication modalities allowed by the DEA for EPCS, giving organizations the flexibility to select the two-factor authentication option that best fits provider workflow requirements based on how, when, and where EPCS will take place. Supported modalities include:

One-Time Password Tokens
Imprivata Confirm ID supports the option of using tokens that generate one-time passwords (OTPs). Imprivata Confirm ID provides out of the box support for FIPS 140-2 compliant OTPs. Using this approach, a physician carries a small hardware device that generates an OTP as a second authentication factor, functioning as the "something the prescriber has" modality.

Hands Free Authentication
This breakthrough solution delivers exceptional speed, convenience, and security for providers. It wirelessly retrieves a secure one time password (OTP) from the Imprivata ID software application on a prescriber's mobile phone without requiring any manual interaction. This approach completely eliminates the need for prescribers to handle tokens or phones, or to type their secure OTP at their endpoint device during the authentication process. Hands Free Authentication improves prescriber convenience while minimizing disruptions to clinical workflows.

Hands Free Authentication is unique, patent protected, and compliant with the DEA's requirements for EPCS. The communication channel it sets up between a prescriber's phone and endpoint uses a DEA-compliant cryptographic architecture to wirelessly transfer the OTP between the devices.

No other solution securely retrieves an OTP from a device without some form of manual intervention. By automatically retrieving the OTP from the prescriber's mobile phone, Hands Free Authentication solves the frustration of manual tokens while offering both convenience and security.

Hands Free Authentication provides a fast second factor of authentication functioning as the "something the prescriber has" modality.

Biometric Authentication
The DEA IFR mandates that the biometrics used for EPCS must meet FIPS-201 Personal Identity Verification (PIV) requirements and have a false match rate of less than 1 in 1,000. Imprivata Confirm ID offers a fingerprint biometric authentication that meets FIPS-201 requirements.

Imprivata uses HTTPS between the client device and the server to secure biometric data in transit between authorized systems. All biometric data is transmitted using symmetric encryption and secured on the server using AES encryption. Further, templates are sent to the Imprivata Confirm ID server within the context of a proprietary session. The server maintains session state, and only accepts the template for authentication once per session. This design protects EPCS systems from replay attacks that capture data and attempt to use it later.

One-Time Password Tokens
Imprivata Confirm ID supports the option of using tokens that generate OTPs. Imprivata Confirm ID provides out of the box support for FIPS 140-2 compliant OTPs. Using this approach, a physician carries a small hardware device that generates an OTP as a second authentication factor, functioning as the "something the prescriber has" modality.

Auditing and Reporting
Imprivata Confirm ID offers detailed reporting capabilities to establish a secure, auditable chain of trust for the entire EPCS process. Imprivata Confirm ID helps organizations demonstrate and prove compliance with DEA and state-level EPCS requirements by delivering comprehensive reports that document the identity proofing, supervised enrollment, and prescription signing processes, including unauthorized access attempts and other potential discrepancies. Imprivata Confirm ID also stores audit records for at least two years to meet DEA specifications, but this timeframe can be configured for longer record keeping periods, in accordance with individual state requirements.

Imprivata Confirm ID streamlines the process of enrolling credentials for providers once they have been sufficiently identity-proofed.

imprivata®

About Imprivata

Imprivata, the healthcare IT security company, enables healthcare globally to access, communicate, and transact patient information, securely and conveniently. The Imprivata platform addresses 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

Summary

Imprivata Confirm ID is a fast, secure solution that creates an auditable chain of trust for the entire EPCS process. Imprivata Confirm ID helps hospitals and practices link the physical identity of authorized prescribers to their electronic prescriptions for controlled substances. It streamlines provider identity-proofing, enables supervised enrollment, and enforces two-factor authentication requirements for prescription signing while maintaining a comprehensive audit trail throughout the entire EPCS process.

For more information, visit www.imprivata.com/EPCS.