DATASHEET

imprivata®

Key considerations when selecting a two-factor authentication solution for EPCS

The best solutions offer ease-of-use, flexibility, and a variety of different authentication options to balance security and DEA compliance with efficiency for providers

The DEA requirements for electronic prescribing for controlled substances (EPCS) include two-factor authentication to improve security and combat fraud. When signing an EPCS order, prescribers must enter a combination of two of the following:

- Something the prescriber knows (such as a password)
- Something the prescriber has (such as a token)
- Something the prescriber is (such as a biometric)

Requiring two-factor authentication for every controlled substance prescription could be cumbersome to providers, creating inefficiency and a stifling EPCS adoption. When selecting the right two-factor authentication options for EPCS, there are several key considerations, including:

Key considerations

- Ease-of-use for providers to make authentication seamless
- Comprehensive options to meet all users' requirements
- Flexibility to adapt authentication options to any given prescribing scenario
- Redundancy to enable backup options

- **Ease-of-use –** The two-factor authentication workflow for EPCS should be fast and easy for providers, because if it isn't, it could create inefficiencies that frustrate providers and barriers to 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 as 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

To help you decide which authentication options are best for your organization, the following tables describe the different options available for EPCS, the ideal workflow use-cases, the benefits and challenges of each, and the relative efficiency and benefits of every possible combination.

Two-factor authentication considerations

Hardware token							
Use case/ workflow examples	**Password**	**FIPS-compliant biometric**	**Manual (hard/soft)**	**Hands free authentication**	**Push token**	**Benefits/ challenges**	**Relative speed and convenience**
Physician prescribing within the hospital (i.e., in a patient exam room, on a shared workstation		✓		✓		• Fastest authentication • No disruption to workflow	●●●●●
		✓			✓	• Fast – swipe fingerprint and approve the push notification • Minimal disruption to workflow	●●●●◐
	✓			✓		• Fast – type password and done • Minimal disruption for workflow	●●●●○
	✓	✓				• Fast – type password and touch finger • Slower than Hands Free Authentication, but fastest workflow when HFA is not available	●●●◐○
	✓				✓	• Slower – type password and approve the push notification • Some disruption to workflow	●●●◐○
		✓	✓			• Slower – swipe fingerprint and type the push notification • Some disruption to workflow	●●●◐○
	✓		✓			• Slowest–type password and type OTP code from token • Most disruptive to workflow	●○○○○

Hardware token							
Use case/ workflow examples	**Password**	**FIPS-compliant biometric**	**Manual (hard/soft)**	**Hands free authentication**	**Push token**	**Benefits/ challenges**	**Relative speed and convenience**
Physician prescribing remotely (i.e., at home, at their remote office, etc.)	✓	Typically unavailable		Typically unavailable	✓	• Slower – type password and approve the push notification • Some disruption to workflow but fastest workflow when HFA is not available	
	✓		✓			• Slowest– type password and type OTP code from token • Most disruptive to workflow	

Imprivata Confirm ID: The most innovative, convenient authentication options for EPCS

Imprivata Confirm IDTM supports the broadest range of innovative, convenient, and DEA-compliant authentication options, including fingerprint biometrics, Hands Free Authentication, and push token notification. This gives providers a fast, seamless two-factor authentication workflow to improve efficiency and drive EPCS adoption. Imprivata Confirm ID also gives your providers the flexibility to use the options that best meet their workflow requirements in any given scenario.

Imprivata Confirm ID is also the most complete, end-to-end platform for meeting the DEA requirements for EPCS and enabling a single, efficient, and consistent e-prescribing workflow for all medications. Imprivata Confirm ID:

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

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

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

CID-DS-key-considerations-1222