



ID.me

Physician Identity Proofing

ELECTRONIC PRESCRIPTION OF CONTROLLED SUBSTANCES (EPCS)

Get Compliant

The Drug Enforcement Administration mandated a NIST 800-63 certified identity proofing and authentication process for physicians digitally prescribing controlled substances to help mitigate the current opioid crisis. ID.me will get your prescribers compliant at the highest level by seamlessly integrating our identity verification solution into your existing workflow.

While virtually all EHRs are enabled for EPCS, the SUPPORT Act mandates that each prescriber must be set up with identity proofing and two-factor authentication. Your EHR vendor can provide compatible options and implementation approaches.

HOW WE DO IT



NIST 800-63-3 CERTIFIED We meet IAL2 / AAL2 identity proofing and authentication standards that comply with DEA, HHS, and state-level requirements.



ONLINE, IN-PERSON, AND VIRTUAL IN-PERSON PROOFING

- Online: simple integrated solution fits into your existing digital workflow
- In-Person: conducted by trained administrative staff via our ID.me Trusted Referee mobile app
- Virtual In-Person: conducted via live video chat with an ID.me Trusted Referee



LOGIN ONCE Once a user has verified their identity with ID.me, they will not have to verify their identity again for any organization integrated with ID.me.



DEA institutes NIST 800-63 compliance



An effort to mitigate the opioid crisis



ID.me gets prescribers compliant



ID.me easily and seamlessly integrates with your workflow

HOW IT WORKS

1 Sign up

The screen shows the ID.me Sign Up form. It includes fields for Email, Password, and Confirm Password. There are checkboxes for accepting terms and privacy policy. Below the form are social media login options for Facebook, Google, and LinkedIn, and a link for other sign up options. At the bottom, there are links for 'What is ID.me?', 'Terms of Service', and 'Privacy Policy'.

If you already have an ID.me account, simply sign in.

2 Secure Account

The screen is titled 'SECURE YOUR ACCOUNT'. It explains that adding an extra layer of security (2-factor authentication) is required. It offers three options: Push Notification, Code Generator, and FIDO U2F Security Key. A fourth option, Mobile YubiKey, is also listed with a note that the ID.me Authenticator app is required. A 'No I don't want to secure my account at this time' link is at the bottom.

Add an additional layer of security using two-factor authentication to strengthen access security.

3 Verify Identity

The screen is titled 'TAKE PHOTOS OF YOUR DRIVER'S LICENSE'. It shows two examples of driver's licenses with a 'Retake' button and a checkmark. At the bottom is a 'Look good?' button.

These options may include: Driver's License, state issued identification, Passport, Passport Card, or questions based on your credit history.

4 Medical Credential Check

The screen is titled 'Verify as a medical provider'. It asks for NPI and DEA numbers. It includes explanatory text for NPI and DEA numbers. There are input fields for NPI Number and DEA Number, and a checkbox for institutional DEA registration. At the bottom, there are radio buttons for DEA Schedule (I, II, III, IV, V) and 'Back' and 'Continue' buttons.

If your Health IT provider chooses to have ID.me verify your Medical Credentials, these steps will be prompted in the workflow. (Optional)

5 Allow Consent

The screen is titled 'Authorize ID.me'. It asks for permission to share verified identity information with RXNow. It lists the information RXNow will receive: Email, Full Name, SSN, Phone, DEA Schedule(s), NPI Number, Issuing State, Secondary Specialty, Gender, Address, Date of Birth, DEA Number, DEA # Expiration Date, State License Number, and Primary Specialty. There are 'Allow' and 'Deny' buttons. At the bottom, there is a note that access can be removed at any time.

Give consent to share your verified identity and medical provider status back to your Health IT platform.

