

Yes, it's legal to e-prescribe controlled substances in Ohio

Ohio is involved with a national initiative to encourage the e-prescribing of controlled substances (EPCS). This effort is being led by Surescripts, the Drug Enforcement Agency (DEA), and CMS at the national level and the Ohio E-Prescribing Task Force at the state level. The process for approval of electronic health record (EHR) systems to send and pharmacy systems to receive controlled substance e-prescriptions has been established by DEA regulations (21 CFR 1311). Pursuant to **4729-5-21 and 4729-5-30 of the Ohio Administrative Code (OAC)**, systems meeting the DEA's requirements to send and receive electronic prescriptions for both controlled and non-controlled substances are considered approved by the State of Ohio Board of Pharmacy.

Here is what is needed for a controlled substance prescription to move successfully between the prescriber and the pharmacy:

1. A prescriber's EHR system must be certified and audited under the DEA process to transmit EPCS using two-factor authentication signing processes. The EHR vendor is responsible for obtaining these approvals.
2. A pharmacy's software system must be certified and audited under the DEA process to receive EPCS. The pharmacy software vendor is responsible for obtaining these approvals. A chain pharmacy corporation will typically oversee the audit process and approvals for all of its individual pharmacy locations and pharmacy software vendors will do so for independent pharmacies.
3. A prescriber must be credentialed under the DEA process to send EPCS. This step may also be referred to as "identity proofing" and is done to verify the prescriber's identity. The individual prescriber or the hospital or clinic is responsible for completing the credentialing process. If an individual prescriber does not know how to obtain credentials for EPCS, he/she should contact the practice's EHR vendor.

Facts about EPCS

Surescripts acts as an intermediary network in the EPCS transmission process for most e-prescriptions in the country. It performs additional functions to make the EPCS process as secure and transparent as possible, such as:

- Verifying pharmacy and prescriber software vendors' compliance with the DEA certification process. Only after this is completed can the prescriber EHR system or pharmacy software system connect to the Surescripts network for EPCS purposes.
- Ensuring that prescriber software vendors verify individual prescriber compliance with credentialing or identity proofing requirements.
- Requiring pharmacy system vendors to display an indication to a pharmacist confirming that the EPCS being received is DEA compliant.
- Publishing both prescriber and pharmacy directories for EPCS. These can be found at <http://getepcs.com/moredetails.html>

Institutional Practitioners Guidance for EPCS

- *The State of Ohio Board of Pharmacy is giving guidance to pharmacists that if a pharmacist is presented with a valid eRx for controlled substances (see **OAC 4729-5-30 and 4729-5-21**), the pharmacy should go ahead and fill the prescription.* The checks and balances created by the DEA and enforced by Surescripts should give a pharmacist assurance that the software certification is both current and complete to allow transmission of controlled substances.
- If a hospital or clinic is unclear whether a pharmacy can receive EPCS prescriptions, individual pharmacy DEA certification can be checked at the Surescripts site at <http://getepcs.com/moredetails.html>
- Prescriber's credentials to use EPCS are being posted by Surescripts at <http://getepcs.com/moredetails.html>
- A hospital or clinic's credentialing office can identity proof a provider for EPCS, but a separate group within the organization must set access controls for EPCS.
- Remember: DEA certification for EPCS does not replace the need for a vendor to comply with the State of Ohio Board of Pharmacy regulations for non-controlled substance eRx transmission (approvable status). Questions can be directed to the Board by email: erx@pharmacy.ohio.gov

CREREDENTIALING FOR CONTROLLED SUBSTANCE E-PRESCRIBING FOR INSTITUTIONAL PRACTITIONERS

Note: *The questions and responses below assume that the practitioner is an institutional practitioner (e.g., a hospital or clinic) and is a DEA registrant lawfully permitted to prescribe controlled substances. They further assume that the practitioner has received an audit or certification report from the application provider of the practitioner's software used to create prescriptions for controlled substances that indicates the application meets DEA's requirements.*

Question 1: *Is identity proofing required for any individual practitioner whom the institutional practitioner is granting access to issue prescriptions using the institution's electronic prescribing application? If so, who will conduct it?*

Yes, as identity proofing is critical to the security of electronic prescribing of controlled substances. DEA is allowing institutional practitioners, who are DEA registrants, to conduct the identity proofing for any individual practitioner whom the institutional practitioner is granting access to issue prescriptions using the institution's electronic prescribing application. Because institutional practitioners have credentialing offices, those offices may conduct in-person identity proofing as part of the credentialing process. Before the institutional practitioner issues the authentication credential, a person designated by the institutional practitioner must check the individual practitioner's government-issued photographic identification against the person presenting it. The institutional practitioner must also check State licensure and DEA registrations, where applicable.

Question 2: *Is an institutional practitioner required to conduct identity proofing?*

No, institutional practitioners are allowed, but not required, to conduct identity proofing. If an institutional practitioner decides to have each practitioner obtain identity proofing and the two-factor authentication credential on his or her own, as other individual practitioners do, that is permissible under DEA rule.

Question 3: *For an institutional practitioner, is remote identity proofing permissible?*

The DEA rule only allows institutional practitioners to conduct in-person identity proofing. Remote identity proofing is not permissible for institutional practitioners.

Question 4: *For an institutional practitioner, how is the two-factor authentication credential issued?*

The institutional practitioner may issue the two-factor authentication credentials or obtain them from a third party which will have to be a Credential Service Provider (CSP) or Certification Authority (CA) that meets the criteria DEA has specified. In the latter case, the institutional practitioner could have each practitioner apply for the two-factor credential himself, which would entail undergoing identity proofing by the CSP or CA. Alternatively, the institutional practitioner can serve as a trusted agent for the third party. Trusted agents conduct part of the identity proofing on behalf of the CSP or CA and submit the information for each person along with a signed agreement that specifies the trusted agent's responsibilities.

Question 5: *Why is the DEA requiring the use of two-factor authentication credentials?*

Two-factor authentication (two of the following – something you know, something you have, something you are) protects the practitioner from misuse of his/her credential by insiders as well as protecting him/her from external threats because the practitioner can retain control of a biometric or hard token. Authentication based only on knowledge factors is easily subverted because they can be observed, guessed, or hacked and used without the practitioner's knowledge.

Question 6: *What two-factor credentials will be acceptable?*

DEA is allowing the use of two of the following – something you know (a knowledge factor), something you have (a hard token stored separately from the computer being accessed), and something you are (biometric information). The hard token, if used, must be a cryptographic device or a one-time-password device that meets Federal Information Processing Standard 140-2 Security Level 1.

Question 7: What is a hard token?

A hard token is a cryptographic key stored on a hardware device (e.g., a PDA, cell phone, smart card, USB drive, one-time password device) rather than on a general purpose computer. A hard token is a tangible, physical object possessed by an individual practitioner.

Question 8: Is it permissible for a practitioner to have another staff person at the institutional practitioner maintain custody of the hard token?

No, the practitioner must retain sole possession of the hard token, where applicable, and must not share the password or other knowledge factor with any other person. The practitioner must not allow any other person to use the token or enter the knowledge factor or other identification means to sign prescriptions for controlled substances.

Question 9: If an institutional practitioner wants to use a biometric as one factor of the two-factor authentication credential issued to persons prescribing controlled substances, does DEA have any special requirements?

DEA is establishing several standards for the use of biometrics and for the testing of the software used to read the biometrics. DEA wishes to emphasize that these standards do not specify the types of biometrics that may be acceptable. Any biometric that meets the criteria DEA has specified may be used as the biometric factor in a two-factor authentication credential used to indicate that prescriptions are ready to be signed and sign controlled substance prescriptions. The use of biometrics as one factor in the two-factor authentication protocol is strictly voluntary, as is all electronic prescribing of controlled substances.

Question 10: Are any additional steps needed to give practitioners the ability to sign controlled substance prescriptions?

Once a person's identity has been confirmed by the credentialing office and a two-factor credential has been issued, another office must set access controls. The application must have the ability to assign permissions by name or role so that only authorized practitioners are allowed to sign controlled substance prescriptions. Two individuals must be involved in setting the access controls; one will enter the data based on information from the credentialing office and the second will approve the entry.

Question 11: Can controlled substance prescriptions be received in Ohio by means other than EPCS?

Pharmacists can continue to receive controlled substance prescriptions by other State of Ohio Board of Pharmacy approved routes such as signed hardcopy prescriptions and facsimile. (See **OAC 4729-5-30 for limits on CII faxing**). However, under the DEA regulations, an EPCS prescription cannot be converted into a computer-generated fax. (21 CFR 1311.170)

Question 12: Can Schedule II drugs be e-prescribed using the EPCS process?

Yes, all controlled substances, Schedule II through V, are permitted to be electronically prescribed in Ohio.