RESOURCE AND PATIENT MANAGEMENT SYSTEM

Electronic Health Record

(EHR)

EPCS Supplemental User Guide

Version 1.1 Patch 25
August 2019

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

The purpose of this manual is to provide the user with the information needed to use the new Electronic Prescribing of Controlled Substance (EPCS) function within the Indian Health Service (IHS) Resource and Patient Management System (RPMS) Electronic Health Record (EHR) that supports e-prescribing.

This manual contains reference information about new EPCS processes and step-by-step procedures to show end users how to perform activities related to Provider Profile Entry, Provider Profile Approval, and Two-factor Authentication needed to meet both Drug Enforcement Administration (DEA) and The Department of Health and Human Services (HHS) regulations. Further, it walks through the safe ordering of Controlled Substances (CS) when they are integrated into the patient's plan of care.

EPCS builds upon the already existing functionality of RPMS-EHR ordering and medication components and the outpatient pharmacy suite within RPMS. Customization of EHR layout templates is allowed; therefore, some images within this manual may differ from the user's version. However, all functionality remains consistent throughout the EPCS process.

For more information about EPCS, the DEA list of controlled substances, or other matters related to e-prescribing, users may consult the following resources:

- EHR: www.ihs.gov/ehr
- EPCS Training: https://www.ihs.gov/rpms/training
- DEA list of controlled substances: https://www.deadiversion.usdoj.gov/schedules/orangebook/e_cs_sched.pdf
- Controlled substance dispensing authority by Mid-Level Practitioners by State: https://www.deadiversion.usdoj.gov/drugreg/practioners/mlp_by_state.pdf

1.0 Introduction

In 2014, the Office of the National Coordinator (ONC) for Health Information Technologies published its second set of rules related to the adoption of standards, implementation, and certification criteria for EHR technology. IHS must meet these HHS ONC 2014 certification requirements, and EPCS has been created to accomplish this. EPCS provides enhancements to the existing electronic prescription (eRx) process within RPMS-EHR to allow for secure electronic prescribing and dispensing of Controlled Substance (CS) medications.

EPCS implements key controlled substance prescribing regulations and fulfillment screens and allows practitioners to transmit a controlled substance prescription with an approved signing function. This new feature also requires a second layer of security in addition to an electronic signature that providers must use before signing the prescription. As many IHS sites are multi-divisional, EPCS permits providers associated with many facilities to order controlled substances for patients in multiple sites. The Pharmacy component of EPCS allows controlled substances to be dispensed from internal pharmacies safely and efficiently.

By streamlining the process of ordering and fulfilling patients' prescriptions that contain controlled drugs, medication errors and prescribing misuses may be minimized, if not avoided. EPCS supports other care-related activities directly or indirectly through various interfaces, including provider-profile credentialing for prescribing controlled medications electronically, pharmacy management and tracking of controlled substances, and patient medication management.

EPCS, along with the implementation of electronic health records, supports the continued progress of healthcare that strengthens the relationship between patients and clinicians. The ability to retrieve timely data from this system will enable providers to make better decisions and provide better care, while ensuring that patients receive the medications they need to control their pain or improve their health.

EPCS is designed for outpatient prescriptions only. Inpatient prescriptions for controlled substances do not require EPCS however, when ordering a CS medication for an inpatient, the provider must have authority for the schedule of the selected CS medication. Outpatient prescriptions that are sent by paper to internal or external pharmacies do not require two-factor authentication.

EPCS allows multiple functions to be performed, which are explained in further detail throughout this User Manual, and include, but are not limited to:

- Approving or editing providers' profiles for EPCS implementation
- Electronic ordering of CS medications

- Signing certificate requirements for providing access controls and authenticating medication orders
- Transmission of electronic prescriptions through Surescripts, if site is authorized to do so
- Receiving of renewal requests from Surescripts for controlled substances if site is authorized to do so

1.1 Key Terms and Definitions

There are several key terms related to EPCS which should be understood prior to reading the remainder of this User Manual:

- Two-Factor Authentication (2FA): A type of Multi-factor authentication. This term indicates that a user must authenticate using two different methods. The most recognizable example for the average user will be an ATM, where you must have both a card and a PIN to get cash. If only one method is presented, no cash is dispensed. The most common methods of authentication are:
  - something you have, such as a card or token
  - something you know, such as a password or PIN, or
  - something you are, such as a fingerprint or facial scan.
- Digital Signature: In the EPCS regulations, this is defined as “a record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate.” Each provider wishing to use EPCS must obtain a digital signing certificate from an IHS-authorized vendor. In addition, the staff who will be verifying the provider’s EPCS profiles will also need a digital signing certificate.
- Electronic Signature: In the EPCS regulations, this is defined as “a method of signing an electronic message that identifies a particular person as the source of the message and indicates the person's approval of the information contained in the message.”
- Electronic Signature Code: This term is used within RPMS and EHR to refer to the specialized password used to apply an electronic signature as defined previously to an item such as an order or a note.
- Hash: A hash as it relates to EPCS, in extremely simplified terms, is a numerical representation of certain aspects of the order as it was created and signed by the provider. It is set at the time the provider signs the order, transmitted with the order to the internal pharmacy, then checked (by recalculating from the aspects used to create the hash initially) at the time the pharmacy processes the order. When the hash calculation at processing does not match the hash set at signing, it indicates that the order has been tampered with or corrupted in transmission. It is important to remember that not all hash mismatches indicate deliberate tampering.

- PIV: The Personal Identity Verification card issued through the Indian Health Service that contains certificates issued by the Health and Human Services Federal Public Key Infrastructure (HHS-FPKI). This is the standard PIV card issued to IHS employees and contractors.
- Token: The device that holds the certificate used for authentication and the digital signing of CS medication order. For the purposes of EPCS, this can be a USB Cryptographic Token issued by an approved credential service provider or a PIV card issued through Health and Human Services.

2.0 Credentialing/Provider Profile Access

The process of approving providers for using the EPCS system is detailed and includes steps not performed in EHR or RPMS. These steps and the required separation of duties are outlined in this section, in addition to the specific steps performed within the EHR.

Before a provider is able to electronically order controlled substances, there is a process of traditional credentialing (e.g., licensure verification), identity proofing and certificate issuance, and then creation of a **Provider Profile** within the RPMS-EHR system where the provider will be practicing. There are strict requirements for separation of duties within these functions. Per regulations, one group must perform the identity proofing and traditional credentialing and propose a user for access (e.g., filling out an Information Technology Access Control (ITAC) form to request RPMS access). While IHS facilities will use an outside vendor for the full identity proofing and certificate issuance, it is likely that the remaining functions will be performed by the same group that currently does the traditional credentialing within the facility. One person within this group will propose a provider for EPCS access, and a second person within this group must approve the provider for access.

The provider’s information is then passed along to a second, completely separate group who will create and verify the provider profile within the RPMS-EHR system. This is known as EPCS credentialing and should not be confused with the “traditional” credentialing described above. The provider profile must be entered into the new EPCS Credentialing component that reflects key information needed for electronically ordering and signing CS medications. References in this manual to “credentialing” from here on out will be referring to this EPCS credentialing process, and not the traditional credentialing a site is already performing.

Note: Once a provider is enabled for EPCS, all provider edits involving a user’s DEA or VA number, allowed schedules, DEA expiration date, and other EPCS related fields as described elsewhere in this manual should be performed in the EPCS Credentialing component in the EHR. Editing these fields in the RPMS database directly may be disallowed or cause the provider to fail the checks for electronic prescribing of CS medications.

It is vital that the group proposing and approving a provider for EPCS and the group creating and verifying a provider profile for EPCS be completely separate people within the organization. Within each group, a user may perform each function, but may not complete both functions on the same provider. This means that a credentialing individual must not both propose for access and approve the access for the same provider, and a provider profile individual may not both create and verify a profile for the same provider.

Note: As IHS users and facilities configure the RPMS-EHR differently, the images of the components and functions depicted in this guide may differ in appearance and location from those at your site. However, the EPCS credentialing functions and ordering of controlled substances follow the same process flow as depicted.

2.1 Security Keys

There are two security keys for provider profile users. The first is the **XUEPCSEDIT** key and should be given to the provider profile group user or users who will create the provider profile in the EPCS Credentialing component. These users are known as EPCS Provider Profile Admins or PPAs.

The second is the **XUZEPCSVERIFY** key, which should be given to the user or users who will verify the profiles that have been created. These users are known as EPCS Provider Access Admins or PAAs. The PAA must have a cryptographic token and digital signing certificate, or PIV card and reader if the site elects to use PIV cards for EPCS. If a verifier is also a provider, a single token and certificate or PIV card is used for both functions.

Note: The following process is only for users who are becoming credentialers and do not already have certificates linked in RPMS. If a user has already been credentialed through the EPCS Credentialing component (e.g., as a provider) and has a certificate linked, they only need to have the XUZEPCSVERIFY key added and they are ready to perform as a PAA. Key assignments are tracked in the EPCS Audit Log events.

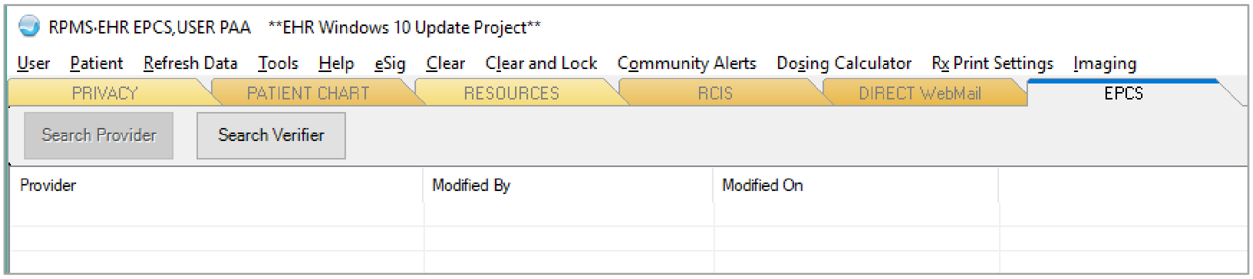
2.2 Set Up an EPCS Provider Access Admin

Beyond the security key noted previously, the PAA user must have a signing certificate linked to their RPMS user file. This is accomplished through the EPCS Credentialing component in the EHR. Another PAA must link the certificate; you cannot link a certificate to your own user. In the initial set up, the first two users identified to perform the PAA duties will have to set each other up in round-robin fashion. This process does require physical access to the cryptographic token or PIV of the user who is being set up.

To link a certificate:

1. Log on to the RPMS-EHR system as a PAA user.

2. Navigate to and select the new credentialing module. In the demo system displayed here, the component has been added to a tab called **EPCS** as seen in Figure 2-1.

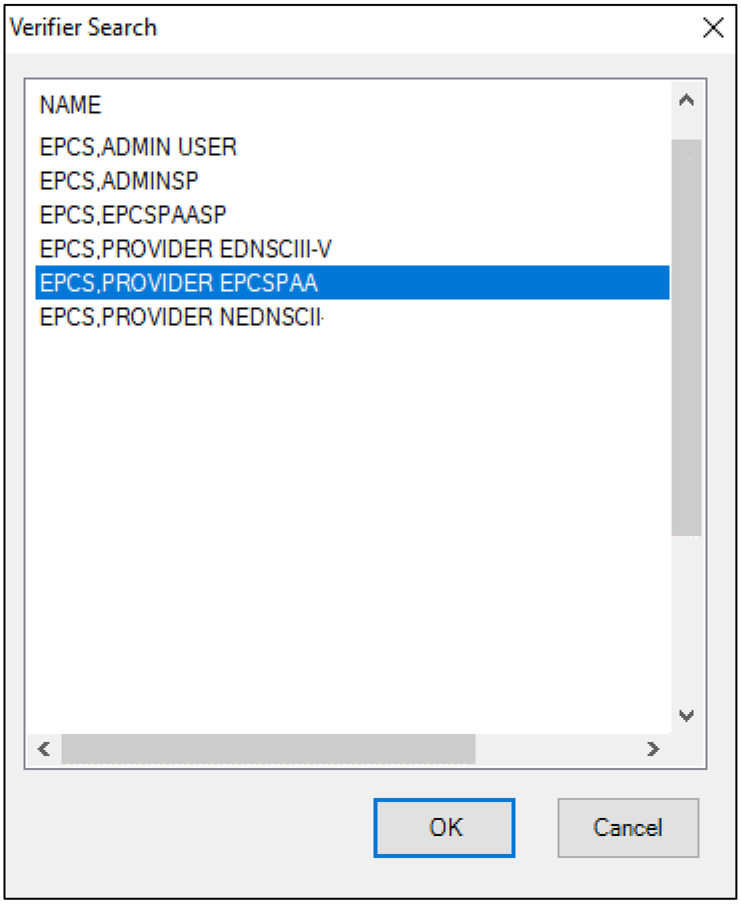

RPMS-EHR EPCS,USER PAA **EHR Windows 10 Update Project**
User Patient Refresh Data Tools Help eSig Clear Clear and Lock Community Alerts Dosing Calculator Rx Print Settings Imaging
PRIVACY PATIENT CHART RESOURCES RCIS DIRECT WebMail EPCS
Search Provider
Search Verifier

Provider	Modified By	Modified On

Figure 2-1: EPCS Credentialing component with PAA user logged in

3. Click the S**earch Verifier** button. The **Verifier Search** dialog opens.

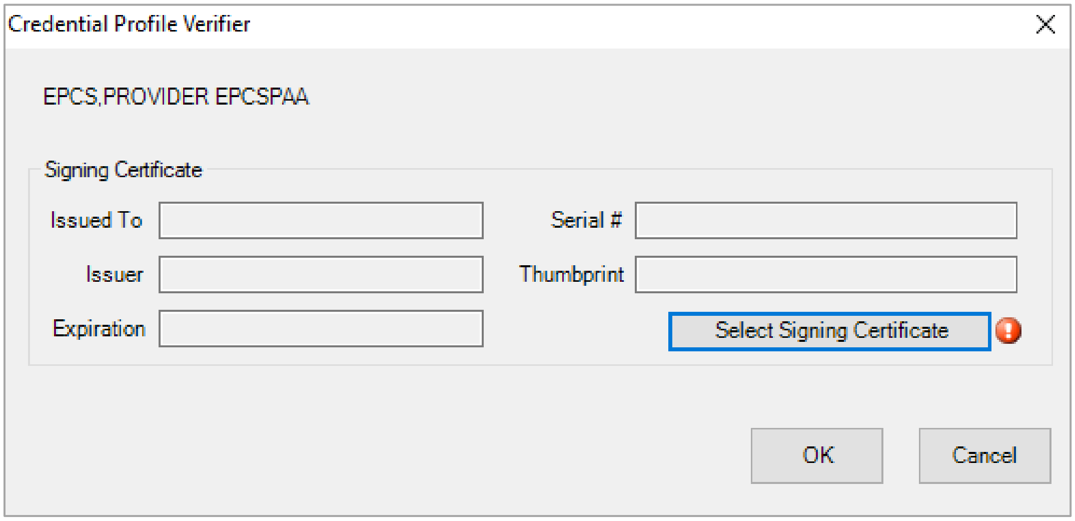
4. Select the PAA user from the list and click **OK**. Only users holding the verify key and who are not the logged-in user will display in the list.



NAME
EPCS,ADMIN USER
EPCS,ADMINSP
EPCS,EPCSPAASP
EPCS,PROVIDER EDNSCIII-V
EPCS,PROVIDER EPCSPAA
EPCS,PROVIDER NEDNSCII

Figure 2-2: Verifier Search dialog

5. The **Credential Profile Verifier** dialog opens. The only option is **Select Signing Certificate**.



EPCS,PROVIDER EPCSPAA

Figure 2-3: Credential Profile Verifier dialog

6. Insert the proposed PAA user's cryptographic token or PIV into the computer being used to set up the PAA user. Click **Select Signing Certificate** and then choose to select from **Verifier's Certs** (preferred) or **All Certs**. The **All Certs** option should only be used if **Verifier's Certs** does not return the correct Certificate. This may occur if the name on the certificate does not exactly match the name in RPMS. Some examples include:

    - RPMS uses full first and middle names, but the certificate uses full first name and middle initial (example: Jo Dee Smith vs. Jo D. Smith).
    - RPMS uses a middle name as the user's preferred name, but the certificate has the full legal name (example: Elizabeth Anne Smith goes by Anne Smith; RPMS uses Anne Smith but the certificate has Elizabeth Anne Smith).
    - RPMS uses a diminutive form of a name while the certificate uses the full legal name (example: James Smith goes by Jim; RPMS has Jim Smith and the certificate has James Smith).

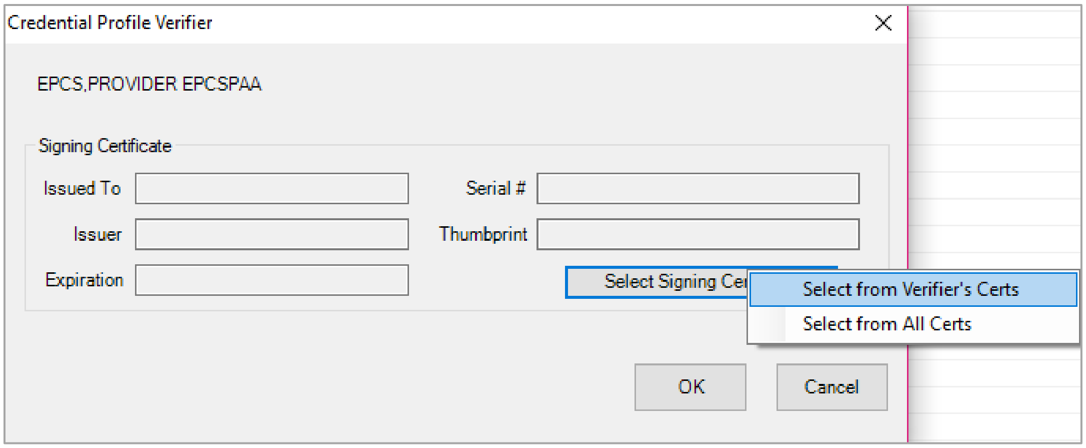
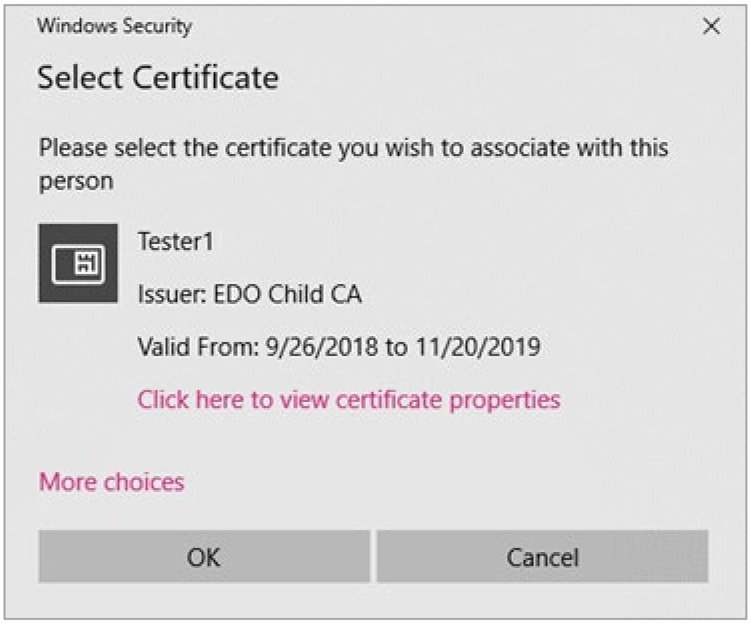


Figure 2-4: Select Signing Certificate options – Select from Verifier's Certs or Select from All Certs

7. Choose the appropriate certificate, making sure the certificate belongs to the user being credentialed, and click **OK**. The window may look different on different versions of the Windows operating system. An example certificate used in internal testing is shown in Figure 2-5. HHS issued PIV cards and certificates contain the HHS initials, IdenTrust certificates contain IGC initials, and Widepoint ORC certificates contain ORC initials. If IHS expands to use other vendors, there will be some identifying characteristics in the certificate names.



Please select the certificate you wish to associate with this person

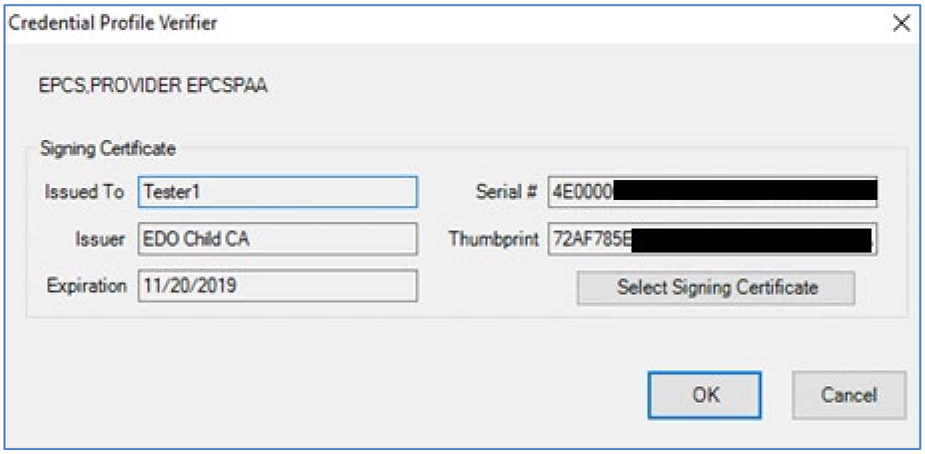
Tester1

Issuer: EDO Child CA

Valid From: 9/26/2018 to 11/20/2019

Figure 2-5: Windows Security Select Certificate window in Windows 10

8. The **Credential Profile Verifier** dialog now displays with information filled in. Ensure the **Issued To**, **Issuer**, **Expiration**, **Serial #**, and **Thumbprint** fields are filled in. These cannot be manually entered or edited, so if missing, re-select a signing certificate. Note that the software will prevent an already expired certificate from being added.



Credential Profile Verifier

EPCS,PROVIDER EPCSPAA

Signing Certificate

Issued To: Tester1

Issuer: EDO Child CA

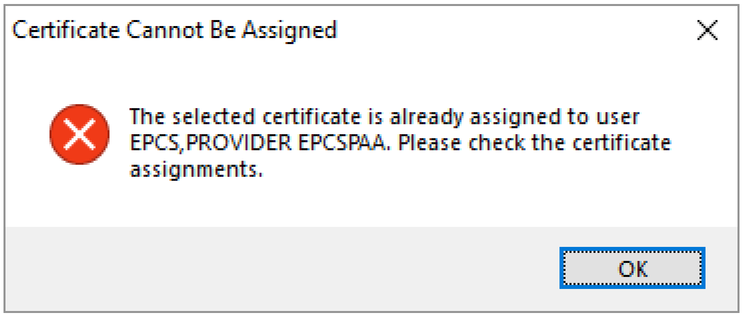
Expiration: 11/20/2019

Serial #: 4E0000[redacted]

Thumbprint: 72AF785E[redacted]

Figure 2-6: Issued To, Issuer, Expiration, Serial #, and Thumbprint fields filled (partially masked for privacy)

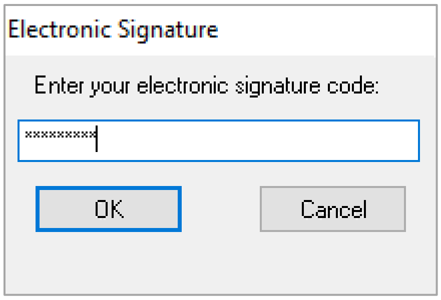
9. Click **OK**. If the selected certificate is already assigned to another user, the **Certificate Cannot Be Assigned** error message displays, similar to the one in Figure 2-7. Otherwise, the **Electronic Signature Code** dialog displays as in Figure 2-8. Enter the logged-in user's **Electronic Signature Code** and click **OK**.



Certificate Cannot Be Assigned

The selected certificate is already assigned to user EPCS,PROVIDER EPCSPAA. Please check the certificate assignments.

Figure 2-7: Certificate Cannot Be Assigned error message



Electronic Signature

Enter your electronic signature code:

****

Figure 2-8: Electronic Signature dialog

10. The Verifier is now set up, as evidenced by the **Credential Profile Verifier** dialog closing.

2.3 Create a Provider Profile

The information needed to create the initial Provider Profile includes the following:

- Provider’s DEA Number or VA Number
- Provider’s DEA Expiration Date
- Provider’s DEA X Number (also known as the Narcotic Addiction DEA Number or NADEAN), if they have one.
- The list of controlled substance schedules for which the provider is authorized to order
- Provider’s signing certificate

When a provider profile is created and verified, it creates a hash, which is a way to ensure that the information that has been verified is not altered by an unauthorized user or corrupted in any way. The following fields are used to calculate a hash:

- DEA #
- VA#
- DEA X Number (sometimes listed as DETOX/MAINTENANCE ID NUMBER)
- SCHEDULE II NARCOTIC
- SCHEDULE II NON-NARCOTIC
- SCHEDULE III NARCOTIC
- SCHEDULE III NON-NARCOTIC
- SCHEDULE IV
- SCHEDULE V
- DEA# EXPIRATION DATE

> **Note:** Editing these hash fields outside of the EPCS Credentialing component will cause a hash mismatch and the user will be required to use paper ink-signed orders until the profile is corrected by being re-created and verified in the EPCS Credentialing component. Editing these fields in RPMS for users who are not EPCS enabled is still acceptable.

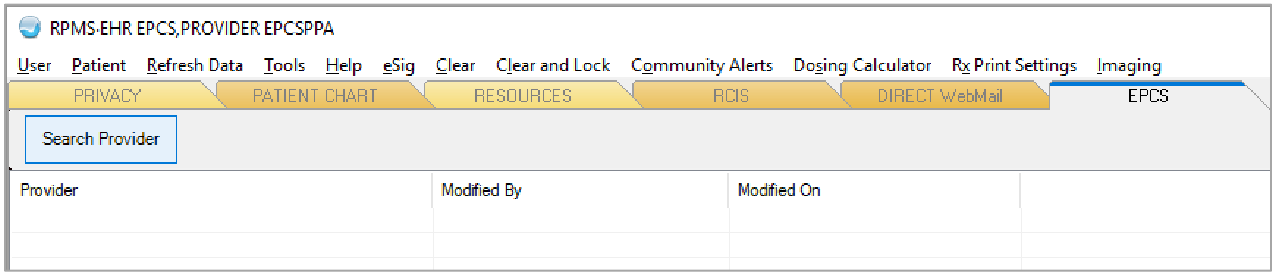
Additionally, there are hashes created using the serial number and thumbprint of the signing certificates and their status is updated every four hours. Changes to these items in RPMS will also cause mismatches that will prevent the user from signing CS orders or verifying EPCS profiles.

To create the Provider Profile:

1. Logon to the RPMS-EHR system.

> **Note:** Your view and location of newly added EPCS screens and fields may differ from those represented within this user manual depending upon your facility's configuration of RPMS-EHR.

2. Navigate to and select the new credentialing module. In the demo system displayed here, the component has been added to a tab called **EPCS** as seen in Figure 2-9.

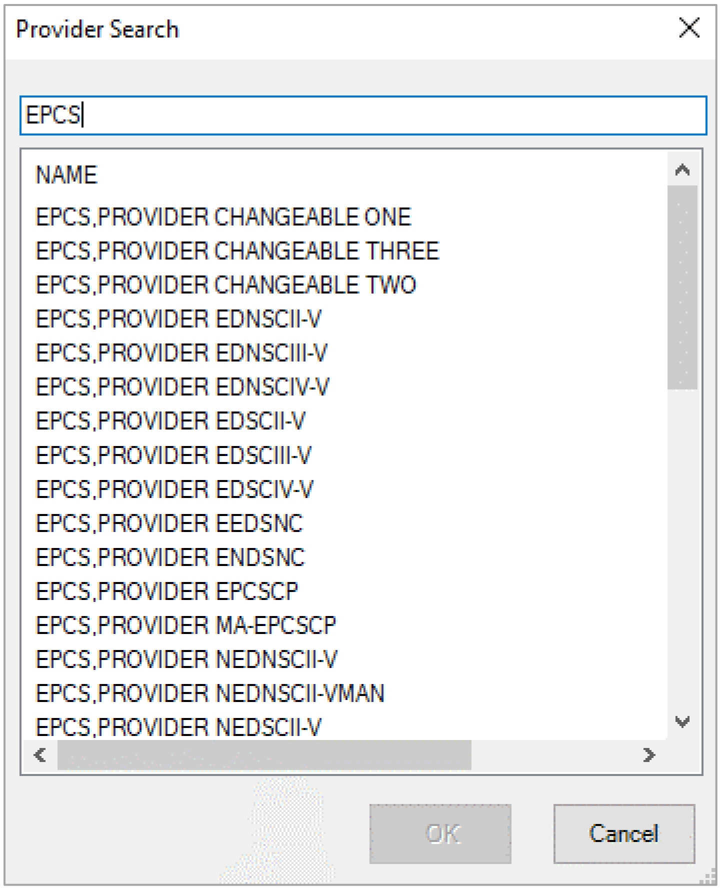

RPMS-EHR EPCS,PROVIDER EPCSPPA
User Patient Refresh Data Tools Help eSig Clear Clear and Lock Community Alerts Dosing Calculator Rx Print Settings Imaging
PRIVACY
PATIENT CHART
RESOURCES
RCIS
DIRECT WebMail
EPCS
Search Provider

Provider	Modified By	Modified On

Figure 2-9: EPCS Module

3. Click the **Search Provider** button in the toolbar. The **Search Provider** button is only enabled if the individual has been assigned the XUEPCSEDIT security key. If the user also holds the verify key, the **Search Verifier** button will also display.

4. The **Provider Search** window opens displaying a list of providers. The window will display a list of the users holding the ORES security key. The PPA user may optionally type in one (1) or more characters in the search box to jump to the portion of the list matching the entered text or use the vertical scroll bar to find the provider. Double-click the name of the desired provider; alternately select the name by clicking once and then click **OK**. If the provider selected already has pending changes from a different PPA user, the system will display a warning stating "Edit disabled" and "There are some pending changes to the profile." In this case, the profile will open but no changes will be able to be saved to the profile.

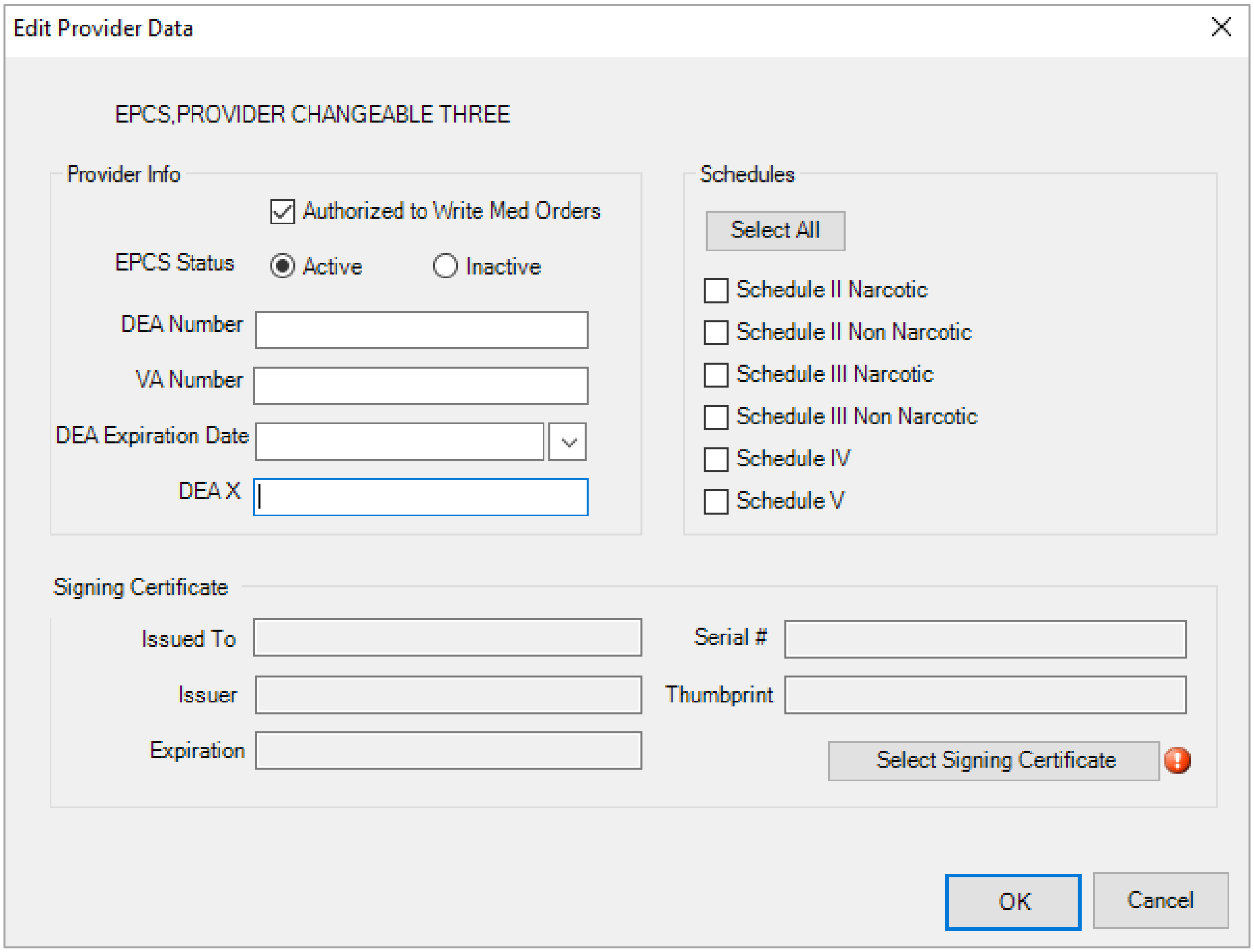


EPCS

NAME
EPCS,PROVIDER CHANGEABLE ONE
EPCS,PROVIDER CHANGEABLE THREE
EPCS,PROVIDER CHANGEABLE TWO
EPCS,PROVIDER EDNSCII-V
EPCS,PROVIDER EDNSCIII-V
EPCS,PROVIDER EDNSCIV-V
EPCS,PROVIDER EDSCII-V
EPCS,PROVIDER EDSCIII-V
EPCS,PROVIDER EDSCIV-V
EPCS,PROVIDER EEDSNC
EPCS,PROVIDER ENDSNC
EPCS,PROVIDER EPCSCP
EPCS,PROVIDER MA-EPCSCP
EPCS,PROVIDER NEDNSCII-V
EPCS,PROVIDER NEDNSCII-VMAN
EPCS,PROVIDER NEDSCII-V

Figure 2-10: Provider Search window

5. The **Edit Provider Data** window displays. If the user has no data for the EPCS related fields, the fields will be empty. If the user had been set up in RPMS prior to EPCS, then any data already present will display in the appropriate fields.



Edit Provider Data

EPCS,PROVIDER CHANGEABLE THREE

Provider Info

☑ Authorized to Write Med Orders

EPCS Status ● Active ○ Inactive

DEA Number

VA Number

DEA Expiration Date

DEA X

Schedules

□ Schedule II Narcotic

□ Schedule II Non Narcotic

□ Schedule III Narcotic

□ Schedule III Non Narcotic

□ Schedule IV

□ Schedule V

Signing Certificate

Issued To

Serial #

Issuer

Thumbprint

Expiration

Figure 2-11: Edit Provider Data window

6. Enter data for all the fields in this window that apply to the provider.

> **Note:** The **Edit Provider Data** window will not prevent you from leaving field elements blank. However, when a provider is ordering CS medications, EPCS checks for these fields and might prevent the provider from placing orders if certain fields are blank, as noted herein.

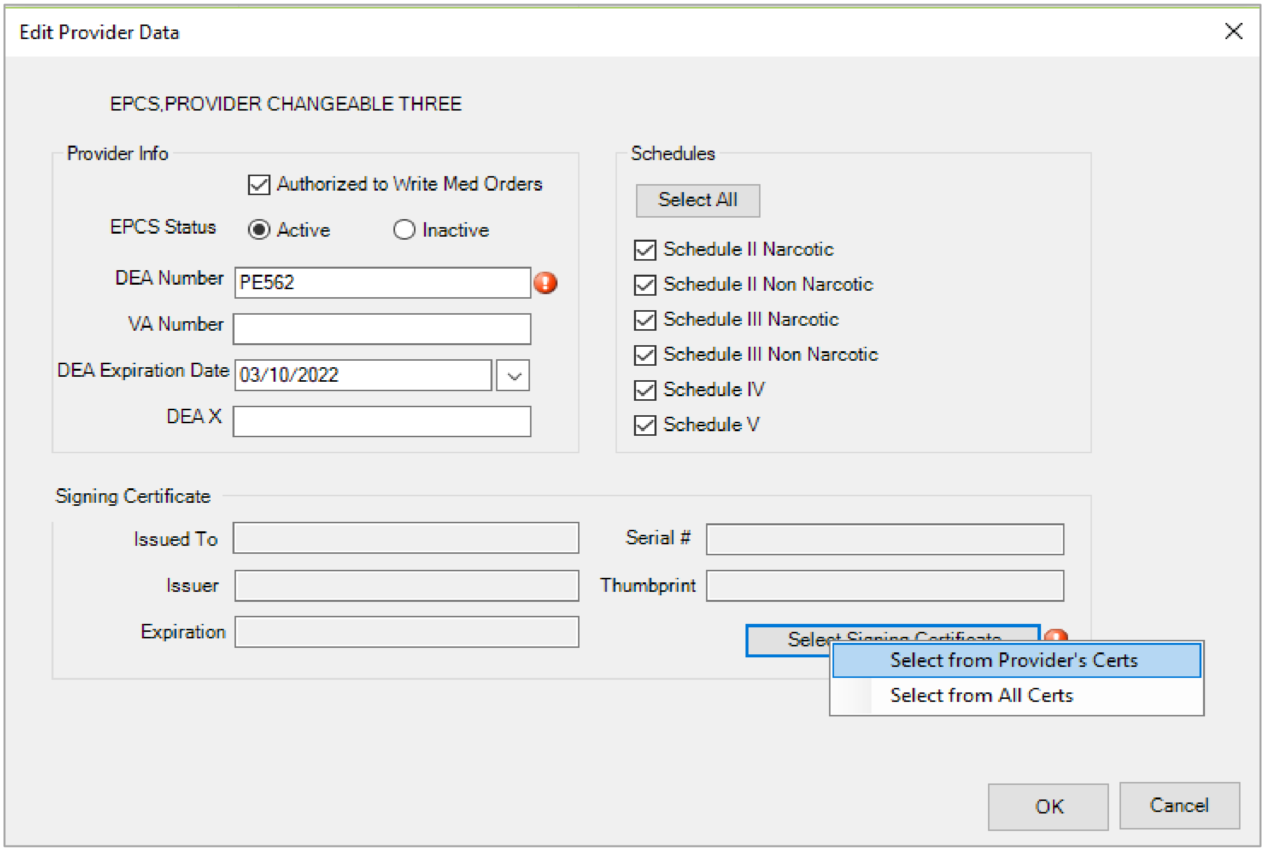
- **Authorized to Write Med Orders** check box: For a new user, this will be defaulted to a checked state. The user will not be able to prescribe any medications, including controlled substances, if this is not checked.
- **EPCS Status**: On a new user this will be defaulted to **Active**. Select **Active** if the user is allowed to prescribe CS medications using EPCS. Select **Inactive** if the provider’s authority to use EPCS had been revoked or is otherwise no longer authorized.

- **DEA Number:** This field (or the VA number field) is required if the provider wishes to order CS medications. A valid DEA number consists of two letters, six numbers, and one check digit.
- **VA Number:** The VA number is a unique identifier used for prescribers who do not have a DEA number of their own, but who are authorized to prescribe controlled substances using the facility's DEA number. Though there is no formal requirement for format (other than that it must be between three and 10 characters), it is often made up of the prescriber's first and last initials plus the last four digits of their social security number (SSN). For example, Jane Doe with an SSN of 123-45-6789 would have a VA number of JD6789. During the controlled substance ordering process, it will be automatically added to the facility's DEA number to comply with associated regulations. Enter only the VA number here; do not add the facility DEA here. A provider will have either a DEA number or a VA number, but not both.
- **DEA Expiration Date:** If the provider is using a VA number and not a DEA number, leave this field blank. Enter the expiration date of the provider's DEA number. Enter the date either manually in the MM/DD/YYYY format or use the calendar control beside the date field. This field contains several validations. A DEA expiration date up to three years in the future is allowed, but expiration dates beyond 39 months will not be accepted. A DEA expiration date in the past will display a message to the user "You have selected a DEA Expiration Date in the past. Do you want to continue?" If the expiration date is left blank and the provider is not using a VA number, the provider will not be able to prescribe controlled substances using the EPCS functions.
- **DEA X:** This is the provider's Narcotic Addiction DEA Number (NADEAN) and is not a required field; enter if applicable or available. Valid DEA X numbers are essentially the same format as DEA Numbers, but begin with an "X."
- **Schedules:** Select the controlled substance schedules for which this provider has privileges or is licensed to order (check individual Scheduled classes that apply or click Select All). If no data has ever been entered into these fields (i.e., the provider is new, and the profile is being created for the first time), the system will assume that all fields are checked. However, adjusting the schedule data will affect which schedules the provider may order.

7. Link the provider's signing certificate. This portion does require physical access to the provider's token or PIV.

    - Insert the provider's token or PIV into the computer being used to credential the user.

- Click **Select Signing Certificate** and then choose **Select from Provider's Certs** (preferred) or **Select from All Certs**. All Certs should only be used if the Provider's Certs option does not find the proper certificate. This may happen if the name on the certificate is not an exact match for the name in the RPMS database (See Section 2.2, item 6 for examples).


Edit Provider Data

EPCS,PROVIDER CHANGEABLE THREE

Provider Info

☑ Authorized to Write Med Orders

EPCS Status ● Active ○ Inactive

DEA Number PE562

VA Number

DEA Expiration Date 03/10/2022

DEA X

Schedules

☑ Schedule II Narcotic

☑ Schedule II Non Narcotic

☑ Schedule III Narcotic

☑ Schedule III Non Narcotic

☑ Schedule IV

☑ Schedule V

Signing Certificate

Issued To

Issuer

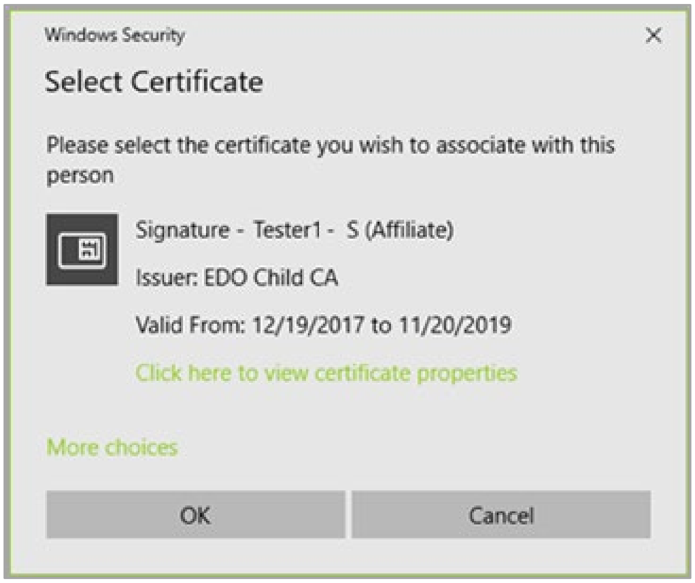
Expiration

Serial #

Thumbprint

Figure 2-12: Select Signing Certificate options

8. Select the appropriate certificate, then click **OK**. The window may look different in different versions of the Windows operating system.



Windows Security

Select Certificate

Please select the certificate you wish to associate with this person

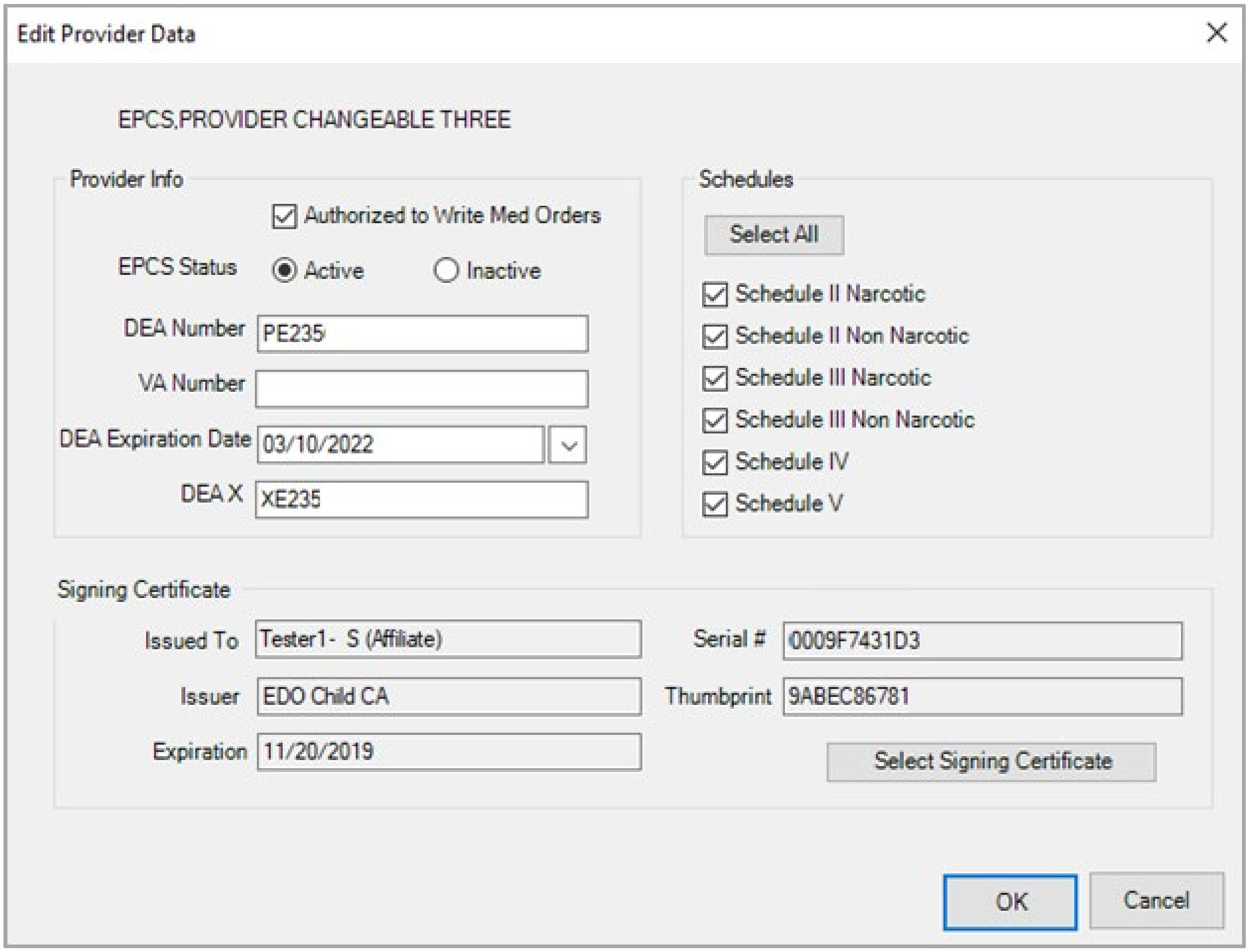
Signature - Tester1 - S (Affiliate)

Issuer: EDO Child CA

Valid From: 12/19/2017 to 11/20/2019

Figure 2-13: Select Certificate

9. Ensure that the Signing Certificate fields are all filled in the Signing Certificate section. The information cannot be entered manually or edited, so if any information is missing, re-select the signing certificate. You will not be able to select a signing certificate that is expired. See Figure 2-14 for an example of a completed profile.



Edit Provider Data

EPCS,PROVIDER CHANGEABLE THREE

Provider Info

☑ Authorized to Write Med Orders

EPCS Status ● Active ○ Inactive

DEA Number: PE235

VA Number:

DEA Expiration Date: 03/10/2022

DEA X: XE235

Schedules

☑ Schedule II Narcotic

☑ Schedule II Non Narcotic

☑ Schedule III Narcotic

☑ Schedule III Non Narcotic

☑ Schedule IV

☑ Schedule V

Signing Certificate

Issued To: Tester1- S (Affiliate)

Issuer: EDO Child CA

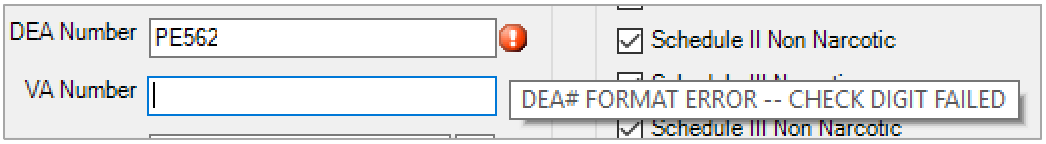
Expiration: 11/20/2019

Serial #: 0009F7431D3

Thumbprint: 9ABEC86781

Figure 2-14: Edit Provider Data window (partially masked for privacy)

10. As the data is entered and the user tabs to the next field, any incorrect formatting or values of data entered will produce a tool tip error or warning. Hover the mouse pointer over the red stop sign with exclamation mark to see the error, then correct the data if possible. The profile may not be saved when incorrect data is present. If the user is using a mouse to navigate fields and then clicks **OK** on the **Edit Provider Data** window, these error warnings will also display.



DEA Number: PE562

VA Number:

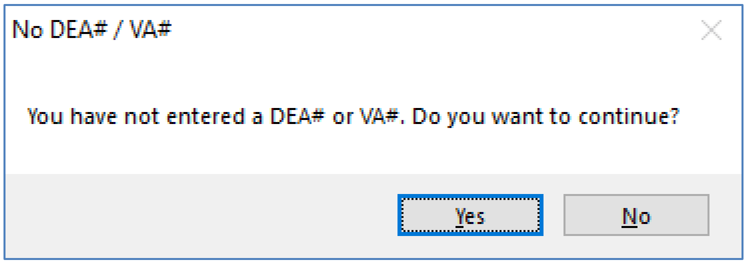
☑ Schedule II Non Narcotic

DEA# FORMAT ERROR -- CHECK DIGIT FAILED

☑ Schedule III Non Narcotic

Figure 2-15: Field with error

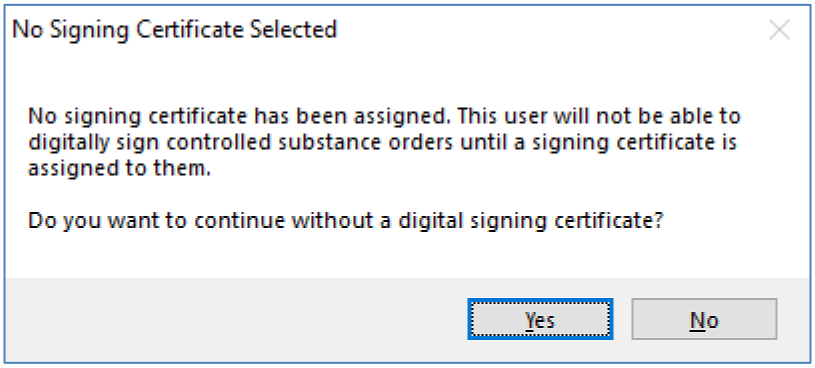
11. Click **OK**. When the user clicks **OK**, the system will check that the fields are filled appropriately; if the provider is missing a signing certificate or DEA or VA number, the user will see a warning but will be given the option to continue, as shown in Figure 2-16 and Figure 2-17.



No DEA# / VA#

You have not entered a DEA# or VA#. Do you want to continue?

Figure 2-16: No DEA#/VA# dialog



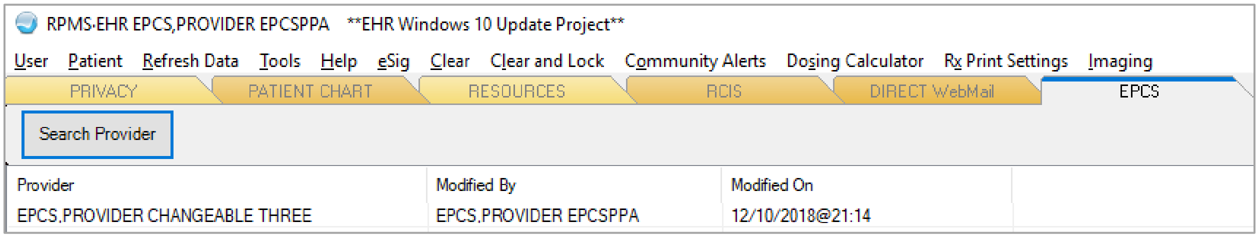
No Signing Certificate Selected

No signing certificate has been assigned. This user will not be able to digitally sign controlled substance orders until a signing certificate is assigned to them.

Do you want to continue without a digital signing certificate?

Figure 2-17: No Signing Certificate Selected dialog

12. The **Edit Provider Data** window closes, and the provider's name displays under the **Provider** list. The profile must still be verified before the provider may use EPCS. The profile changes may also be deleted or further edited as needed.



RPMS-EHR EPCS,PROVIDER EPCSPPA **EHR Windows 10 Update Project**

Provider	Modified By	Modified On
EPCS,PROVIDER CHANGEABLE THREE	EPCS,PROVIDER EPCSPPA	12/10/2018@21:14

Figure 2-18: Profile update list

2.4 Verify a Provider Profile

After the provider's profile information is entered or modified, the provider's name displays on the **Provider List** of the EPCS Credentialing component as shown in Figure 2-19.

The verify action must be performed by a different individual from the user who made the provider profile modifications, and the software will enforce this restriction, even if the user who created the profile also has the key to verify. Verification requires an individual with specific privileges to approve the request, including a digital signing certificate and token, PIV card, or other means for digitally signing to approve provider profile requests. The provider profile changes may only be altered by the person who initiated the changes, so any corrections that are needed must be sent back to that individual. In the event that individual is no longer available, the pending changes may be deleted by another user with the XUEPCSEDIT security key, and the profile changes may be recreated with the necessary adjustments.

To verify the provider's profile request:

1. Double-click a provider's name on the **Provider** list. If the provider does not display in the list and is known to have been created, click the **Refresh Data** menu option, or right-click anywhere in the list and select **Refresh** from the context menu, as seen in Figure 2-19.

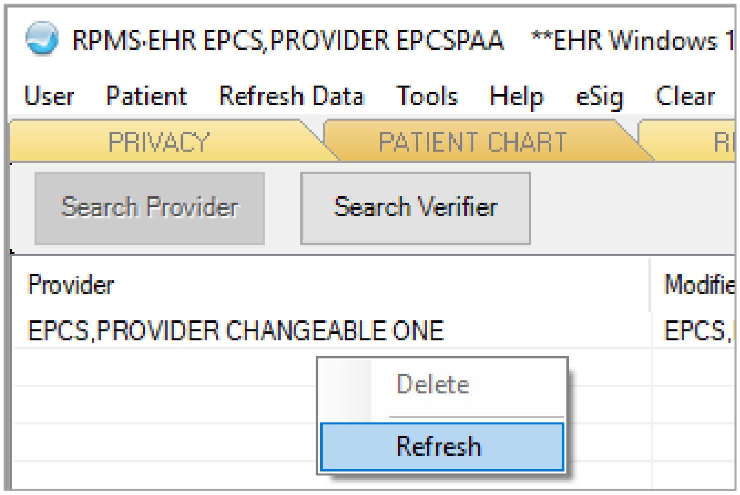
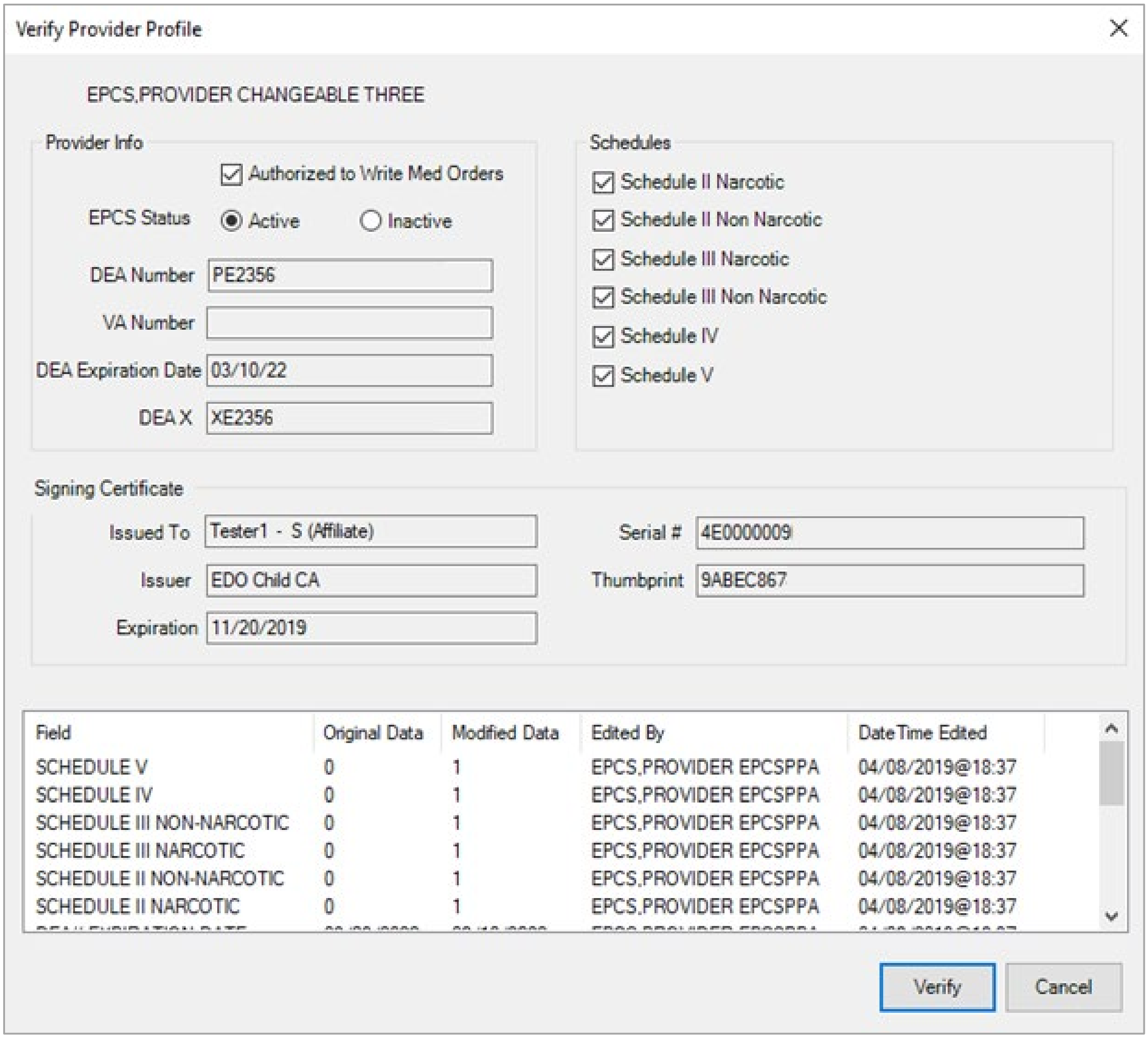


Figure 2-19: Refresh context menu option

2. The **Verify Provider Profile** window displays. If the user is the same one who created the profile changes, the profile will open in edit mode instead of verify mode and the user will not be able to verify the profile. Otherwise, review all information for accuracy. Modified data will display in the bottom of this screen in a panel including the name of the person who modified the data, the field within the profile that was changed, and the date and time the modifications were made.

Note: If any information is inaccurate, do not proceed with verification. Notify the person responsible for making the edits and request them to correct any mistaken information. If all the information is correct, proceed.



Verify Provider Profile

EPCS,PROVIDER CHANGEABLE THREE

Provider Info

☑ Authorized to Write Med Orders

EPCS Status ● Active ○ Inactive

DEA Number: PE2356

VA Number:

DEA Expiration Date: 03/10/22

DEA X: XE2356

Schedules

☑ Schedule II Narcotic

☑ Schedule II Non Narcotic

☑ Schedule III Narcotic

☑ Schedule III Non Narcotic

☑ Schedule IV

☑ Schedule V

Signing Certificate

Issued To: Tester1 - S (Affiliate)

Issuer: EDO Child CA

Expiration: 11/20/2019

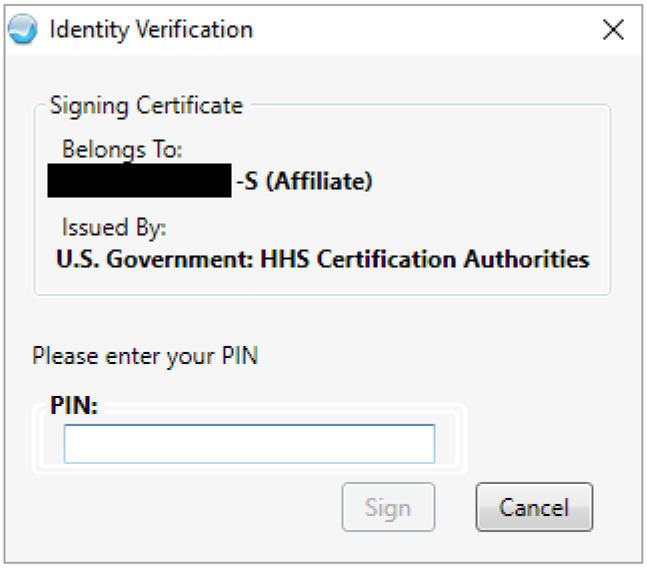
Serial #: 4E0000009

Thumbprint: 9ABEC867

Field	Original Data	Modified Data	Edited By	Date Time Edited
SCHEDULE V	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37
SCHEDULE IV	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37
SCHEDULE III NON-NARCOTIC	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37
SCHEDULE III NARCOTIC	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37
SCHEDULE II NON-NARCOTIC	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37
SCHEDULE II NARCOTIC	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37

Figure 2-20: Field, Original Data, Modified Data, Edited By, and Date Time Edited (some data masked for privacy)

3. Insert the verifier’s token or PIV into the computer then click **Verify** at the bottom right of the **Verify Provider Profile** window. An **Identity Verification** dialog displays with the logged-in user’s signing certificate information and a field to enter the **PIN** for the verifier’s cryptographic token or PIV. See the *bepc010o_EPCS_Token_Provisioning_Guide* for detailed information on using and setting up a cryptographic token.



Identity Verification

Signing Certificate

Belongs To:
[redacted]-S (Affiliate)

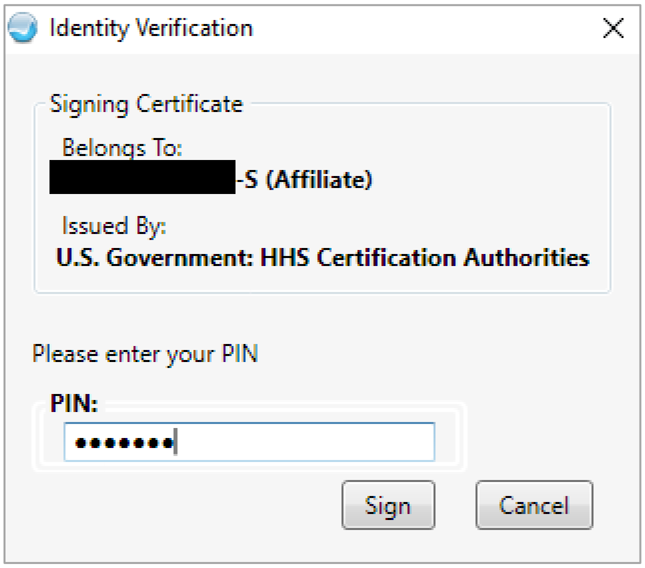
Issued By:
U.S. Government: HHS Certification Authorities

Please enter your PIN

PIN:

Figure 2-21: Identity Verification window (partially masked for privacy)

4. Enter the **PIN** for the EPCS token or PIV and click **Sign**.



Identity Verification

Signing Certificate

Belongs To:
[redacted]-S (Affiliate)

Issued By:
U.S. Government: HHS Certification Authorities

Please enter your PIN

PIN: •••••••

Figure 2-22: Authenticate with the token or PIV PIN (partially masked for privacy)

5. The provider is successfully verified.

Note: No message displays after clicking the **Verify** button; the **Authenticate** window closes, as does the **Verify Provider Profile** window. The provider’s name is removed from list.

2.5 Edit a Provider Profile

A provider profile may be edited before or after it is verified; however, any changes made will also require verification. If a profile with existing unverified changes must be further edited prior to verification, only the user who created the current changes may edit the profile. If the user who originally created the profile changes is not available and further alterations must be made to the profile, the pending profile changes may be deleted, and new profile changes may be created by an authorized user.

To edit pending profile changes, double-click on the provider's name in the **EPCS Credentialing** component list. If the profile does not open, the user is not authorized to edit the profile. Adjust the fields as outlined in Section 2.3. If pending changes exist from a different PPA user there will be a warning that Edit is disabled. When the warning is dismissed, the profile will open, but the second PPA user will be unable to save any changes to the profile.

To edit an existing verified profile, click the **Search Provider** button and follow the steps outlined in Section 2.3 to change content within the fields.

2.6 Delete Pending Provider Profile Changes

Pending profile changes may be deleted without being verified. A verified profile must be inactivated and cannot be deleted. Only a user authorized to create and edit a provider profile may delete pending profile changes.

To delete pending profile changes:

1. Find the provider's name in the list in the **EPCS Credentialing** component.
2. Right-click on the name and select **Delete** from the context menu, as shown in Figure 2-23.

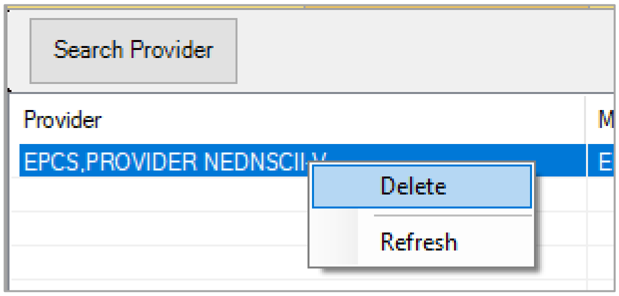
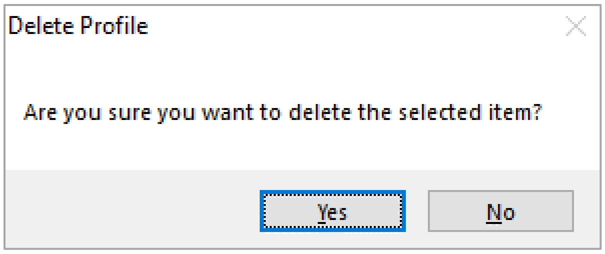


Figure 2-23: Delete a pending profile

3. Confirm the deletion by clicking **OK** in the **Delete Profile** dialog, as shown in Figure 2-24:


Delete Profile

Are you sure you want to delete the selected item?

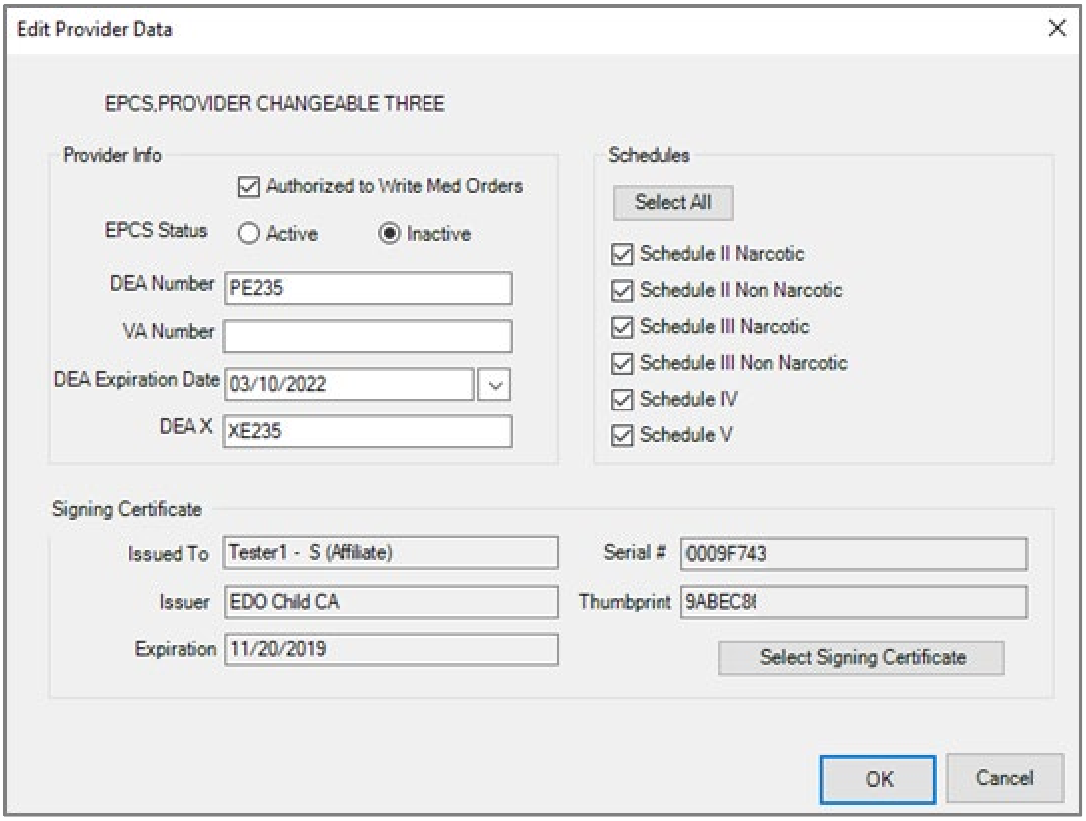
Figure 2-24: Delete Profile Confirmation pop-up

2.7 Inactivate a Provider Profile

A provider’s access to EPCS may be inactivated for the following reasons:

- If a cryptographic token or PIV is lost, stolen, or compromised.
- If the provider’s individual DEA registration expires.
- If the provider’s DEA registration is terminated, revoked, or suspended.
- If for any other reason the provider is no longer authorized to use the EPCS application.

In the event that a provider’s access to EPCS has to be inactivated, the same steps are followed as noted in Section 2.3. Instead of selecting the EPCS status of **Active** on the provider’s profile screen, the PPA selects **Inactive** as shown in Figure 2-25. Best practice suggests that the user’s authorized schedules should also be removed if the provider is no longer allowed to order controlled substances at the site; however, if the provider is still able to write paper prescriptions (e.g., if inactivating due to a lost, stolen, or compromised token or PIV), leave the information as is and just inactivate the profile.



EPCS,PROVIDER CHANGEABLE THREE

Provider Info

☑ Authorized to Write Med Orders

EPCS Status ○ Active ● Inactive

DEA Number PE235

VA Number

DEA Expiration Date 03/10/2022

DEA X XE235

Schedules

☑ Schedule II Narcotic
☑ Schedule II Non Narcotic
☑ Schedule III Narcotic
☑ Schedule III Non Narcotic
☑ Schedule IV
☑ Schedule V

Signing Certificate

Issued To Tester1 - S (Affiliate)

Issuer EDO Child CA

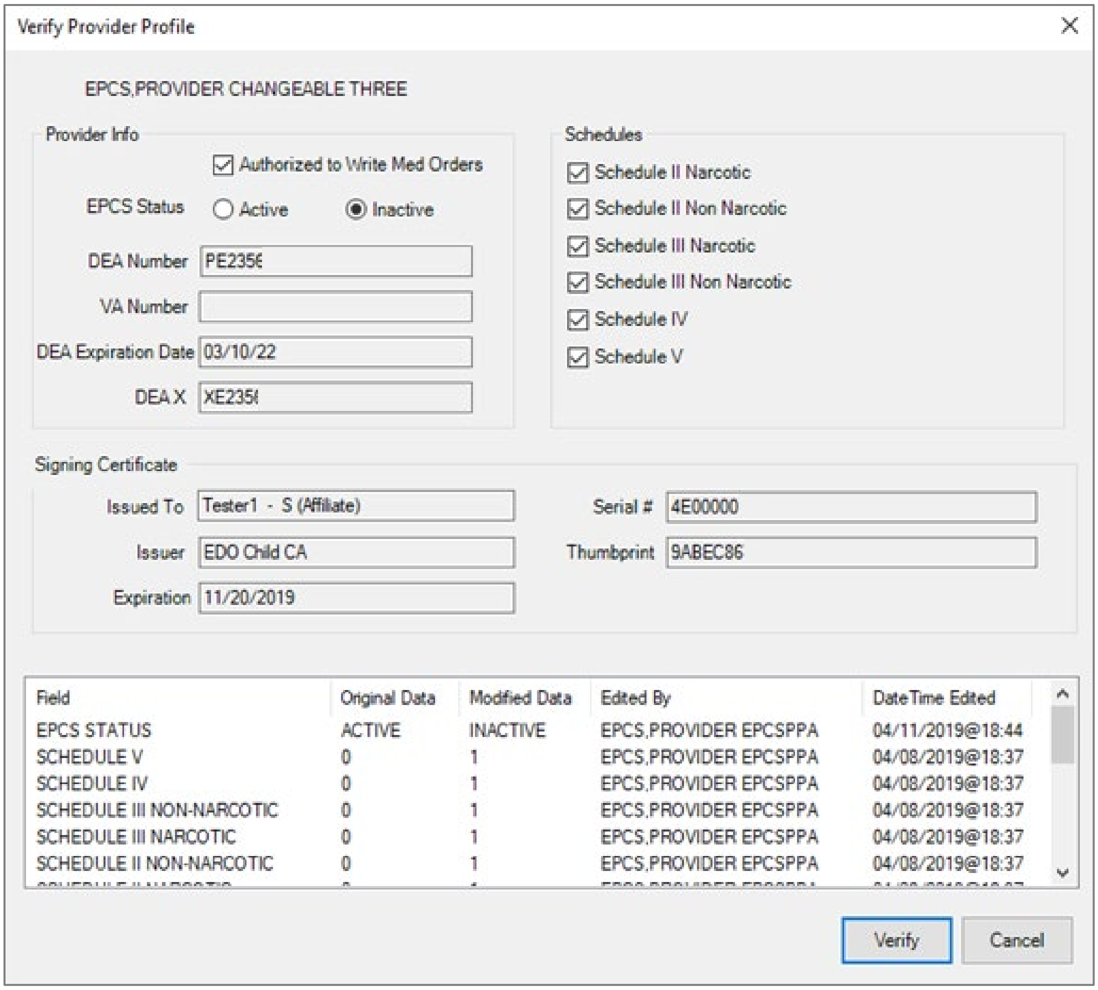
Expiration 11/20/2019

Serial # 0009F743

Thumbprint 9ABEC8

Figure 2-25: EPCS Status set as Inactive on Edit Provider Data (partially masked for privacy)

Once the provider's EPCS privileges are submitted to be inactivated, the **Verify Provider Profile** screen reflects this action in the **Logical Access Control** section, as shown in Figure 2-26.



Verify Provider Profile

EPCS,PROVIDER CHANGEABLE THREE

Provider Info

☑ Authorized to Write Med Orders

EPCS Status ○ Active ● Inactive

DEA Number	PE2356
VA Number	
DEA Expiration Date	03/10/22
DEA X	XE2356

Schedules

☑ Schedule II Narcotic
☑ Schedule II Non Narcotic
☑ Schedule III Narcotic
☑ Schedule III Non Narcotic
☑ Schedule IV
☑ Schedule V

Signing Certificate

Issued To	Tester1 - S (Affiliate)	Serial #	4E00000
Issuer	EDO Child CA	Thumbprint	9ABEC86
Expiration	11/20/2019		

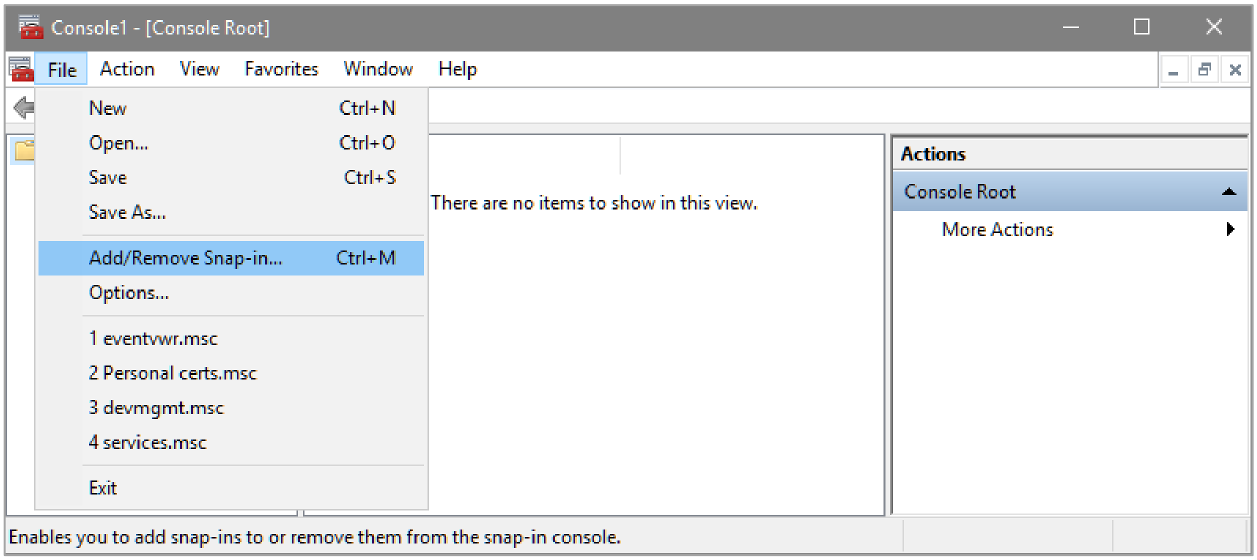
Field	Original Data	Modified Data	Edited By	DateTime Edited
EPCS STATUS	ACTIVE	INACTIVE	EPCS,PROVIDER EPCSPPA	04/11/2019@18:44
SCHEDULE V	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37
SCHEDULE IV	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37
SCHEDULE III NON-NARCOTIC	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37
SCHEDULE III NARCOTIC	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37
SCHEDULE II NON-NARCOTIC	0	1	EPCS,PROVIDER EPCSPPA	04/08/2019@18:37

Figure 2-26: Verify Provider Profile – Inactive

2.8 Clear the Certificate Cache

The PPA users may notice that the certificate list on their computer grows very large, as each certificate from each token and PIV inserted is cached. A user with Administrator permissions on the windows machine may clear the cache. To clear the cache:

1. Go to **Start** and **Run**.
2. Type **mmc** and press Enter. The **Console1 [Console Root]** window opens.
3. Select **File**, then **Add/Remove Snap-in**.

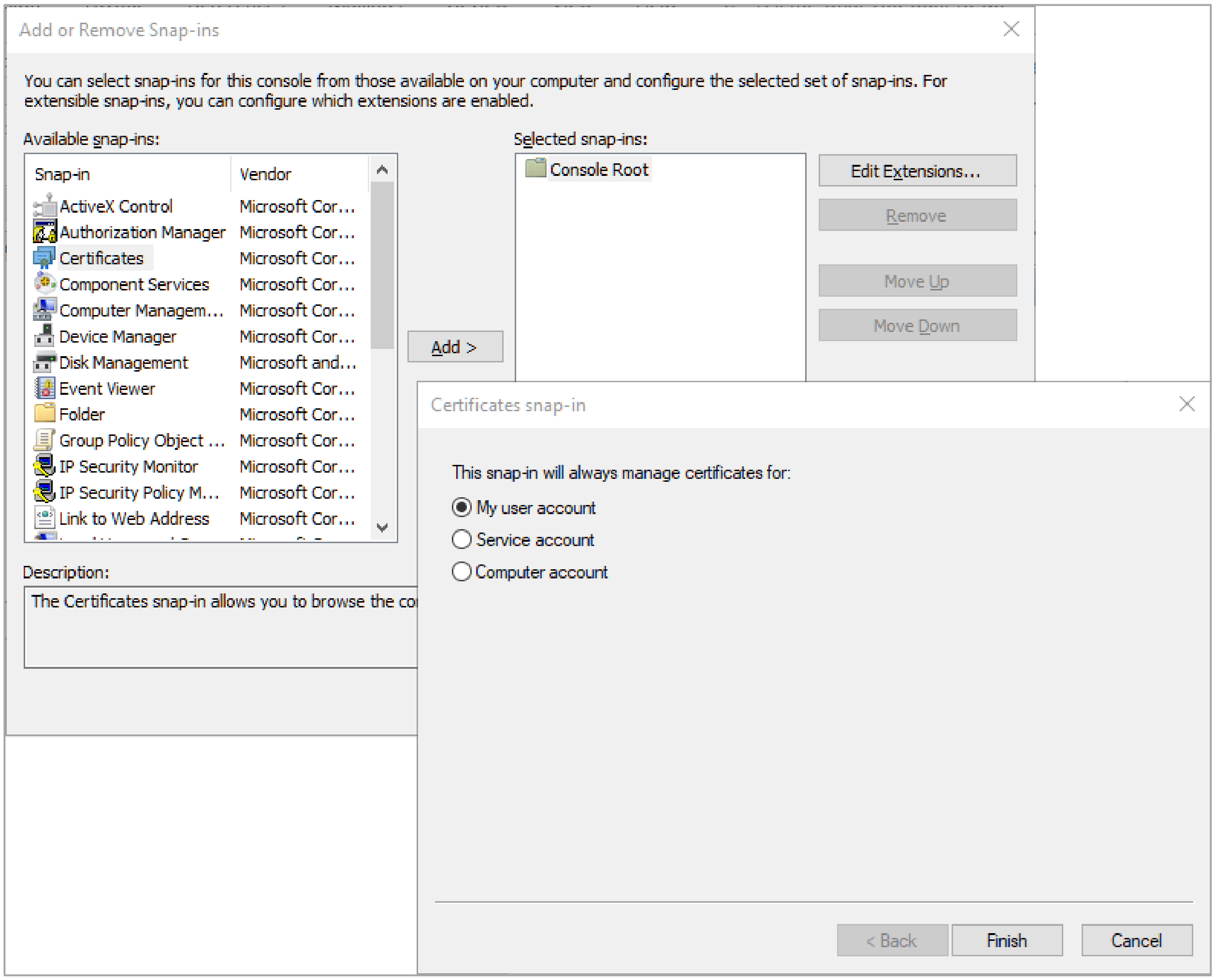


There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

Figure 2-27: Console 1 – Add/Remove Snap-in

4. Add the **Certificates Snap-in**. It will ask which certificate store you should use; select **My user account**.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the co

Certificates snap-in

This snap-in will always manage certificates for:

● My user account

○ Service account

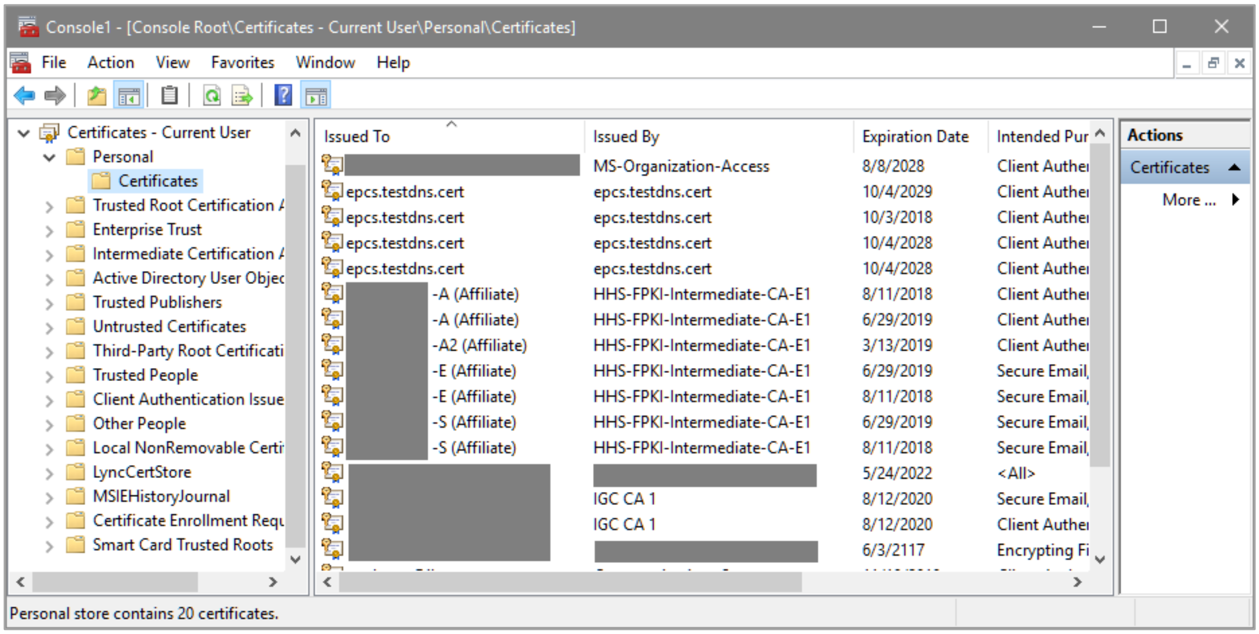
○ Computer account

Figure 2-28: Certificate snap-in, selecting My user account

5. Click **Finish**, then **OK** to close the **Add or Remove Snap-ins** dialog.

6. To see a list of all the certificates imported into the Personal certificate store, open **Certificates – Current User**, then **Personal**, then select **Certificates**.

Note: Some information in Figure 2-29 is masked for privacy.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification A
Enterprise Trust
Intermediate Certification A
Active Directory User Objec
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificati
Trusted People
Client Authentication Issue
Other People
Local NonRemovable Certi
LyncCertStore
MSIEHistoryJournal
Certificate Enrollment Requ
Smart Card Trusted Roots
Actions
Certificates
More ...

Issued To	Issued By	Expiration Date	Intended Pur
[redacted]	MS-Organization-Access	8/8/2028	Client Authei
epcs.testdns.cert	epcs.testdns.cert	10/4/2029	Client Authei
epcs.testdns.cert	epcs.testdns.cert	10/3/2018	Client Authei
epcs.testdns.cert	epcs.testdns.cert	10/4/2028	Client Authei
epcs.testdns.cert	epcs.testdns.cert	10/4/2028	Client Authei
[redacted]-A (Affiliate)	HHS-FPKI-Intermediate-CA-E1	8/11/2018	Client Authei
[redacted]-A (Affiliate)	HHS-FPKI-Intermediate-CA-E1	6/29/2019	Client Authei
[redacted]-A2 (Affiliate)	HHS-FPKI-Intermediate-CA-E1	3/13/2019	Client Authei
[redacted]-E (Affiliate)	HHS-FPKI-Intermediate-CA-E1	6/29/2019	Secure Email,
[redacted]-E (Affiliate)	HHS-FPKI-Intermediate-CA-E1	8/11/2018	Secure Email,
[redacted]-S (Affiliate)	HHS-FPKI-Intermediate-CA-E1	6/29/2019	Secure Email,
[redacted]-S (Affiliate)	HHS-FPKI-Intermediate-CA-E1	8/11/2018	Secure Email,
[redacted]	[redacted]	5/24/2022	<All>
[redacted]	IGC CA 1	8/12/2020	Secure Email,
[redacted]	IGC CA 1	8/12/2020	Client Authei
[redacted]	[redacted]	6/3/2117	Encrypting Fi

Personal store contains 20 certificates.

Figure 2-29: Console1 dialog displaying the personal store of certificates

7. To remove entries that are no longer needed, right-click on the certificate you wish to remove and select **Delete**. This will remove the certificate from the store but will not affect the use of the certificate if the token or PIV is inserted into the computer in the future.

Note:	If the token or PIV is inserted into the computer again while this user is logged in, the certificate will be added to the store again.

2.9 Unlocking a Token or PIV

A token or PIV may become locked if the PIN is entered incorrectly too many times. To unlock a PIV, the user must contact the IHS help desk and follow the instructions given. To unlock a token, the user will need to know the unlock code that was created when the certificate was installed. If the user does not remember the unlock code, please see the *bepc010o_EPCS_Token_Provisioning_Guide* for instructions on receiving a new unlock code.

Once the user has a valid unlock code:

1. Launch the **ActivClient User Console**.

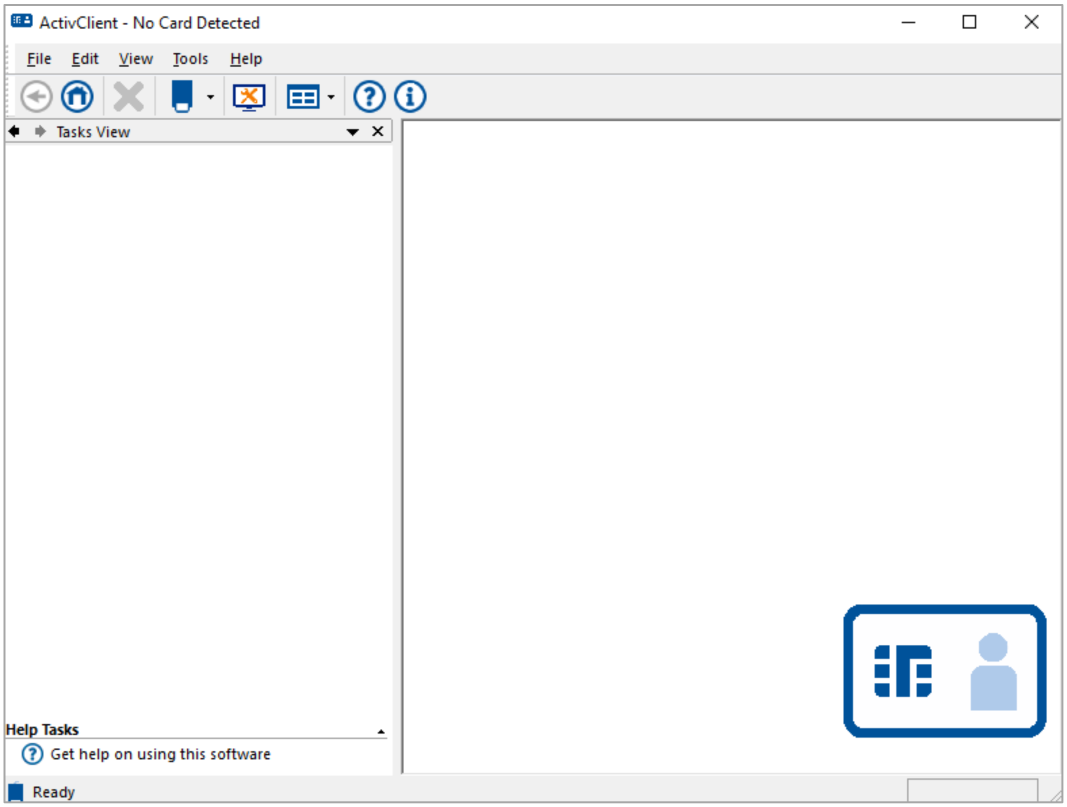
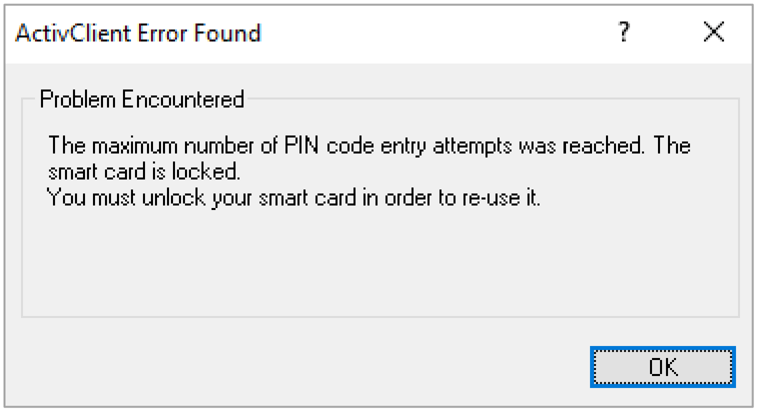

ActivClient - No Card Detected
File
Edit
View
Tools
Help
Tasks View
Help Tasks
Get help on using this software
Ready

Figure 2-30: ActivClient user console application

2. Insert the locked token. The following messages will display. Note that the tokens are seen by the Windows operating system as a smart card and are labeled as such in the error message.

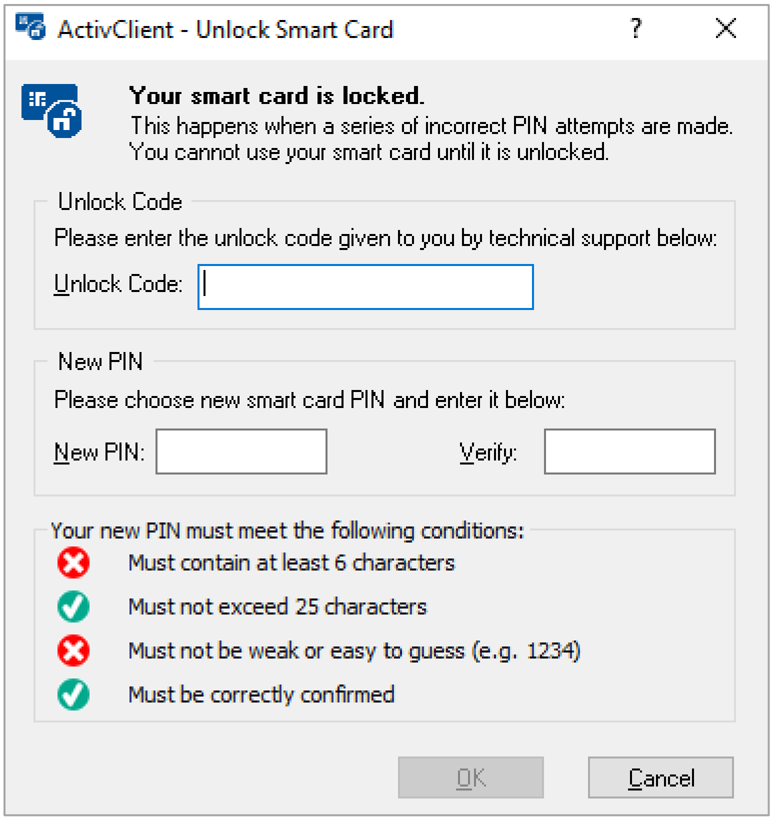


ActivClient Error Found

Problem Encountered

The maximum number of PIN code entry attempts was reached. The smart card is locked.
You must unlock your smart card in order to re-use it.

Figure 2-31: ActiveClient – Problem Encountered


ActivClient - Unlock Smart Card

Your smart card is locked.
This happens when a series of incorrect PIN attempts are made.
You cannot use your smart card until it is unlocked.

Unlock Code
Please enter the unlock code given to you by technical support below:
Unlock Code:

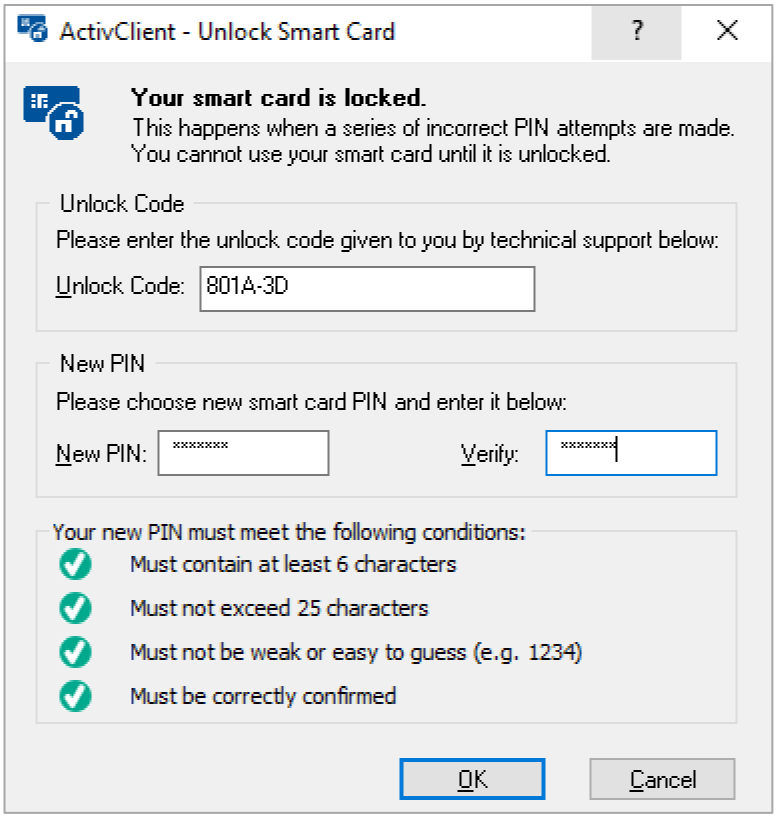
New PIN
Please choose new smart card PIN and enter it below:
New PIN: Verify:

Your new PIN must meet the following conditions:
- ✗ Must contain at least 6 characters
- ✓ Must not exceed 25 characters
- ✗ Must not be weak or easy to guess (e.g. 1234)
- ✓ Must be correctly confirmed

Figure 2-32: ActivClient – Unlock Smart Card dialog

3. Enter the **Unlock Code**.

4. Set a new PIN, making sure it meets the conditions displayed. The PIN may be reset to the old PIN if desired. If the PIN meets all the requirements, the conditions will all show green check mark notations.



ActivClient - Unlock Smart Card

Your smart card is locked.
This happens when a series of incorrect PIN attempts are made.
You cannot use your smart card until it is unlocked.

Unlock Code

Please enter the unlock code given to you by technical support below:

Unlock Code: 801A-3D

New PIN

Please choose new smart card PIN and enter it below:

New PIN: ******** Verify: ********

Your new PIN must meet the following conditions:

✓ Must contain at least 6 characters

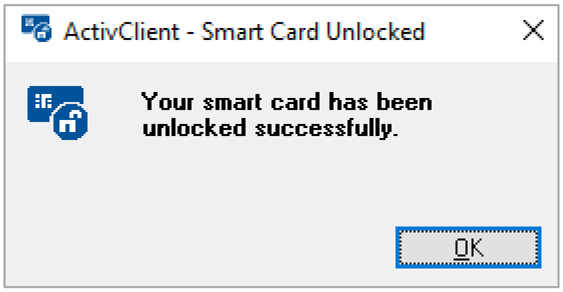
✓ Must not exceed 25 characters

✓ Must not be weak or easy to guess (e.g. 1234)

✓ Must be correctly confirmed

Figure 2-33: Unlock Smart Card with fields completed

5. Click **OK**. The following message should display:



ActivClient - Smart Card Unlocked

Your smart card has been unlocked successfully.

Figure 2-34: Smart Card Unlocked

6. Click **OK**. The token and certificate are now unlocked and may be used again as normal.

3.0 Ordering Controlled Substance Medications

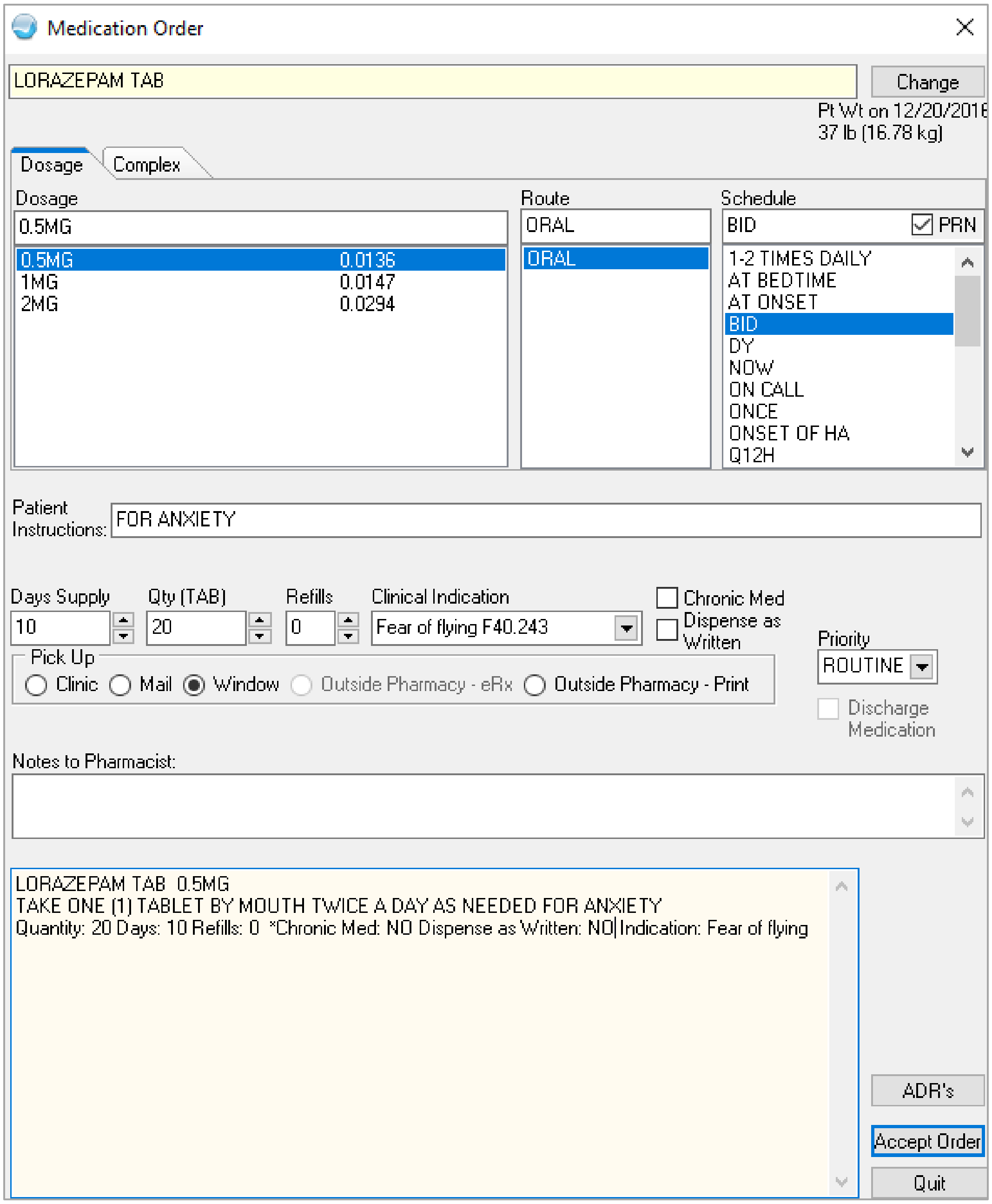
CS medications are ordered using the Medication Ordering process as reflected in the EHR User Manual under the Medication Management or the Orders components of RPMS-EHR. CS medications can be ordered using quick orders or the generic ordering dialogs. No changes need to be made to site's current order menus. The ordering process is essentially the same whether using EPCS functions or not, though the signing process will be different depending on the set up of the site, division, and provider and the pick-up method selected in the order.

3.1 Create an Outpatient Order

Create an outpatient order using the following steps. Some changes were made to the Medication Order dialog during the development of the EPCS functions, and these are noted.

> **Note:** The **Medications** menu may be customized and appear differently than depicted within this user manual.

1. Log in as a provider.
2. Proceed to the **Medication Management** (or **Orders**) component of the patient chart and select the CS medication to be prescribed for this patient as an outpatient.
3. The **Medication Order** window will display as in Figure 3-1. Complete the dialog as appropriate for the order. Note that the clinical indication may or may not be required depending on the medication chosen and the site settings. There is a change in the display of the pick-up options: in pre-EPCS systems, only the applicable options were displayed, while after EPCS is installed, all options will display. However, the options that are not available for the order and provider are inactive and dimmed.



LORAZEPAM TAB

Pt Wt on 12/20/2016
37 lb (16.78 kg)

Dosage: 0.5MG

0.5MG	0.0136
1MG	0.0147
2MG	0.0294

Route: ORAL

ORAL

Schedule: BID ☑ PRN

1-2 TIMES DAILY
AT BEDTIME
AT ONSET
BID
DY
NOW
ON CALL
ONCE
ONSET OF HA
Q12H

Patient Instructions: FOR ANXIETY

Days Supply: 10 Qty (TAB): 20 Refills: 0 Clinical Indication: Fear of flying F40.243

□ Chronic Med
□ Dispense as Written

Pick Up: ○ Clinic ○ Mail ● Window ○ Outside Pharmacy - eRx ○ Outside Pharmacy - Print

Priority: ROUTINE

□ Discharge Medication

Notes to Pharmacist:

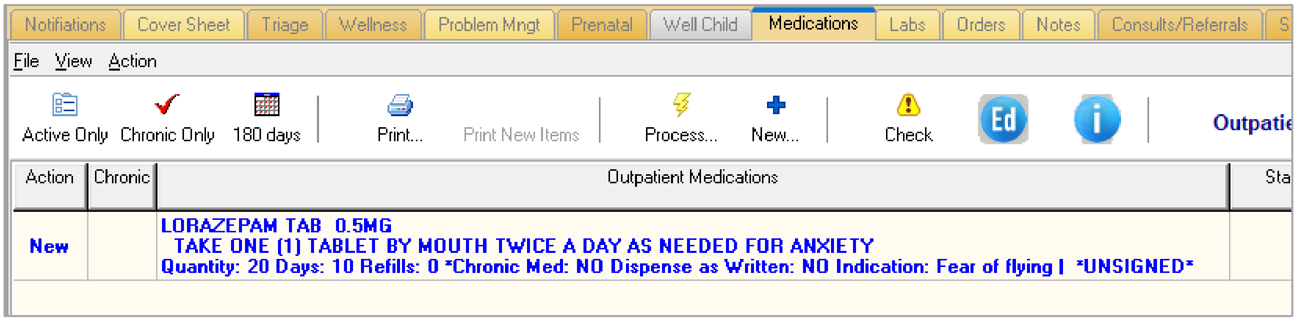
LORAZEPAM TAB 0.5MG
TAKE ONE (1) TABLET BY MOUTH TWICE A DAY AS NEEDED FOR ANXIETY
Quantity: 20 Days: 10 Refills: 0 *Chronic Med: NO Dispense as Written: NO Indication: Fear of flying

Figure 3-1: Medication Order dialog

4. If the order is for Outside Pharmacy - eRx using Surescripts, the user must select a pharmacy that can process EPCS orders. Not all Surescripts pharmacies are EPCS certified.

5. After completing all required fields, click **Accept Order**. If the **Accept Order** button is not active, scroll to view the entire order summary to activate the button. The **Order Checking** pop-up window may display.

6. After closing the **Order Checking** pop-up window, the newly ordered CS medication will display in the **Outpatient Medications** list as **New** and **Unsigned** as shown in Figure 3-2. It will display similarly in the Orders component.



New LORAZEPAM TAB 0.5MG
TAKE ONE (1) TABLET BY MOUTH TWICE A DAY AS NEEDED FOR ANXIETY
Quantity: 20 Days: 10 Refills: 0 *Chronic Med: NO Dispense as Written: NO Indication: Fear of flying | *UNSIGNED*

Figure 3-2: Outpatient Medications – new CS medication order

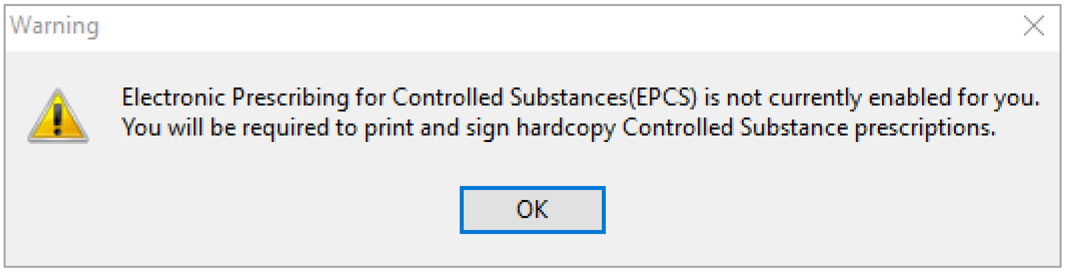
7. If a medication order is not electronically signed by the prescribing provider, the provider will receive a notification of the unsigned medication order. As soon as the order is signed by the provider, this notification is automatically deleted.

3.1.1 EPCS Controlled Substance Ordering Error Messages

There are several points where the EPCS system may provide warnings or errors during the ordering process.

3.1.1.1 EPCS Not Enabled for Division

If the EPCS system has not been enabled for the division the provider is logged into, the error message in Figure 3-3 will display as soon as a controlled substance is selected. Click **OK** to continue to the medication ordering dialog.



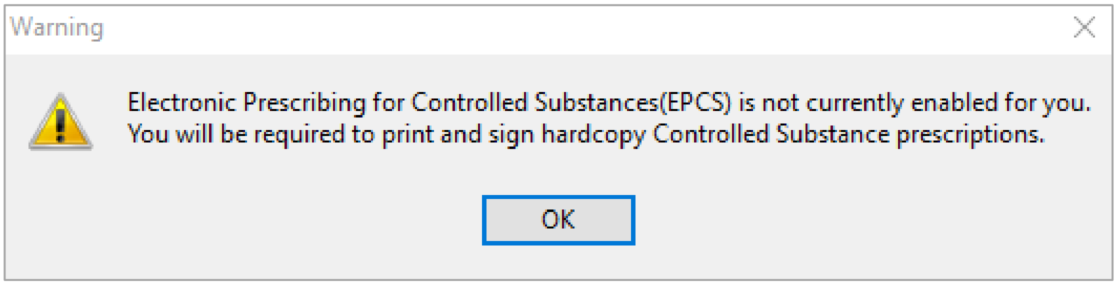
Electronic Prescribing for Controlled Substances(EPCS) is not currently enabled for you. You will be required to print and sign hardcopy Controlled Substance prescriptions.

Figure 3-3: Warning that EPCS is not enabled for Division or Site

Providers at divisions that are not enabled are required to print and sign the hard copy of the CS medication order, and no two-factor authentication will be required.

3.1.1.2 Provider Not Enabled

If the provider is not enabled for EPCS by having a profile created and verified, the message in Figure 3-4 will display as soon as the controlled substance is selected.



Electronic Prescribing for Controlled Substances(EPCS) is not currently enabled for you.
You will be required to print and sign hardcopy Controlled Substance prescriptions.

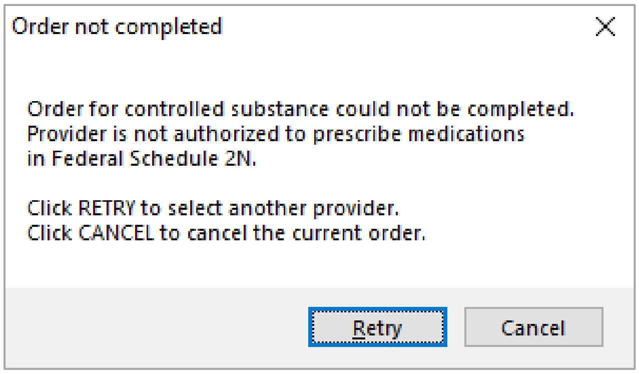
Figure 3-4: Provider Not Enabled message

A provider who is not enabled will not be able to transmit CS orders electronically to internal or external pharmacies and must print and sign the order in ink. Because the messages regarding a division not enabled and provider not enabled appear to be the same to the end user, the provider should discuss the error message with the personnel in charge of maintaining the RPMS database.

3.1.1.3 Provider DEA-Related Warnings

A provider may see warning messages regarding their DEA authorization. The warnings will display as soon as the drug is selected.

If a provider tries to enter a CS order of a schedule for which they are not authorized, they will receive a message similar to the one in Figure 3-5.

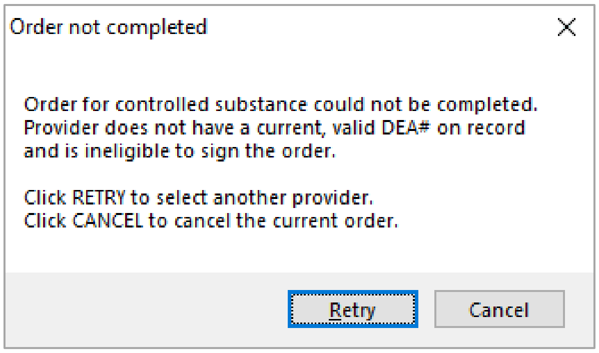


Order for controlled substance could not be completed.
Provider is not authorized to prescribe medications
in Federal Schedule 2N.

Click RETRY to select another provider.
Click CANCEL to cancel the current order.

Figure 3-5: Provider not authorized for schedule

If the provider has a missing DEA number or one that is invalid or expired, the message in Figure 3-6 will display.


Order not completed

Order for controlled substance could not be completed.
Provider does not have a current, valid DEA# on record
and is ineligible to sign the order.

Click RETRY to select another provider.
Click CANCEL to cancel the current order.

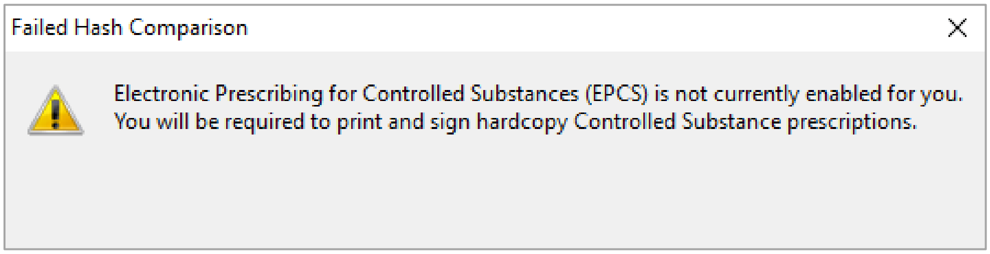
Figure 3-6: Provider does not have current valid DEA number

For either of these errors, the user may do any one of the following:

- Select a different provider to sign the order by clicking **Retry** and selecting a new ordering provider.
- Cancel the order by clicking **Cancel**.
- Select a different medication by canceling and starting a new order.

3.1.1.4 Failed Hash

The failed hash message displays when an EPCS provider's credentials have been changed without using the authorized credentialing component. The provider will need to report this message to the appropriate personnel in charge of maintaining the RPMS database and will need to print and sign hard copies of all controlled substance orders until it is rectified.

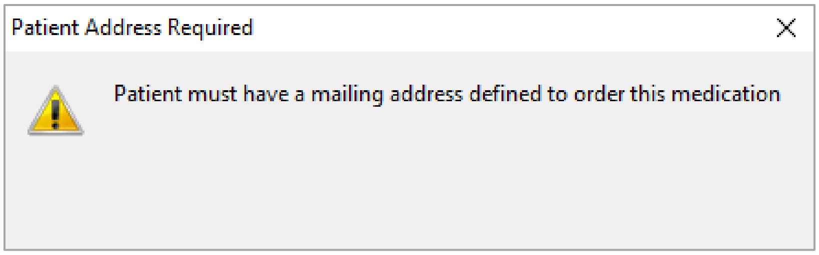

Failed Hash Comparison

Electronic Prescribing for Controlled Substances (EPCS) is not currently enabled for you.
You will be required to print and sign hardcopy Controlled Substance prescriptions.

Figure 3-7: Failed Hash Comparison pop-up

3.1.1.5 Missing Address

If the patient does not have a mailing address on file, the message in Figure 3-8 will display as soon as the controlled substance is selected. The EPCS regulations require that any patient receiving a CS prescription electronically must have a mailing address in the system. If this message displays, notify the registration office so that they can determine and enter the correct patient mailing address.

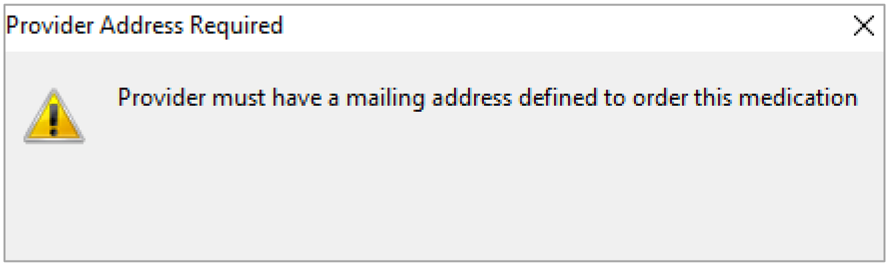


Patient Address Required

Patient must have a mailing address defined to order this medication

Figure 3-8: Patient Address Required pop-up

If the site does not have the address identified for the institution, the following error will occur when a controlled substance is selected:



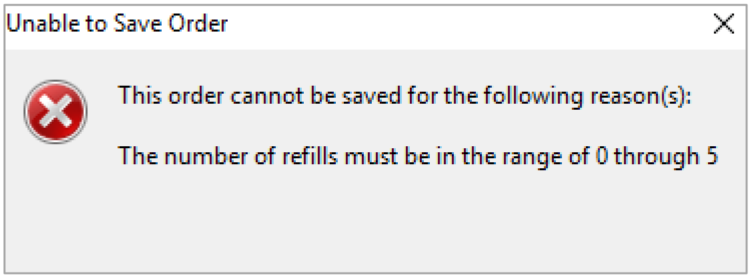
Provider Address Required

Provider must have a mailing address defined to order this medication

Figure 3-9: Provider Address Required pop-up

3.1.1.6 Refills Entered Exceed the Allowable Number of Refills

As was the behavior prior to the implementation of EPCS, orders for Schedule III, IV, and V CS medications cannot be refilled more than five times. If the provider attempts to order more than five refills, the application will not allow this order to be saved as shown in Figure 3-10.



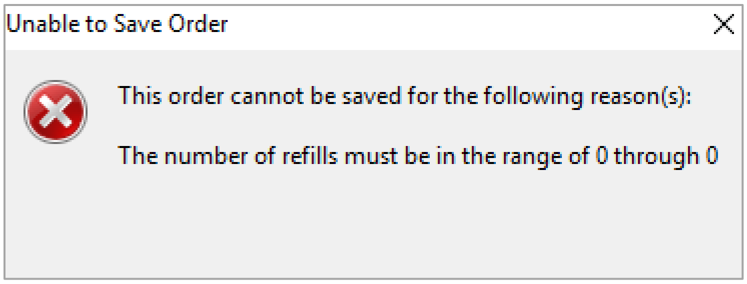
Unable to Save Order

This order cannot be saved for the following reason(s):

The number of refills must be in the range of 0 through 5

Figure 3-10: Allowable refill range pop-up

If a provider attempts to type in a refill for a CS II medication, they will receive an error message indicating that refills are not permitted for CS II medications as depicted in Figure 3-11.


Unable to Save Order

This order cannot be saved for the following reason(s):

The number of refills must be in the range of 0 through 0

Figure 3-11: No refills allowed for Schedule II medications

3.1.2 CS Order Restrictions

There are three parameters that control the maximum days' supply for the various schedules of CS orders, how long after a schedule C-II order is created before it may no longer be filled, and how long after being filled a C-II order will expire. These parameters will allow sites to comply with any applicable state laws regarding CS medication orders.

3.1.2.1 Max Days' Supply CS

The maximum number of days' supply parameter (BEHORX MAX DAYS SUPPLY CS) allows sites to specify the maximum allowed days' supply (up to 30 days) for CS medications. If sites elect not to configure this parameter, the days' supply parameter will default to 30 days. Prescribers will not be able to save an order for CS medications that exceed the days entered for this parameter.

3.1.2.2 Order Date Max

The maximum order date parameter (APSP CS II ORDER DATE MAX) sets the number of days after the ordered earliest fill date the order for a C-II medication may still be filled in the pharmacy package. Orders that have not been processed within the allowable time frame may not be processed by the internal pharmacy. This parameter has a maximum setting of 365 days. A blank value for this parameter will be interpreted as 0 days.

3.1.2.3 Prescription Expire Days

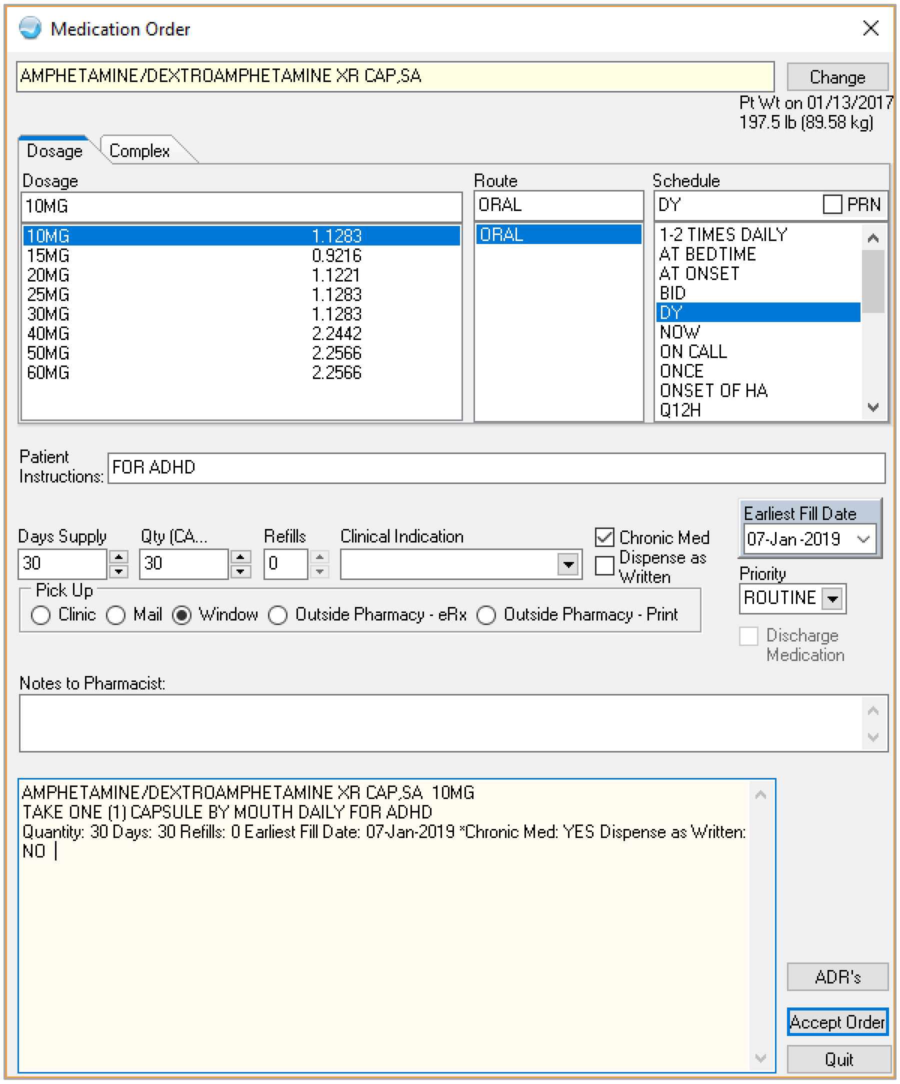
The Prescription Expire Days parameter (APSP CS II RX EXPIRE DAYS) sets the number of days after filling that a C-II prescription will expire. This parameter has a maximum setting of 365 days. A blank value for this parameter will be interpreted as 0 days.

3.1.3 Special Ordering Situations

There are several situations that users may encounter when ordering CS medications, including adding an earliest fill date and creating more than one order for the same medication in one session, using a scribe or proxy to create the order for the provider to sign later, ordering via the Clinical Information Reconciliation (CIR) tool, creating an order for an outpatient detox medication, or creating an order for gamma-hydroxybutyrate (GHB).

3.1.3.1 Earliest Fill Date for Schedule C II

The **Earliest Fill Date** field will display on the **Medication Order** dialog as shown in Figure 3-12 when the drug selected is in schedule C-II and the field is enabled. The earliest fill date will default to the current date. Adjust the date as required.



AMPHETAMINE/DEXTROAMPHETAMINE XR CAP,SA

Pt Wt on 01/13/2017
197.5 lb (89.58 kg)

Dosage: 10MG
Route: ORAL
Schedule: DY □ PRN

10MG	1.1283
15MG	0.9216
20MG	1.1221
25MG	1.1283
30MG	1.1283
40MG	2.2442
50MG	2.2566
60MG	2.2566

Patient Instructions: FOR ADHD

Days Supply: 30
Qty (CA...: 30
Refills: 0
Clinical Indication:
☑ Chronic Med
□ Dispense as Written
Earliest Fill Date: 07-Jan-2019
Priority: ROUTINE
□ Discharge Medication

Pick Up: ○ Clinic ○ Mail ● Window ○ Outside Pharmacy - eRx ○ Outside Pharmacy - Print

Notes to Pharmacist:

AMPHETAMINE/DEXTROAMPHETAMINE XR CAP,SA 10MG
TAKE ONE (1) CAPSULE BY MOUTH DAILY FOR ADHD
Quantity: 30 Days: 30 Refills: 0 Earliest Fill Date: 07-Jan-2019 *Chronic Med: YES Dispense as Written: NO |

Figure 3-12: Earliest Fill Date field enabled on C-II Orders

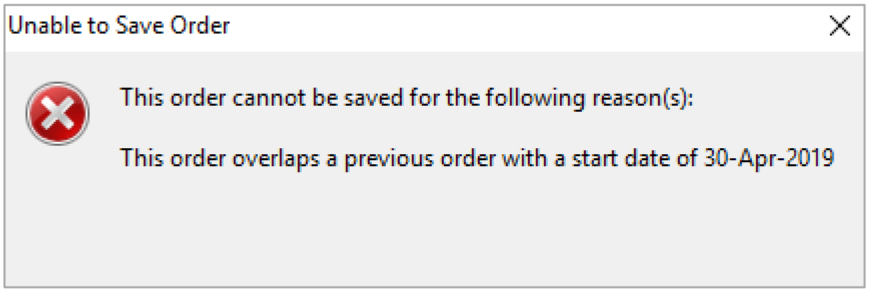
3.1.3.2 Multiple Orders for the Same Schedule C-II Drug in a Single Session

The medication ordering and pharmacy processing functions have been adjusted to allow a provider to enter up to three orders in a single session for the same medication (as determined by the dispense drug) in schedule C-II, provided each order is for no more than 30 days and all three together are for not more than 90 days, unless your site has different limits to accommodate State Law. Each order in the set must contain an earliest fill date. For the purposes of EPCS, a "single session" is defined to be the same calendar day. Note that inpatient orders and orders using the "clinic" pick-up location are excluded from these checks.

When creating more than one order for the same medication in a single session, the earliest fill date field will have a validation for the second and third orders. A provider will not be able to add an earliest fill date that overlaps with the previously chosen earliest fill date, based on the quantity and day's supply ordered.

For example, if the initial order is written with an earliest fill date of January 1, 2019, and the order is for 28 days, the next order must be at least 28 days after January 1, which is January 29, 2019. If that order is also for 28 days, the third and final order must be for 28 days after January 29, or February 26, 2019. Even if the orders are entered out of order, the system will check for overlapping dates.

If the chosen earliest fill date is not valid, an error message will display similar to the one shown in Figure 3-13.


Unable to Save Order

This order cannot be saved for the following reason(s):

This order overlaps a previous order with a start date of 30-Apr-2019

Figure 3-13: Earliest fill date error

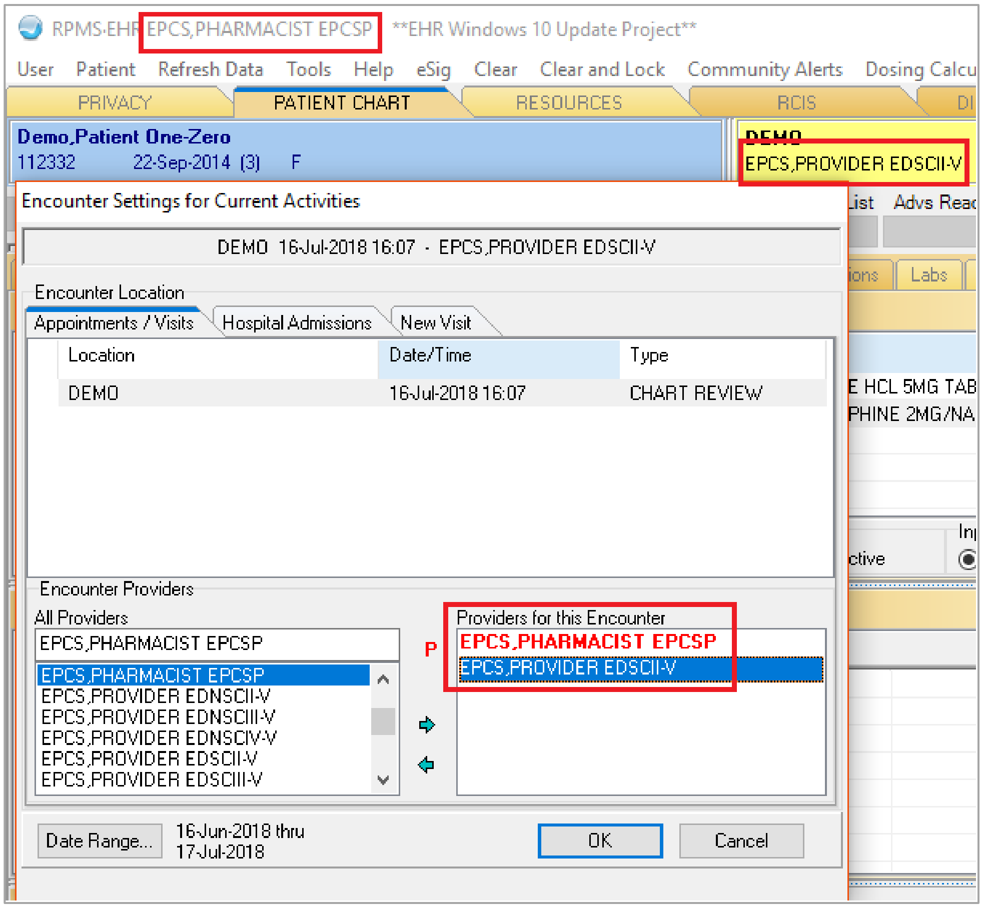
It is important to remember that the special handling of multiple orders for the same drug apply only to those orders completed in a single session. Orders for the same medication that are created and signed in multiple sessions will behave as they did prior to the EPCS changes, in that the processing of one order will cause any remaining pending orders to be discontinued.

3.1.3.3 Order Created by Scribe or Proxy

RPMS-EHR allows for an order to be input by another user on behalf of the provider such as with a verbal order given to an ancillary healthcare provider or if a prescriber uses a scribe to input data into the RPMS-EHR system. The EPCS functions do accommodate this practice. There are a few changes to the process when used with medications, especially CS medications. The person acting as scribe may or may not have ordering keys and may or may not have the AUTHORIZED TO WRITE MED ORDERS field in the NEW PERSON file set to Yes.

The ordering provider who will sign the order must be an encounter provider on the visit. The ordering provider should be highlighted in the **Encounter Settings for Current Activities** dialog, and will then display in the **Visit** box instead of the logged-in user as shown in Figure 3-14.

> **Note:** The ordering provider may or may not be the primary provider for the encounter.



EPCS,PHARMACIST EPCSP

Demo,Patient One-Zero
112332 22-Sep-2014 (3) F

DEMO
EPCS,PROVIDER EDSCII-V

Encounter Settings for Current Activities

DEMO 16-Jul-2018 16:07 - EPCS,PROVIDER EDSCII-V

Location	Date/Time	Type
DEMO	16-Jul-2018 16:07	CHART REVIEW

All Providers

EPCS,PHARMACIST EPCSP

EPCS,PHARMACIST EPCSP
EPCS,PROVIDER EDNSCII-V
EPCS,PROVIDER EDNSCIII-V
EPCS,PROVIDER EDNSCIV-V
EPCS,PROVIDER EDSCII-V
EPCS,PROVIDER EDSCIII-V

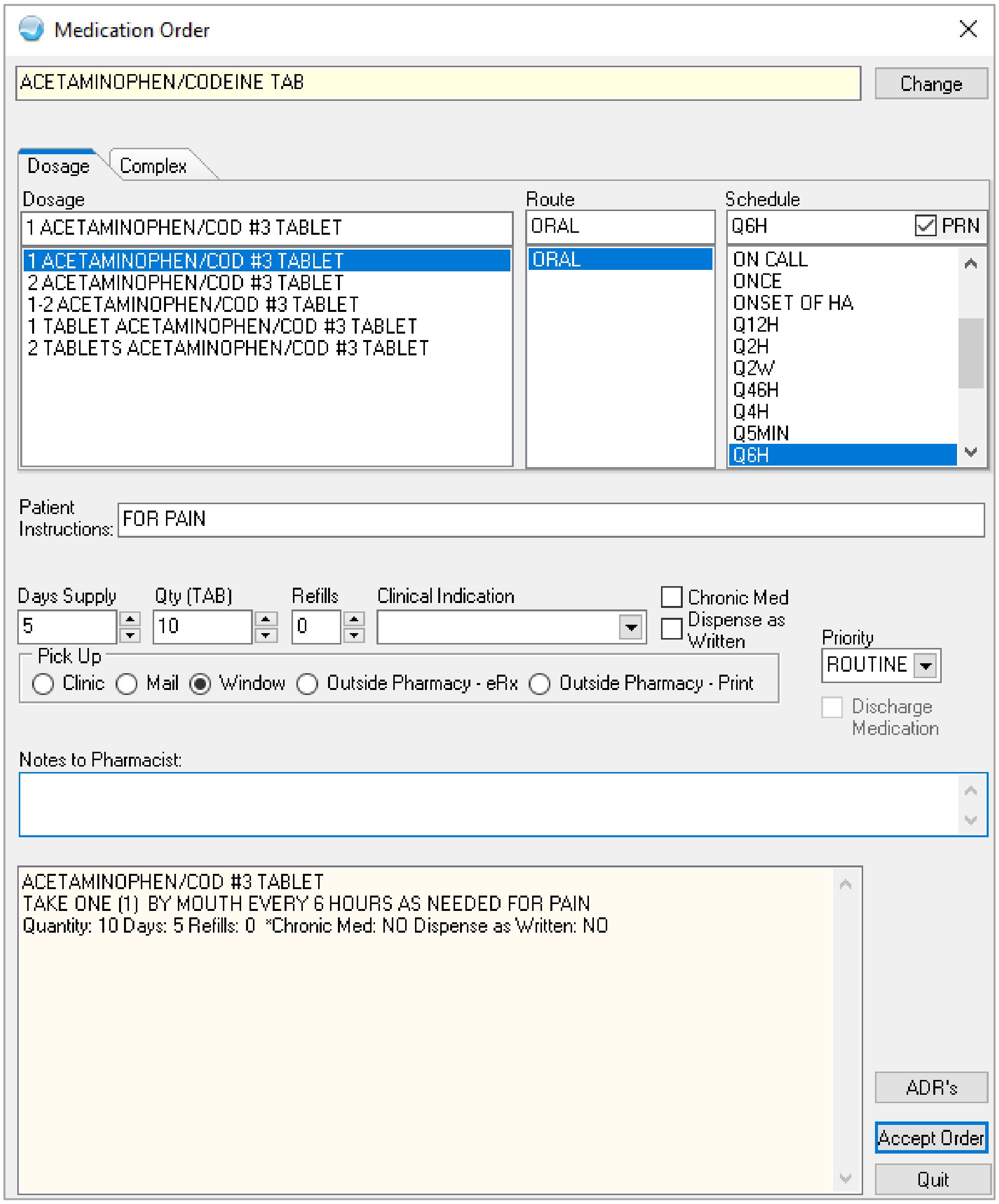
Providers for this Encounter

P EPCS,PHARMACIST EPCSP
EPCS,PROVIDER EDSCII-V

16-Jun-2018 thru
17-Jul-2018

Figure 3-14: RPMS-EHR showing logged-in user, Visit box with ordering provider, and Encounter Setting for Current Activities window with ordering provider

Create a new order as usual. The **Order** dialog for the controlled substance can display for the person entering the order even though they cannot order controlled substances independently. This is because the lookup checks the ordering provider rather than the logged-in user for their ability to order a class of controlled substances, their DEA number, if they are EPCS enabled, and if their hash is valid.



Medication Order

ACETAMINOPHEN/CODEINE TAB

Dosage: 1 ACETAMINOPHEN/COD #3 TABLET

- 1 ACETAMINOPHEN/COD #3 TABLET
- 2 ACETAMINOPHEN/COD #3 TABLET
- 1-2 ACETAMINOPHEN/COD #3 TABLET
- 1 TABLET ACETAMINOPHEN/COD #3 TABLET
- 2 TABLETS ACETAMINOPHEN/COD #3 TABLET

Route: ORAL

Schedule: Q6H ☑ PRN

- ON CALL
- ONCE
- ONSET OF HA
- Q12H
- Q2H
- Q2W
- Q46H
- Q4H
- Q5MIN
- Q6H

Patient Instructions: FOR PAIN

Days Supply: 5

Qty (TAB): 10

Refills: 0

Clinical Indication:

□ Chronic Med

□ Dispense as Written

Pick Up: ○ Clinic ○ Mail ● Window ○ Outside Pharmacy - eRx ○ Outside Pharmacy - Print

Priority: ROUTINE

□ Discharge Medication

Notes to Pharmacist:

ACETAMINOPHEN/COD #3 TABLET
TAKE ONE (1) BY MOUTH EVERY 6 HOURS AS NEEDED FOR PAIN
Quantity: 10 Days: 5 Refills: 0 *Chronic Med: NO Dispense as Written: NO

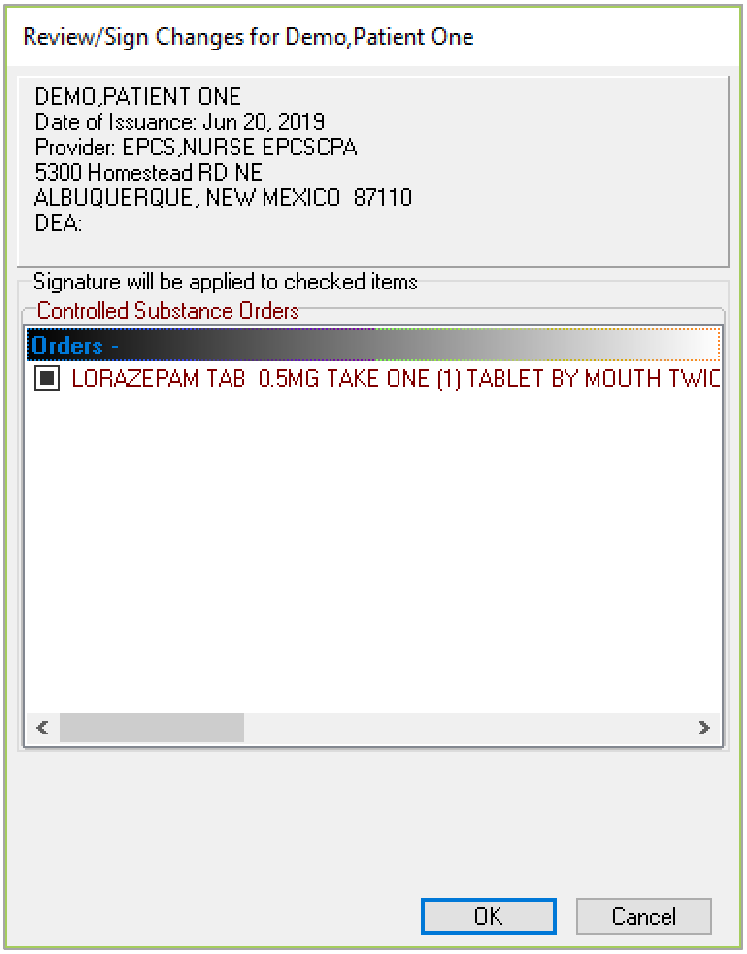
Figure 3-15: Medication Order dialog

Scribes generally should not have any order keys. Ancillary healthcare providers may have the ORELSE key. While the logged-in user can create the order as long as an appropriate ordering provider is chosen, the logged-in user may not sign the order on behalf of the ordering provider.

When signing, the person logged in is checked and not the ordering provider. This prevents the unauthorized user from signing the order.

A user with no order keys will see the dialog in Figure 3-16 when attempting to sign a CS medication order. Clicking **OK** will dismiss the dialog.

Leaving the order unsigned, whether an attempt was made at signing the order or not, causes a notification to be sent to the ordering provider to sign the order.



Review/Sign Changes for Demo,Patient One

DEMO,PATIENT ONE
Date of Issuance: Jun 20, 2019
Provider: EPCS,NURSE EPCSCPA
5300 Homestead RD NE
ALBUQUERQUE, NEW MEXICO 87110
DEA:

Signature will be applied to checked items

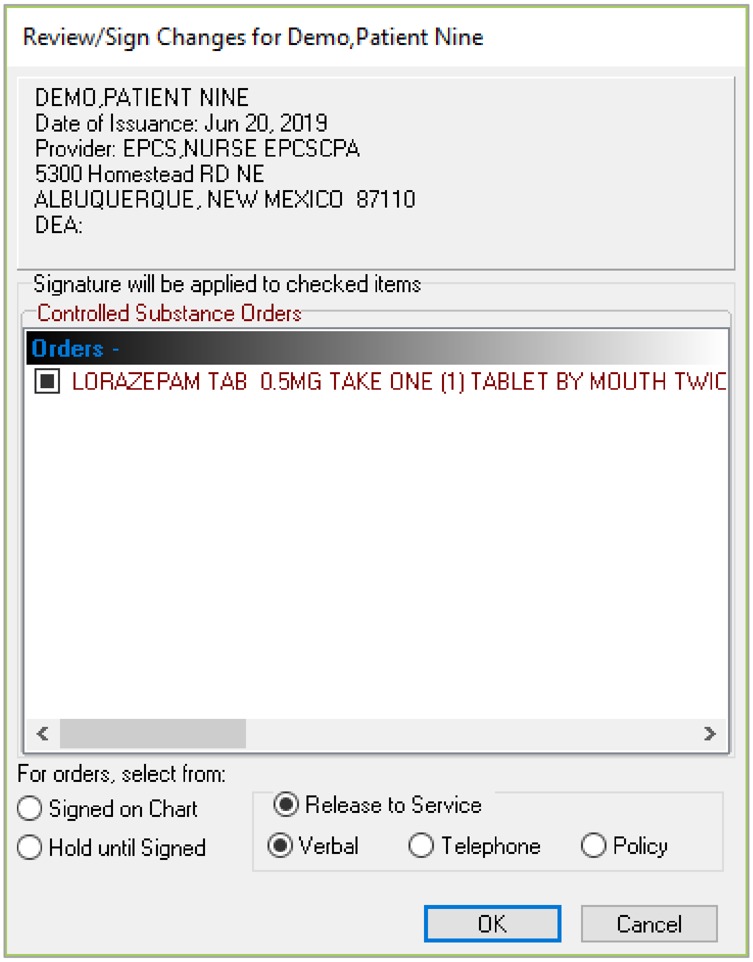
Controlled Substance Orders

Orders -

■ LORAZEPAM TAB 0.5MG TAKE ONE (1) TABLET BY MOUTH TWIC

Figure 3-16: Signing dialog of scribe with no ordering key

An ancillary healthcare provider will see the standard ORELSE key holder signing dialog as shown in Figure 3-17. No matter which option the user chooses on this dialog, the order will ***not*** be released because the user does not have the authorization and is not EPCS enabled. This will also be true if attempting to release an order by policy from the Order component, which will look slightly different from the figure below. It is best to simply enter the order and leave it unsigned. The provider will receive a notification to sign the order.


Review/Sign Changes for Demo,Patient Nine

DEMO,PATIENT NINE
Date of Issuance: Jun 20, 2019
Provider: EPCS,NURSE EPCSCPA
5300 Homestead RD NE
ALBUQUERQUE, NEW MEXICO 87110
DEA:

Signature will be applied to checked items

Controlled Substance Orders

Orders -

☒ LORAZEPAM TAB 0.5MG TAKE ONE (1) TABLET BY MOUTH TWIC

For orders, select from:

○ Signed on Chart
○ Hold until Signed

● Release to Service

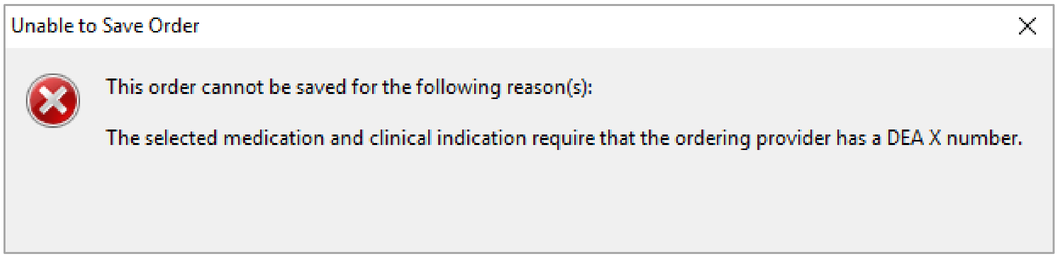
● Verbal ○ Telephone ○ Policy

Figure 3-17: Ancillary Healthcare Provider signing dialog

3.1.3.4 Outpatient Detoxification Orders

Orders for schedule III-V medications intended for detox of outpatients have special requirements. An order for a drug approved by the FDA specifically for outpatient “detoxification treatment”, when used for a “detoxification” indication, must include the provider’s DEA X (also known as the NADEAN) and must contain the medical need for using the selected drug.

Because the system must be able to access the reason the medication is being ordered to determine if the DEA X is included, these orders will require the clinical indication, regardless of the site’s settings for clinical indication for medications. This will also satisfy the need for a medical reason. If the selected medication is in the set of approved detox drugs, and the selected clinical indication is included in the set designated as “detox,” the system will check to see if the ordering provider has a valid DEA X. If the provider does not have a valid DEA X, EPCS will not allow the order to be processed and the provider will receive an error message as seen in Figure 3-18:



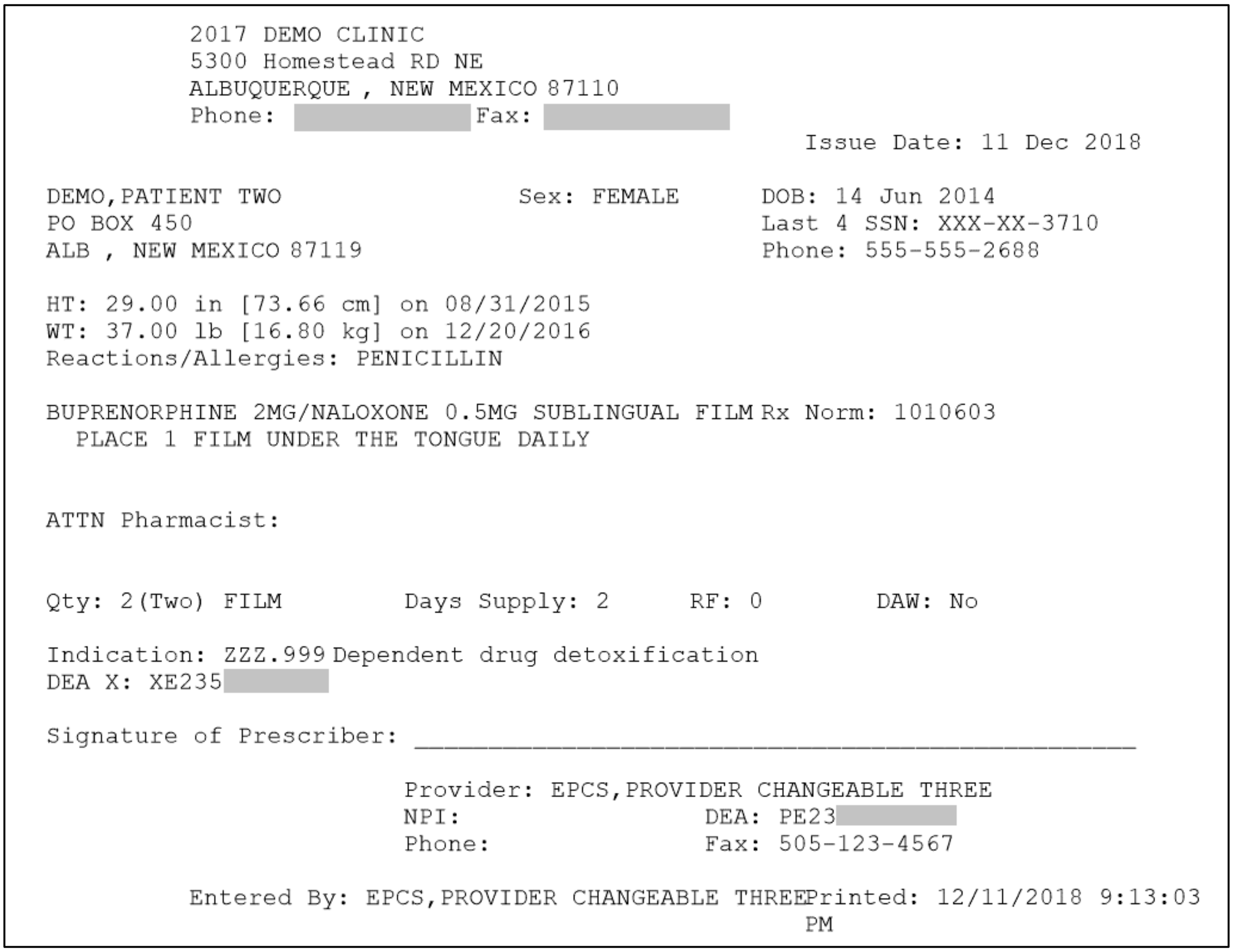
Unable to Save Order

This order cannot be saved for the following reason(s):

The selected medication and clinical indication require that the ordering provider has a DEA X number.

Figure 3-18: Unable to Save Order warning for no DEA X Number

The DEA X will display on the printed prescription as noted in Figure 3-19 (provided the user selects an EPCS-approved format).

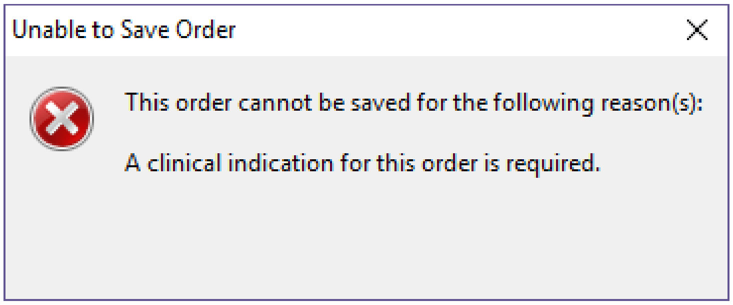


```
          2017 DEMO CLINIC
          5300 Homestead RD NE
          ALBUQUERQUE , NEW MEXICO 87110
          Phone: [redacted] Fax: [redacted]
                                                  Issue Date: 11 Dec 2018

DEMO,PATIENT TWO               Sex: FEMALE      DOB: 14 Jun 2014
PO BOX 450                                      Last 4 SSN: XXX-XX-3710
ALB , NEW MEXICO 87119                          Phone: 555-555-2688

HT: 29.00 in [73.66 cm] on 08/31/2015
WT: 37.00 lb [16.80 kg] on 12/20/2016
Reactions/Allergies: PENICILLIN

BUPRENORPHINE 2MG/NALOXONE 0.5MG SUBLINGUAL FILM Rx Norm: 1010603
  PLACE 1 FILM UNDER THE TONGUE DAILY


ATTN Pharmacist:


Qty: 2(Two) FILM        Days Supply: 2      RF: 0        DAW: No

Indication: ZZZ.999 Dependent drug detoxification
DEA X: XE235[redacted]

Signature of Prescriber: _________________________________________________

                        Provider: EPCS,PROVIDER CHANGEABLE THREE
                        NPI:                DEA: PE23[redacted]
                        Phone:              Fax: 505-123-4567

          Entered By: EPCS,PROVIDER CHANGEABLE THREEPrinted: 12/11/2018 9:13:03
                                                  PM
```

Figure 3-19: DEA X displays on printed order (partially masked for privacy)

3.1.3.5 Gamma-hydroxybutyrate (GHB) Orders

Orders for GHB-containing medications have special requirements. When ordering a medication containing GHB or its derivatives, the clinical indication is required in the order, regardless of the site settings for clinical indication for medications.



Unable to Save Order

This order cannot be saved for the following reason(s):

A clinical indication for this order is required.

Figure 3-20: GHB medication missing clinical indication

3.1.4 Surescripts Refill Request Restrictions

For sites that are set up with Surescripts for ePrescribing, the renew requests and responses may include CS medications once the site is EPCS enabled. All the same requirements for creating a CS order as outlined previously will still apply, including the requirement for 2FA when signing the orders. In addition, CS renewal request responses are restricted to Denied or Denied with New Order to Follow if:

- The provider’s complete name was not included in the message.
- The provider is not authorized for EPCS.
- The provider is not authorized for the class of medication requested.
- The patient does not have an address, or the address check failed.
- The incoming request is beyond the issue date restrictions for the category of CS medication requested.
- The medication requested is in the C-II schedule.
- The Notes to Pharmacist field is too long to fit the RPMS restrictions.

3.1.5 Order Using the CIR Tool

The provider may order controlled substances using the EPCS functions even when ordering through the CIR tool. The CIR tool was updated to mirror the ordering functions from the Medication Management or Order components.

As in the normal ordering process, a provider may order a CS medication electronically via the CIR tool if the provider is EPCS credentialed and has an address; the pharmacy selected to fill the CS medication accepts electronically signed CS medication orders or the order is sent to the internal pharmacy; the site is enabled for EPCS, and the patient has an address. The same warnings received outside of the CIR tool will display inside the CIR tool for the same situations.

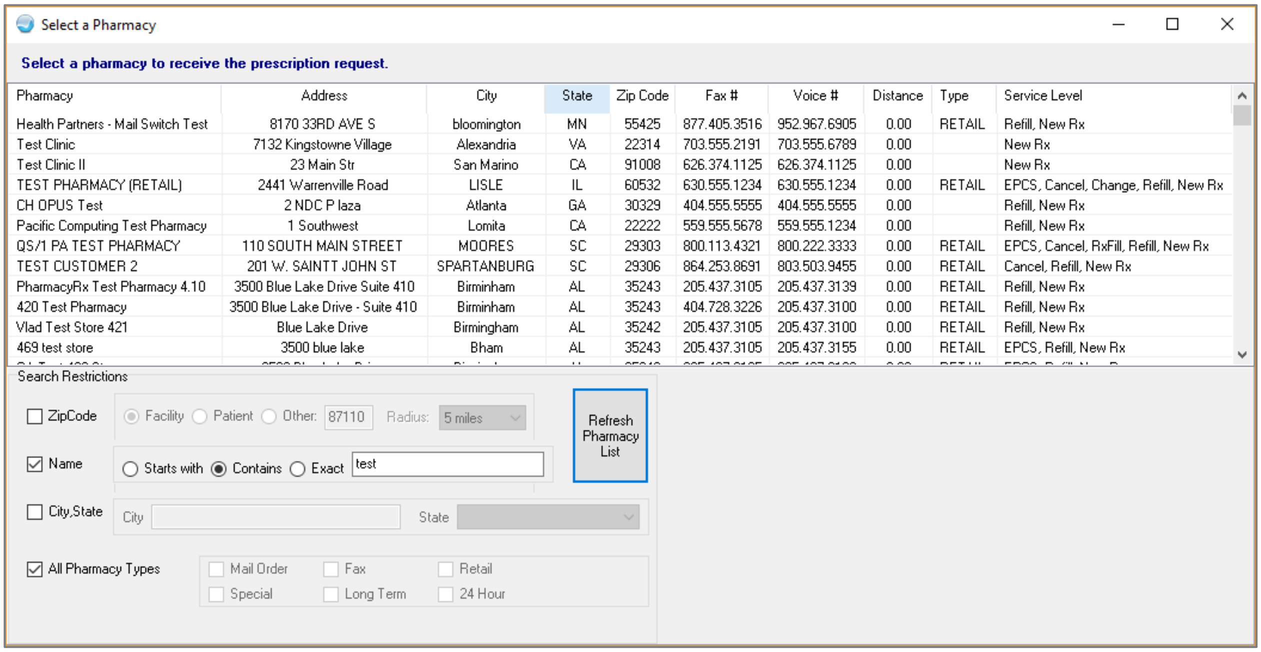
Similarly, the **Days' Supply** field honors the parameter discussed previously that determines the maximum allowable day's supply for a CS order. The value for **Days Supply** field defaults to the value set in the parameter. For example, if the parameter is set to 30, the default value for day's supply will be 30, and only a 30-day supply of a CS medication may be ordered by the provider.

The **Refills** field allows up to five refills to be entered if the CS medication is a C-III, C-IV, or C-V, as is done with the normal ordering process. Entering a number greater than five in the refill field for these schedules will result in an error message as is seen in the normal ordering process. If the provider or ancillary staff attempts to select refills for a C-II medication, the order will not be able to be saved.

The **Earliest Fill Date** field is available for C-II medications ordered via the CIR Tool. The same logic and business rules apply to the CIR Tool as the EHR Medications Order component as to when this date can occur. An Earliest Fill Date cannot be greater than 90 days, or the user receives an error message.

The **Pick Up** locations within the CIR tool have been aligned with those available in the normal ordering process. A 2FA token/certificate pair or PIV and the associated PIN is required to process the electronic order in the CIR tool just as in the medication component of the EHR. If a provider is not EPCS credentialed or does not have a Surescripts Provider Identifier (SPI), the Outside Pharmacy – eRx option is grayed out and is not activated.

If the **Outside Pharmacy – eRx** pick up option is selected, the menu allows the user to select another pharmacy of choice. Within the **Pharmacy Search** window there is a column **Service Level** listing EPCS if a pharmacy accepts CS orders electronically, as seen in Figure 3-21.



Select a pharmacy to receive the prescription request.

Pharmacy	Address	City	State	Zip Code	Fax #	Voice #	Distance	Type	Service Level
Health Partners - Mail Switch Test	8170 33RD AVE S	bloomington	MN	55425	877.405.3516	952.967.6905	0.00	RETAIL	Refill, New Rx
Test Clinic	7132 Kingstowne Village	Alexandria	VA	22314	703.555.2191	703.555.6789	0.00		New Rx
Test Clinic II	23 Main Str	San Marino	CA	91008	626.374.1125	626.374.1125	0.00		New Rx
TEST PHARMACY (RETAIL)	2441 Warrenville Road	LISLE	IL	60532	630.555.1234	630.555.1234	0.00	RETAIL	EPCS, Cancel, Change, Refill, New Rx
CH OPUS Test	2 NDC P laza	Atlanta	GA	30329	404.555.5555	404.555.5555	0.00		Refill, New Rx
Pacific Computing Test Pharmacy	1 Southwest	Lomita	CA	22222	559.555.5678	559.555.1234	0.00		Refill, New Rx
QS/1 PA TEST PHARMACY	110 SOUTH MAIN STREET	MOORES	SC	29303	800.113.4321	800.222.3333	0.00	RETAIL	EPCS, Cancel, RxFill, Refill, New Rx
TEST CUSTOMER 2	201 W. SAINTT JOHN ST	SPARTANBURG	SC	29306	864.253.8691	803.503.9455	0.00	RETAIL	Cancel, Refill, New Rx
PharmacyRx Test Pharmacy 4.10	3500 Blue Lake Drive Suite 410	Birminham	AL	35243	205.437.3105	205.437.3139	0.00	RETAIL	Refill, New Rx
420 Test Pharmacy	3500 Blue Lake Drive - Suite 410	Birminham	AL	35243	404.728.3226	205.437.3100	0.00	RETAIL	Refill, New Rx
Vlad Test Store 421	Blue Lake Drive	Birmingham	AL	35242	205.437.3105	205.437.3100	0.00	RETAIL	Refill, New Rx
469 test store	3500 blue lake	Bham	AL	35243	205.437.3105	205.437.3155	0.00	RETAIL	EPCS, Refill, New Rx

Search Restrictions

☐ ZipCode ● Facility ○ Patient ○ Other: 87110 Radius: 5 miles

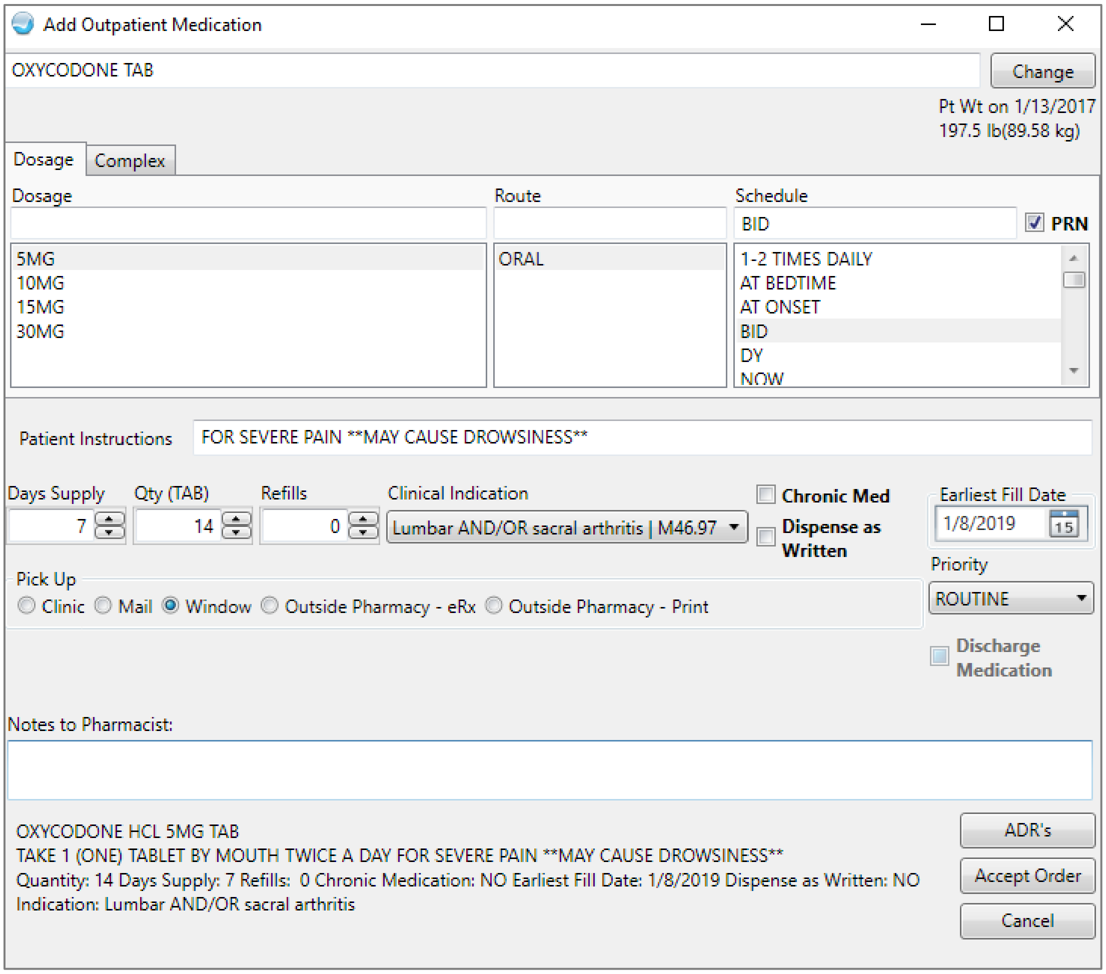
☑ Name ○ Starts with ● Contains ○ Exact test

☐ City,State City State

☑ All Pharmacy Types ☐ Mail Order ☐ Fax ☐ Retail ☐ Special ☐ Long Term ☐ 24 Hour

Figure 3-21: Select a Pharmacy dialog with Service level column on right

In the field below the **Notes to Pharmacist** area, the medication orders window contains the name of the medication, dose, strength, form, quantity, directions for use, the number of refills, the earliest fill date (if the order is for a C-II medication), and the clinical indication for the CS medication as seen in Figure 3-22:



OXYCODONE TAB

Pt Wt on 1/13/2017
197.5 lb(89.58 kg)

Dosage: 5MG, 10MG, 15MG, 30MG

Route: ORAL

Schedule: BID ☑ PRN

1-2 TIMES DAILY
AT BEDTIME
AT ONSET
BID
DY
NOW

Patient Instructions: FOR SEVERE PAIN **MAY CAUSE DROWSINESS**

Days Supply: 7
Qty (TAB): 14
Refills: 0
Clinical Indication: Lumbar AND/OR sacral arthritis | M46.97
□ Chronic Med
□ Dispense as Written
Earliest Fill Date: 1/8/2019

Pick Up: ○ Clinic ○ Mail ● Window ○ Outside Pharmacy - eRx ○ Outside Pharmacy - Print

Priority: ROUTINE

□ Discharge Medication

Notes to Pharmacist:

OXYCODONE HCL 5MG TAB
TAKE 1 (ONE) TABLET BY MOUTH TWICE A DAY FOR SEVERE PAIN **MAY CAUSE DROWSINESS**
Quantity: 14 Days Supply: 7 Refills: 0 Chronic Medication: NO Earliest Fill Date: 1/8/2019 Dispense as Written: NO
Indication: Lumbar AND/OR sacral arthritis

Figure 3-22: Add Outpatient Medication dialog with Earliest Fill Date field enabled

Additional information about the CS order has been added to the Order Reconciled Medication field. The name of the CS medication now appears with the following details about that order: Name of medication; dosage; route and frequency; reason for medication; quantity (number of days) of medication to be dispensed; number of refills, whether or not the medication is for chronic administration; the earliest fill date, and other directions from the prescribing provider.

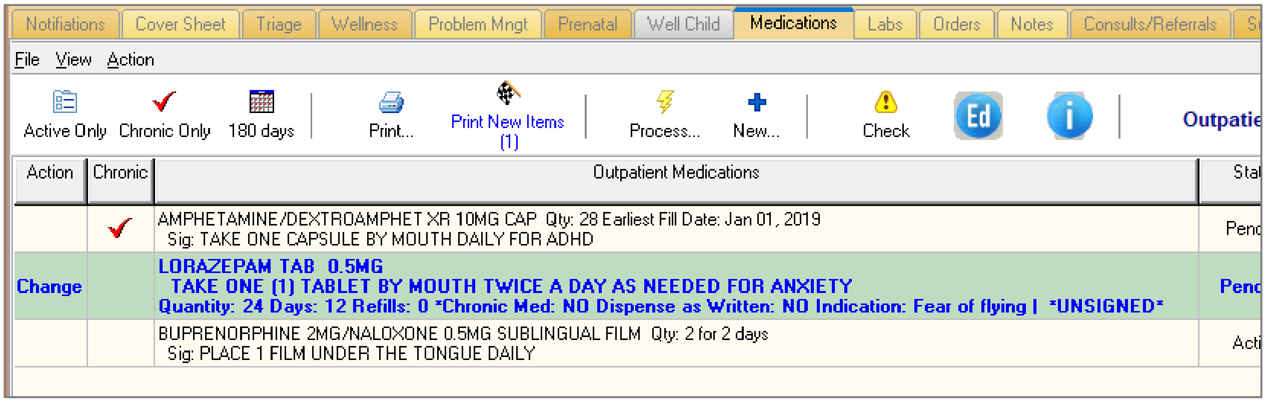
When providers order a CS Detox or GHB medication via the CIR Tool, the same behavior is seen as noted in Section 3.1.3.4 or 3.1.3.5, respectively.

3.1.6 Working with Existing CS Medication Orders

All the options that previously existed within the Medications Management component still exist, with some additional steps added to accommodate changes made to electronically sign CS medication outpatient orders. These changes are as noted in the following menu options.

3.1.6.1 Change

As before, when changing an outpatient CS medication order or prescription, select the medication you want to change and select **Action** then **Change** (or select the **Change** option on the right-click menu). Complete the changes to the dosage, route, schedule, etc. of an existing medication order. This option does not allow you to change the medication itself (the Change button will not be active). Upon clicking **Accept Order**, the **Outpatient Medication** order changes color with the action noted as **Change** in the far-left column as seen in Figure 3-23:



Action	Chronic	Outpatient Medications	Stat
	✓	AMPHETAMINE/DEXTROAMPHET XR 10MG CAP Qty: 28 Earliest Fill Date: Jan 01, 2019 Sig: TAKE ONE CAPSULE BY MOUTH DAILY FOR ADHD	Pend
Change		LORAZEPAM TAB 0.5MG TAKE ONE (1) TABLET BY MOUTH TWICE A DAY AS NEEDED FOR ANXIETY Quantity: 24 Days: 12 Refills: 0 *Chronic Med: NO Dispense as Written: NO Indication: Fear of flying | *UNSIGNED*	Pend
		BUPRENORPHINE 2MG/NALOXONE 0.5MG SUBLINGUAL FILM Qty: 2 for 2 days Sig: PLACE 1 FILM UNDER THE TONGUE DAILY	Acti

Figure 3-23: Changed medication displays “Change” in the Action column

3.1.6.2 Copy to New Order

The **Copy to New Order** option continues to appear on the Outpatient and Inpatient group boxes. The steps to complete this task have not been changed from its previous functionality, with the exception of signing a CS medication order if the provider is EPCS credentialed and the site is as well.

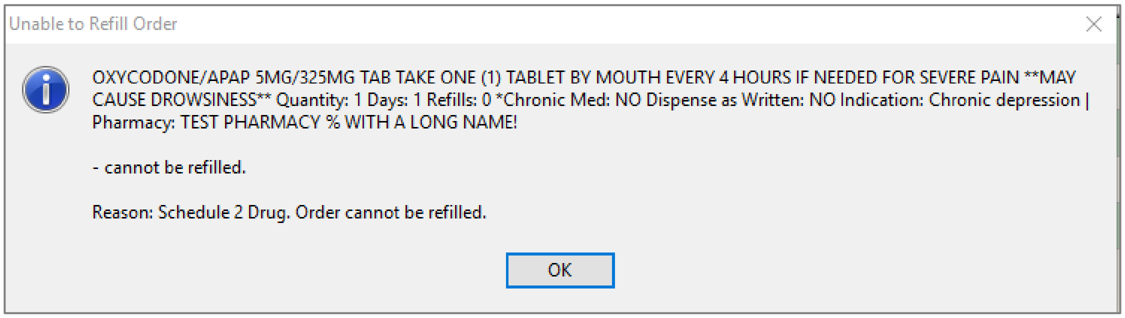
3.1.6.3 Discontinue or Cancel

The user is still able to discontinue or cancel an order or prescription as before. If the order has not been signed at the time it is cancelled, the order is deleted from the system entirely. If the order was signed or signed and processed, then the order details are retained in the system but marked as discontinued. Discontinuing a controlled substance does not require 2FA.

3.1.6.4 Refill

Providers can request a refill on behalf of the patient only for outpatient medications that are active and have refills available. If a prescription is not active and/or does not have refills available, the prescription must be renewed or have a new order created.

The Unable to Refill Order message will display if attempts are made to refill a C-II medication, or if there are no refills remaining from the initial prescription.



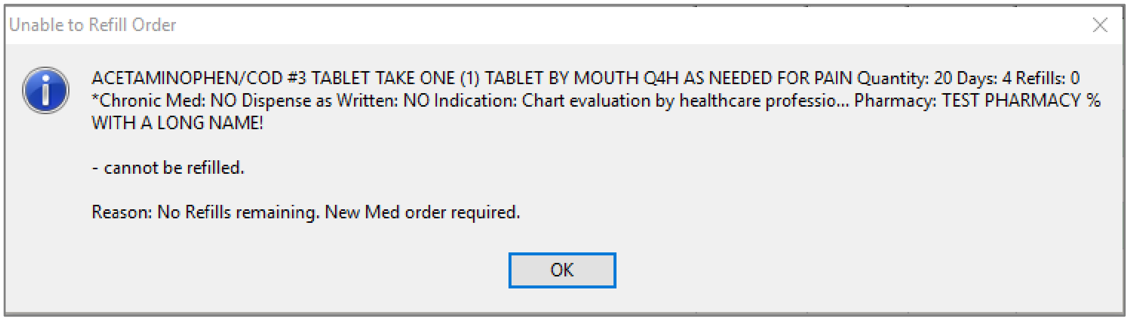
Unable to Refill Order

OXYCODONE/APAP 5MG/325MG TAB TAKE ONE (1) TABLET BY MOUTH EVERY 4 HOURS IF NEEDED FOR SEVERE PAIN **MAY CAUSE DROWSINESS** Quantity: 1 Days: 1 Refills: 0 *Chronic Med: NO Dispense as Written: NO Indication: Chronic depression | Pharmacy: TEST PHARMACY % WITH A LONG NAME!

- cannot be refilled.

Reason: Schedule 2 Drug. Order cannot be refilled.

Figure 3-24: Unable to Refill Order message for a C-II medication



Unable to Refill Order

ACETAMINOPHEN/COD #3 TABLET TAKE ONE (1) TABLET BY MOUTH Q4H AS NEEDED FOR PAIN Quantity: 20 Days: 4 Refills: 0 *Chronic Med: NO Dispense as Written: NO Indication: Chart evaluation by healthcare professio... Pharmacy: TEST PHARMACY % WITH A LONG NAME!

- cannot be refilled.

Reason: No Refills remaining. New Med order required.

Figure 3-25: Unable to Refill Order message for a CS medication that is not a C-II

3.1.6.5 Renew

As was the previous behavior, certain active or recently expired prescriptions may be renewed. The maximum number of days following the expiration can be configured for your site; however, the default is 30 days for controlled substances. Orders and prescriptions for C-II medications, medications marked as narcotics, and other medications specifically designated as “not renewable” in the pharmacy files may not be renewed. For all CS medications, the EPCS rules will apply and the behavior will be the same as creating a new CS order.

3.1.6.6 Process

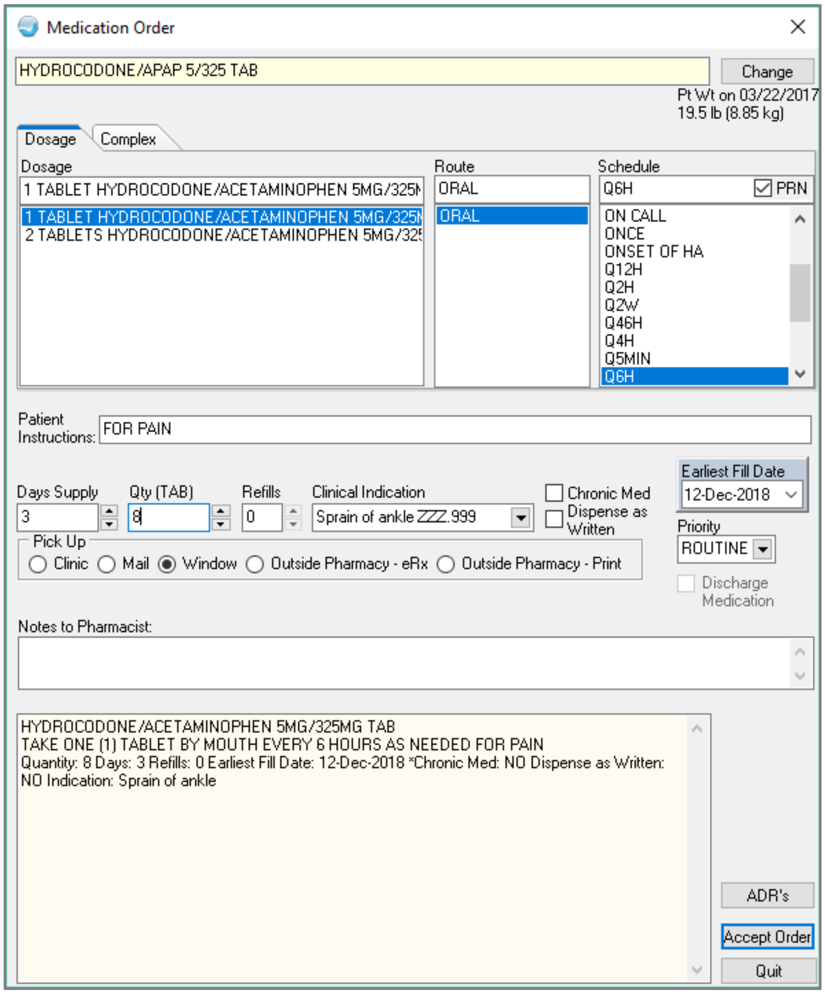
The user may select several medication orders or prescriptions to which different actions will be applied and select the Process function using the Process button or selecting Process from the Action menu or the context menu. Each medication will be presented in turn, and the user may then select the specific action (change, renew, refill, DC) to apply. The selected action will behave as described previously. For all CS medications, the EPCS rules will apply and the behavior will be the same as creating a new CS order.

3.1.6.7 Transfer to Outpatient

The user may select an inpatient or a non-VA medication order and use the transfer to outpatient function to create a new outpatient order for the selected medication. The resulting outpatient order will need to comply with the EPCS rules, so a user who is not authorized to order a C-II medication may not transfer a C-II inpatient or non-VA medication to outpatient. For all CS medications, the EPCS rules will apply and the behavior will be the same as creating a new CS order.

3.2 Pick Up Locations and EPCS

Due to some technical changes unrelated to EPCS regulations, the pick-up options will display differently after installing the EPCS patches. Instead of only displaying the available pick up options for the site, provider, and medication, all pick up locations will be displayed on every order. Some pick-up location options may be inactive, depending on the local site and provider set up. Selection of a Pick Up location will affect the need for a two-factor authentication when signing the CS medication order (Section 3.3), as described in the following sections.



Medication Order

HYDROCODONE/APAP 5/325 TAB

Pt Wt on 03/22/2017
19.5 lb (8.85 kg)

Dosage: 1 TABLET HYDROCODONE/ACETAMINOPHEN 5MG/325M
1 TABLET HYDROCODONE/ACETAMINOPHEN 5MG/325M
2 TABLETS HYDROCODONE/ACETAMINOPHEN 5MG/325

Route: ORAL
ORAL

Schedule: Q6H ☑ PRN
ON CALL
ONCE
ONSET OF HA
Q12H
Q2H
Q2W
Q46H
Q4H
Q5MIN
Q6H

Patient Instructions: FOR PAIN

Days Supply: 3
Qty (TAB): 8
Refills: 0
Clinical Indication: Sprain of ankle ZZZ.999
□ Chronic Med
□ Dispense as Written
Earliest Fill Date: 12-Dec-2018
Priority: ROUTINE
□ Discharge Medication

Pick Up: ○ Clinic ○ Mail ● Window ○ Outside Pharmacy - eRx ○ Outside Pharmacy - Print

Notes to Pharmacist:

HYDROCODONE/ACETAMINOPHEN 5MG/325MG TAB
TAKE ONE (1) TABLET BY MOUTH EVERY 6 HOURS AS NEEDED FOR PAIN
Quantity: 8 Days: 3 Refills: 0 Earliest Fill Date: 12-Dec-2018 *Chronic Med: NO Dispense as Written:
NO Indication: Sprain of ankle

Figure 3-26: Pick Up Location Options

3.2.1 Clinic

When a CS medication is ordered with a Pick Up Location of **Clinic**, 2FA is not required. There are two potential situations where a clinic pickup might be used: a dose of a medication that is administered to the patient while they are in the facility, or a pre-packaged container of a medication that is dispensed to the patient directly by the provider. Both of these situations are exempt from the DEA requirements for ordering CS medications electronically, and thus do not require 2FA to process the order. In addition, the user will not be required to print the order so the Print function will not be triggered.

Duplicate orders for C-II medications will be allowed when the Clinic pick up option is selected; that is, users will be able to enter a Clinic medication to be administered on site, and create an additional order with a different pick up location for the same medication without being prompted to discontinue the first order. The Clinic order may be input before the non-clinic order or after it.

3.2.2 Mail

When a CS medication is ordered with a Pick Up location of **Mail**, the system will require 2FA if:

- The site is EPCS enabled.
- The provider is EPCS enabled.
- The provider hash is valid.

In all other cases, the order must be printed and manually signed.

3.2.3 Window

When a CS medication is ordered with a Pick Up location of **Window**, the order will be sent to the internal pharmacy for processing.

The following conditions must be met to trigger 2FA for **Window** Pick Up:

- The Site has an internal pharmacy.
- The Site is EPCS enabled.
- The provider is EPCS enabled.
- The provider hash is valid.

In all other cases, the order must be printed and manually signed.

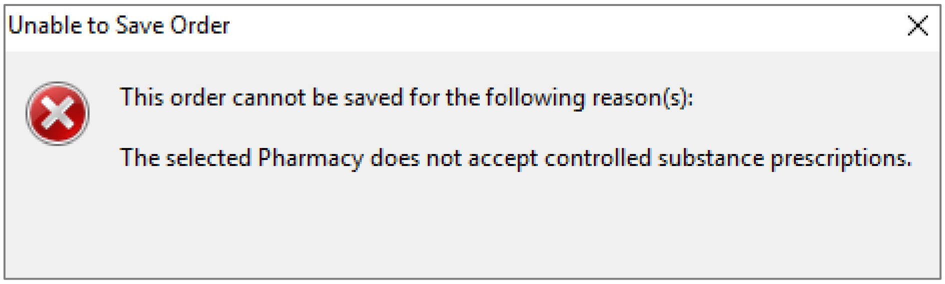
3.2.4 Outside Pharmacy – eRx

The **Outside Pharmacy – eRx** Pick Up location is only enabled for CS medications when the facility meets all the requirements and is set up for Surescripts transmission. This Pick Up location will always require 2FA.

Because there is no option to print and sign for this pickup location, it will only be active if the following conditions are met:

- The provider has a valid DEA or VA number.
- The provider has a valid SPI number.
- The site is approved to send controlled substances to Surescripts.
- The Surescripts parameters are set to allow sending of controlled substances.
- The Site is EPCS enabled.
- The provider is EPCS enabled.

In addition, to save the order, the pharmacy selected must be able to receive EPCS medications. If the pharmacy selected does not process EPCS orders, the provider will get a message to select a different pharmacy.



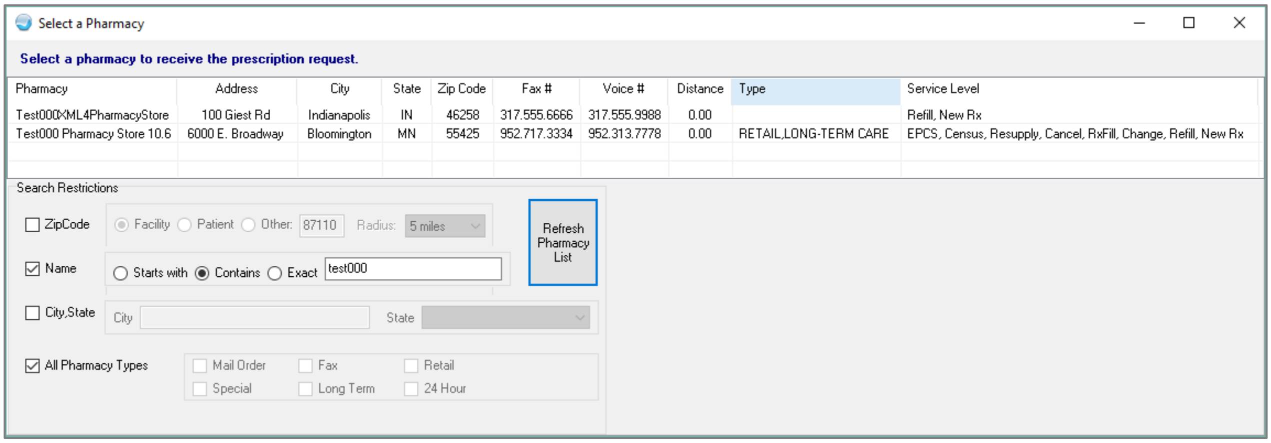
Unable to Save Order

This order cannot be saved for the following reason(s):

The selected Pharmacy does not accept controlled substance prescriptions.

Figure 3-27: Unable to Save Order dialog for non-EPCS pharmacy

To see which pharmacies accept EPCS orders, a new column displays in the **Select a Pharmacy** window, called **Service Level**. All pharmacies that can accept EPCS orders will display with “EPCS” in that column.



Select a Pharmacy

Select a pharmacy to receive the prescription request.

Pharmacy	Address	City	State	Zip Code	Fax #	Voice #	Distance	Type	Service Level
Test000XML4PharmacyStore	100 Giest Rd	Indianapolis	IN	46258	317.555.6666	317.555.9988	0.00		Refill, New Rx
Test000 Pharmacy Store 10.6	6000 E. Broadway	Bloomington	MN	55425	952.717.3334	952.313.7778	0.00	RETAIL,LONG-TERM CARE	EPCS, Census, Resupply, Cancel, RxFill, Change, Refill, New Rx

Search Restrictions

□ ZipCode ● Facility ○ Patient ○ Other: 87110 Radius: 5 miles

☑ Name ○ Starts with ● Contains ○ Exact test000

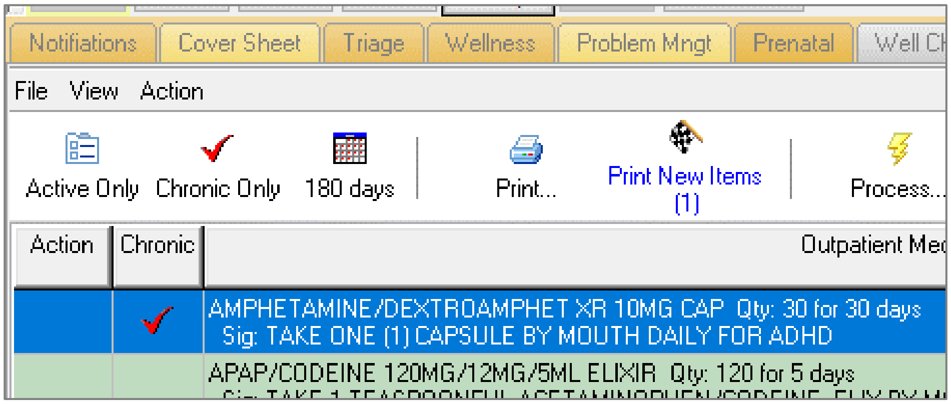
□ City,State City State

☑ All Pharmacy Types □ Mail Order □ Fax □ Retail □ Special □ Long Term □ 24 Hour

Figure 3-28: The Select a Pharmacy dialog showing Service Level column

3.2.5 Outside Pharmacy – Print

When a CS medication is ordered with a Pick Up location of **Outside Pharmacy - Print**, the system will add the prescription to the Print Queue. The provider will then print a hard copy to sign and send with the patient for pharmacy processing. The system will not prompt the provider for 2FA when this location is selected.



Action	Chronic	Outpatient Med
	✓	AMPHETAMINE/DEXTROAMPHET XR 10MG CAP Qty: 30 for 30 days Sig: TAKE ONE (1) CAPSULE BY MOUTH DAILY FOR ADHD
		APAP/CODEINE 120MG/12MG/5ML ELIXIR Qty: 120 for 5 days

Figure 3-29: Print Queue with prescription awaiting action

3.3 Signing Controlled Substance Orders

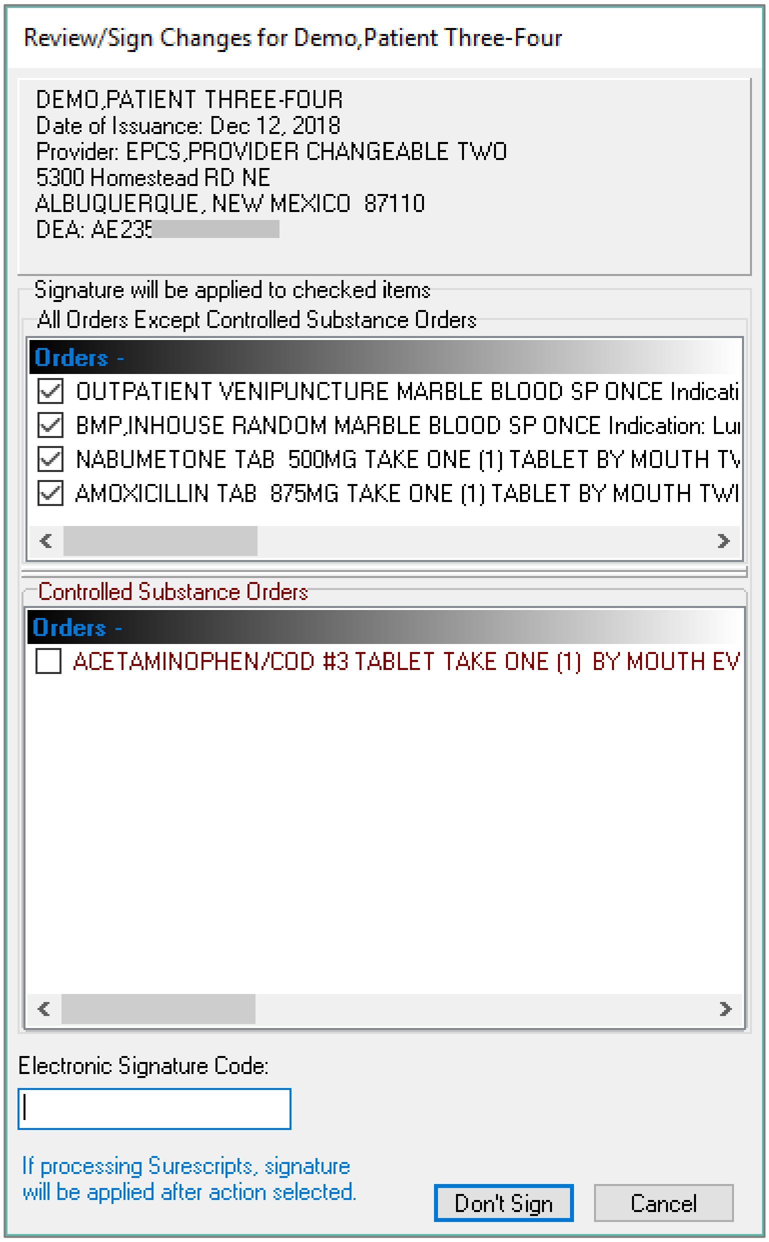
After a CS medication order is placed, the provider may electronically sign the order using the Integrated Signature Tool and an electronic signature code. If the provider, site, and order characteristics allow the provider to use EPCS, the provider will also use a two-factor authentication method in the form of a cryptographic token/certificate pair or PIV with the associated PIN in addition to the electronic signature code.

3.3.1 Signing Without 2FA Methods

The process for signing without 2FA methods is essentially the same as it was prior to EPCS. However, the signing dialog does contain some changes. The dialog may have one, two, or three panes depending on the items ordered:

- The top pane includes non-CS medications, inpatient CS medications, and non-medication orders (if any are present);
- The middle pane includes other orders such as unsigned orders from another day or another provider (depending on site settings);
- The bottom pane includes outpatient CS orders (if any are present).

The non-CS orders will be checked by default, the CS orders must be checked by the provider to indicate that they are "ready to sign." Only panes with active orders of that type will display. For example, if only EPCS CS orders are present, only one pane displays. Likewise, if non-CS orders and CS orders are present but not any "other" orders, only two panes display.



Review/Sign Changes for Demo,Patient Three-Four

DEMO,PATIENT THREE-FOUR
Date of Issuance: Dec 12, 2018
Provider: EPCS,PROVIDER CHANGEABLE TWO
5300 Homestead RD NE
ALBUQUERQUE, NEW MEXICO 87110
DEA: AE235[redacted]

Signature will be applied to checked items

All Orders Except Controlled Substance Orders

Orders -

☑ OUTPATIENT VENIPUNCTURE MARBLE BLOOD SP ONCE Indicati
☑ BMP,INHOUSE RANDOM MARBLE BLOOD SP ONCE Indication: Lu
☑ NABUMETONE TAB 500MG TAKE ONE (1) TABLET BY MOUTH T\
☑ AMOXICILLIN TAB 875MG TAKE ONE (1) TABLET BY MOUTH TWI

Controlled Substance Orders

Orders -

☐ ACETAMINOPHEN/COD #3 TABLET TAKE ONE (1) BY MOUTH EV

Electronic Signature Code:

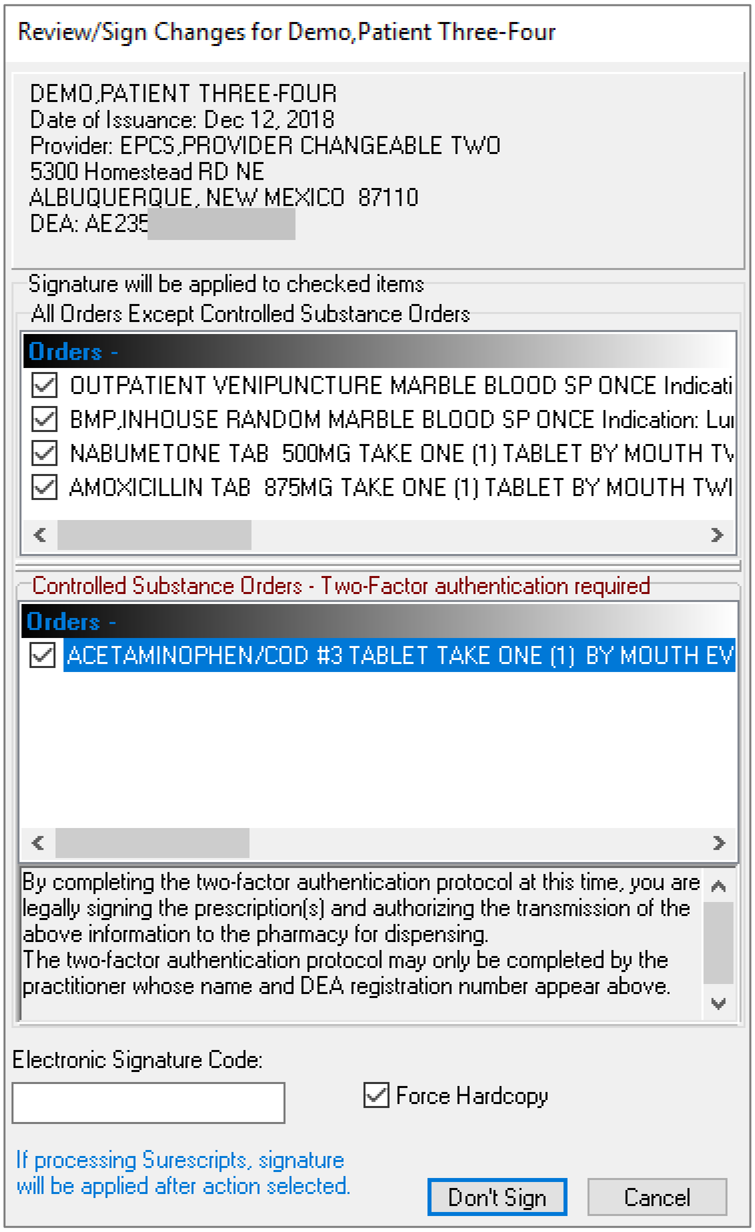
If processing Surescripts, signature will be applied after action selected.

Figure 3-30: Review/Sign Changes dialog with non-CS orders checked and CS orders unchecked by default

When no CS medications requiring a digital signature are present or the provider has not checked such orders, the 2FA informational text will not display, and no 2FA method will be required. All items checked will be signed immediately.

3.3.1.1 Force Hardcopy

There is a parameter that will display a **Force Hardcopy** check box in the **Review/Sign Changes** dialog for a provider who is EPCS-enabled. This parameter should be used conservatively, and only for situations where a provider has justifiable reasons to use a hardcopy order even though the provider is approved for EPCS. This is not allowed to be used if a token or PIV is lost, stolen, or otherwise compromised; in that instance the EPCS permissions must be inactivated until a new token or PIV is obtained. The check box will display when the CS order is marked as ready to sign. When **Force Hardcopy** is checked, the order will not require 2FA.



Review/Sign Changes for Demo,Patient Three-Four

DEMO,PATIENT THREE-FOUR
Date of Issuance: Dec 12, 2018
Provider: EPCS,PROVIDER CHANGEABLE TWO
5300 Homestead RD NE
ALBUQUERQUE, NEW MEXICO 87110
DEA: AE235[redacted]

Signature will be applied to checked items

All Orders Except Controlled Substance Orders

Orders -

☑ OUTPATIENT VENIPUNCTURE MARBLE BLOOD SP ONCE Indicati
☑ BMP,INHOUSE RANDOM MARBLE BLOOD SP ONCE Indication: Lu
☑ NABUMETONE TAB 500MG TAKE ONE (1) TABLET BY MOUTH TV
☑ AMOXICILLIN TAB 875MG TAKE ONE (1) TABLET BY MOUTH TWI

Controlled Substance Orders - Two-Factor authentication required

Orders -

☑ ACETAMINOPHEN/COD #3 TABLET TAKE ONE (1) BY MOUTH EV

By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing.
The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear above.

Electronic Signature Code:

☑ Force Hardcopy

If processing Surescripts, signature will be applied after action selected.

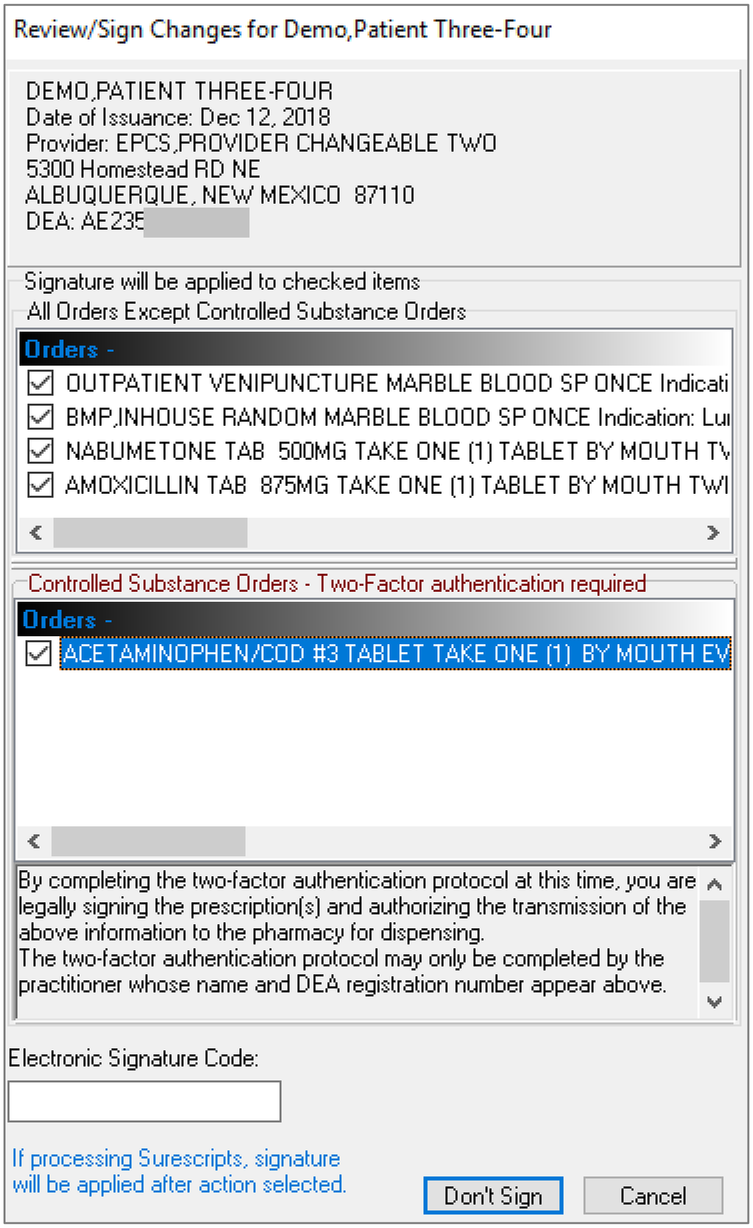
Figure 3-31: Review/Sign Changes dialog with Force Hardcopy check box

3.3.2 Signing with 2FA Methods

The process for signing with 2FA methods adds one step to the process, in addition to the changes to the Order dialog described previously.

To sign using 2FA:

1. Click the Integrated **Signature Tool** button to display the **Review/Sign Changes** dialog. Any CS medication orders will be unchecked by default. Each CS medication order must be checked to be signed.



Review/Sign Changes for Demo,Patient Three-Four

DEMO,PATIENT THREE-FOUR
Date of Issuance: Dec 12, 2018
Provider: EPCS,PROVIDER CHANGEABLE TWO
5300 Homestead RD NE
ALBUQUERQUE, NEW MEXICO 87110
DEA: AE235[redacted]

Signature will be applied to checked items

All Orders Except Controlled Substance Orders

Orders -

☑ OUTPATIENT VENIPUNCTURE MARBLE BLOOD SP ONCE Indicati
☑ BMP,INHOUSE RANDOM MARBLE BLOOD SP ONCE Indication: Lu
☑ NABUMETONE TAB 500MG TAKE ONE (1) TABLET BY MOUTH TV
☑ AMOXICILLIN TAB 875MG TAKE ONE (1) TABLET BY MOUTH TWI

Controlled Substance Orders - Two-Factor authentication required

Orders -

☑ ACETAMINOPHEN/COD #3 TABLET TAKE ONE (1) BY MOUTH EV

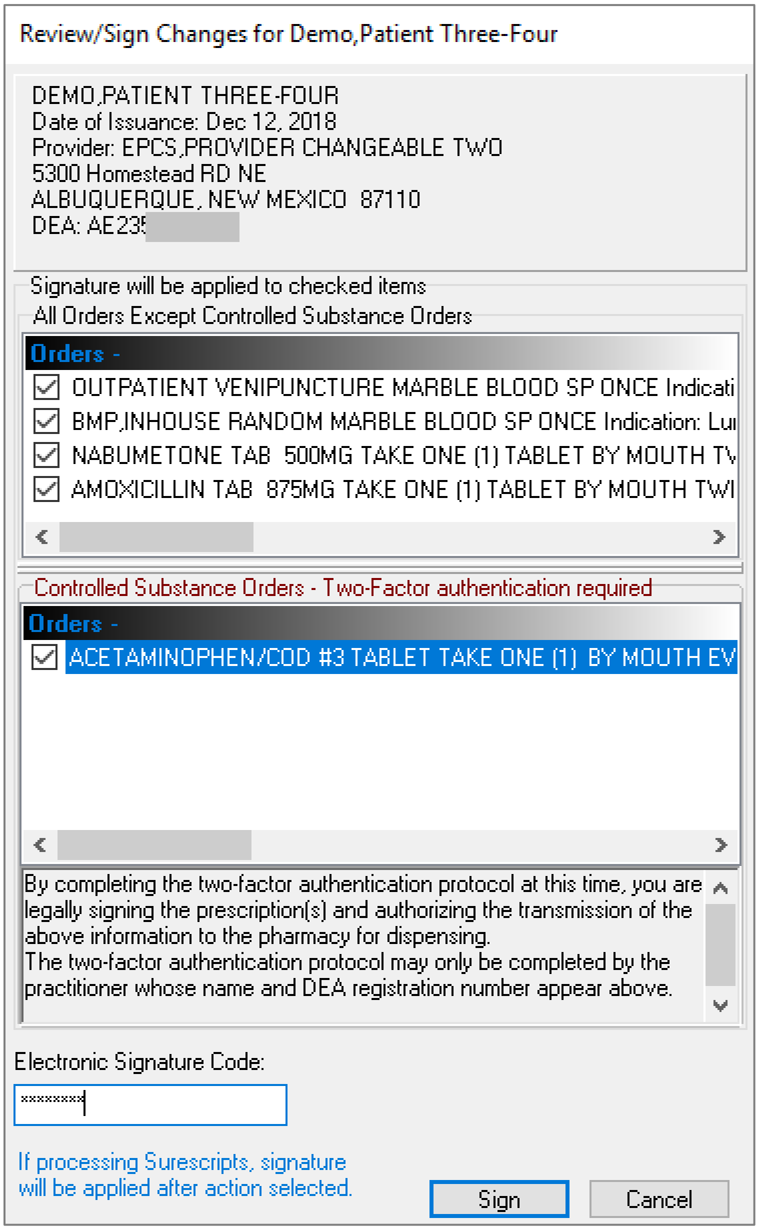
By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing.
The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear above.

Electronic Signature Code:

If processing Surescripts, signature will be applied after action selected.

Figure 3-32: The Review/Sign Changes dialog with CS order checked and 2FA informational text displaying

2. The **Electronic Signature Code** field displays, as does the informational text about completing the 2FA protocol. Upon entering your electronic signature, the **Don't Sign** button changes to a **Sign** button.



Review/Sign Changes for Demo,Patient Three-Four

DEMO,PATIENT THREE-FOUR
Date of Issuance: Dec 12, 2018
Provider: EPCS,PROVIDER CHANGEABLE TWO
5300 Homestead RD NE
ALBUQUERQUE, NEW MEXICO 87110
DEA: AE23[redacted]

Signature will be applied to checked items

All Orders Except Controlled Substance Orders

Orders -

☑ OUTPATIENT VENIPUNCTURE MARBLE BLOOD SP ONCE Indicati
☑ BMP,INHOUSE RANDOM MARBLE BLOOD SP ONCE Indication: Lu
☑ NABUMETONE TAB 500MG TAKE ONE (1) TABLET BY MOUTH TV
☑ AMOXICILLIN TAB 875MG TAKE ONE (1) TABLET BY MOUTH TWI

Controlled Substance Orders - Two-Factor authentication required

Orders -

☑ ACETAMINOPHEN/COD #3 TABLET TAKE ONE (1) BY MOUTH EV

By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing.
The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear above.

Electronic Signature Code: ********

If processing Surescripts, signature will be applied after action selected.

Figure 3-33: The Don't Sign button changes to a Sign button

3. Insert the token or PIV and click **Sign**. An **Order Checking** dialog may display.

4. Once the Order Checks are cleared, the **Identity Verification** dialog displays with the certificate information and a field to enter the token or PIV's PIN and buttons **Sign** and **Cancel**. Until an entry in the PIN field is made, the Sign button is inactive. Once an entry has been made, the Sign button becomes active. Any non-CS orders and CS orders not requiring 2FA will be signed immediately upon selection of the Sign button, while the CS orders requiring 2FA will not be signed until the 2FA steps that follow are completed.

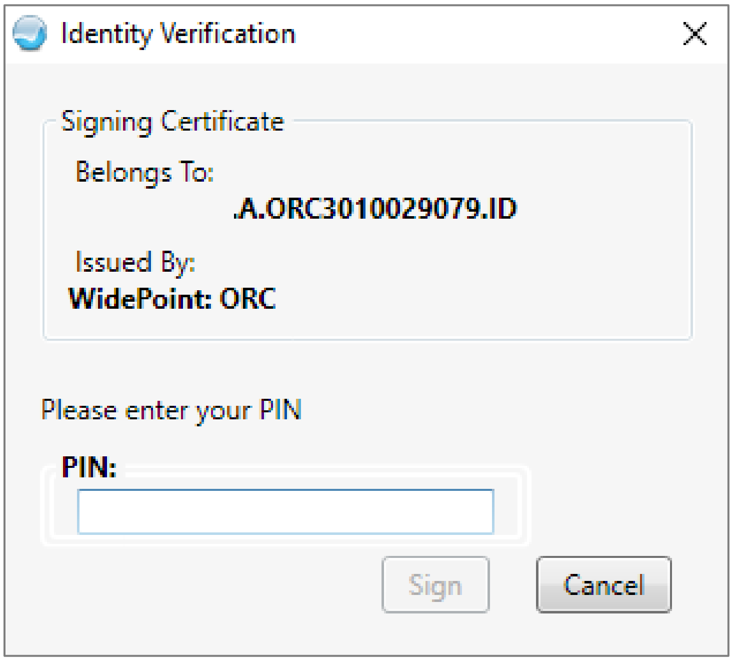


Figure 3-34: Identity Verification dialog

Note: Depending on the certificate issuer and the specific token or PIV being used, the PIN may be all numeric or alphanumeric. An alphanumeric PIN will be case-sensitive, so a pop-up warning will display if the Caps Lock is engaged.

5. The CS medication orders will be signed on successful PIN entry and will display as usual in the Medication Management and Orders components. Orders will be Active for auto-finished orders or Pending for non-Auto-finished orders.

3.3.3 Signing Multiple CS Orders at Once

When a provider orders more than one CS order requiring 2FA and signs them all in the same session, only one entry of the token's or PIV's PIN is required to sign all the orders.

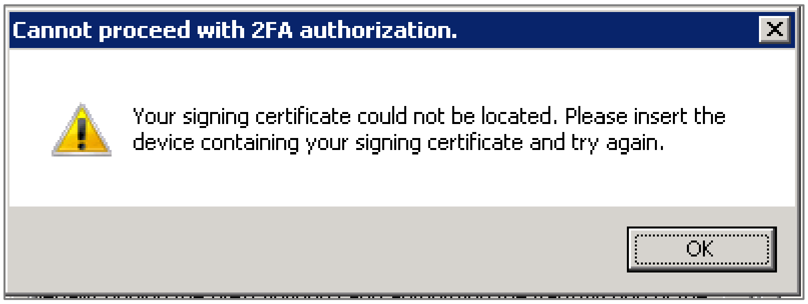
3.3.4 Error Messages Related to Signing EPCS Orders

There are several warning and error messages that may display to the user during the signing process. When the user attempts to sign orders, there is a check for the logged-in user's EPCS authorization, DEA or VA number, and authorized schedules. Errors on these points during signing are most likely to occur if the user attempts to sign an unsigned order entered by another provider but might also occur if the user's credentials have changed between ordering and signing (e.g., if the DEA number expired, the hash changed, or the user's EPCS profile was inactivated), or if the site has turned off EPCS.

The same error messages seen during the ordering process may occur, including the "not authorized for EPCS," "failed hash," and "not authorized for schedule." In addition, the user may see errors related to the certificates and the monitoring process that checks the validity of the certificates. These types of errors will include a reason for the failure. Make note of the message and inform the personnel responsible for maintaining the RPMS system.

3.3.4.1 Token/PIV Never Inserted

This error occurs when a provider is using a computer to order EPCS medications on a computer where the token or PIV has never been inserted. It is resolved by inserting the provider's token or PIV.



Cannot proceed with 2FA authorization.

Your signing certificate could not be located. Please insert the device containing your signing certificate and try again.

Figure 3-35: Signing certificate could not be located

3.3.4.2 Token/PIV Not Inserted

This error occurs if the provider's token or PIV has previously been inserted in the computer but is not currently inserted when the system is attempting to access it. When using a token and the computer has a PIV card reader attached or built in, the PIV reader device will display in the dialog. Once the token has been inserted, it will also be listed and may be selected.

Note: The token is seen by the Windows system as a "smart card" and it is thus referred to as a smart card in the Windows dialogs.

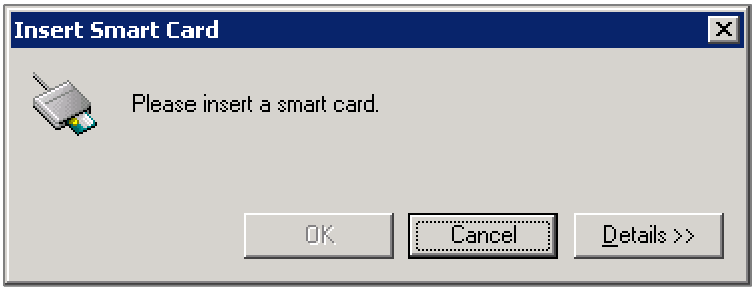


Figure 3-36: Token not inserted, pre-Windows 10

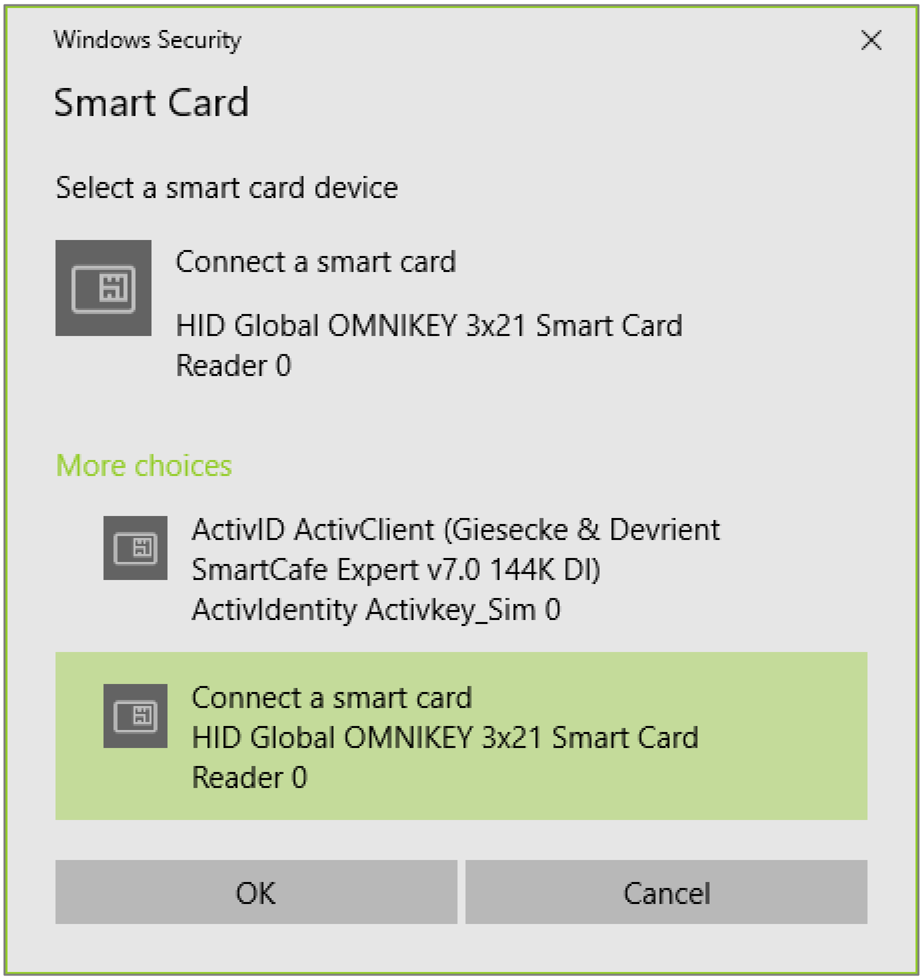
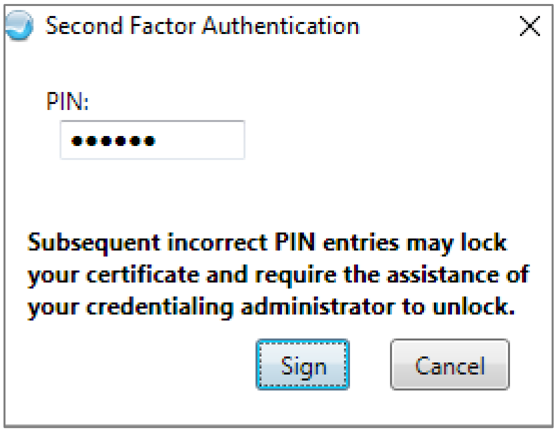

Windows Security
Smart Card
Select a smart card device
Connect a smart card
HID Global OMNIKEY 3x21 Smart Card Reader 0
More choices
ActivID ActivClient (Giesecke & Devrient SmartCafe Expert v7.0 144K DI) ActivIdentity Activkey_Sim 0
Connect a smart card
HID Global OMNIKEY 3x21 Smart Card Reader 0
OK
Cancel

Figure 3-37: Windows 10 Windows Security dialog lists the PIV card reader as well as the newly inserted token as smart card devices

3.3.4.3 Incorrect PIN

This error occurs when the PIN is entered incorrectly or does not match the token or PIV inserted. This message notes that too many incorrect entries may cause the token or PIV to become locked. The number of incorrect entries may vary with the token provider.

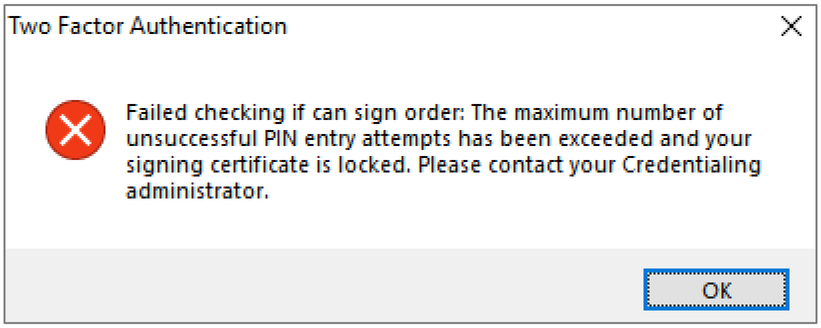


Subsequent incorrect PIN entries may lock your certificate and require the assistance of your credentialing administrator to unlock.

Figure 3-38: Second Factor Authentication dialog with warning for incorrect PIN

3.3.4.4 Token/PIV Locked

If the incorrect PIN is entered too many times for a token or PIV, regardless of whether the PIN is requested inside the EHR or outside of it, the token or PIV may become locked. The user will see a message similar to the one in Figure 3-39. To unlock a token, the user will need the unlock code provided during the certificate application process, and the ActivClient User Console, most likely available on the computers of the EPCS Provider Profile Admins at the site. See Section 2.9 for steps to unlock the token. To unlock a PIV, contact the IHS Help Desk.



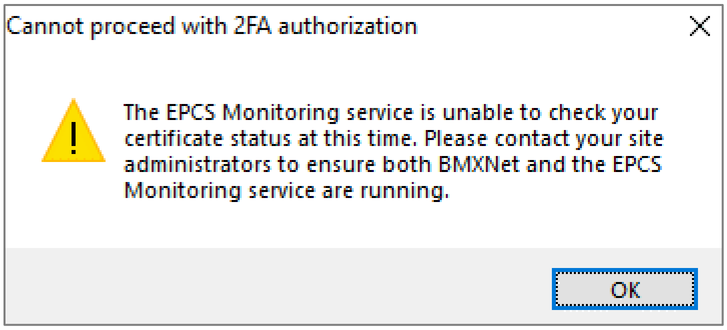
Failed checking if can sign order: The maximum number of unsuccessful PIN entry attempts has been exceeded and your signing certificate is locked. Please contact your Credentialing administrator.

Figure 3-39: Signing certificate is locked

3.3.4.5 Status Not Updated

This error occurs when the certificate status has not been updated in the last eight hours. The failure to update may occur when the EPCS Monitoring Service is not running, if the BMX listeners are not running, or if the user set up in the monitoring service cannot log in (such as when the verify code expires or the user is inactivated). Correcting the underlying issue will correct the error.

Note: Restarting the BMX listeners may also require the site to stop and restart the EPCS monitoring service to trigger an immediate update of the certificates.

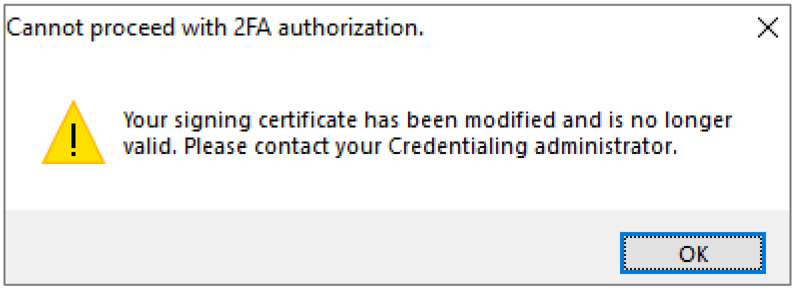

Cannot proceed with 2FA authorization

The EPCS Monitoring service is unable to check your certificate status at this time. Please contact your site administrators to ensure both BMXNet and the EPCS Monitoring service are running.

Figure 3-40: Signing certificate not updated recently

3.3.4.6 Thumbprint Mismatch

This error occurs when the thumbprint for the device does not match the token or PIV inserted. This is resolved by reassigning the certificate to the provider via the EPCS Credentialing component, then verifying the changes.

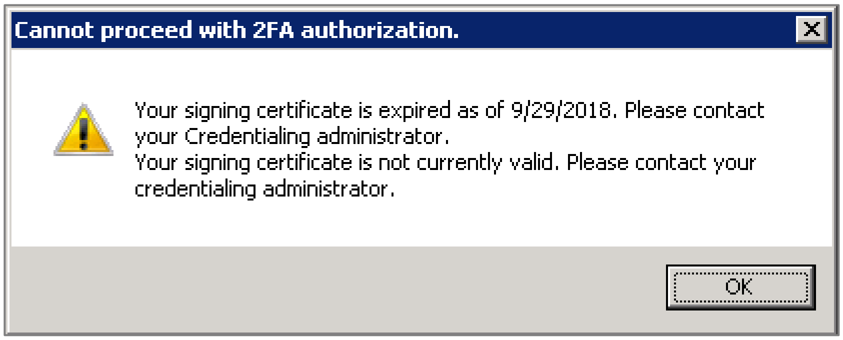

Cannot proceed with 2FA authorization.

Your signing certificate has been modified and is no longer valid. Please contact your Credentialing administrator.

Figure 3-41: The signing certificate has been modified and is no longer valid

3.3.4.7 Expired

This error occurs when the certificate has expired. It is resolved by renewing the certificate. Certificate holders may renew certificates prior to their expiration to avoid this error. For users with tokens, the renewed certificate must be loaded to the token using the process identified by the token issuer (see *bepc010o_EPCS_Token_Provisioning_Guide* for details). PIV certificates are loaded to the card through a different process as defined by IHS policy and procedure. In both cases, because the actual certificate is new, it must be associated with the user profile through the EPCS Credentialing component. The edited profile must be verified before the user can digitally sign with the new certificate.



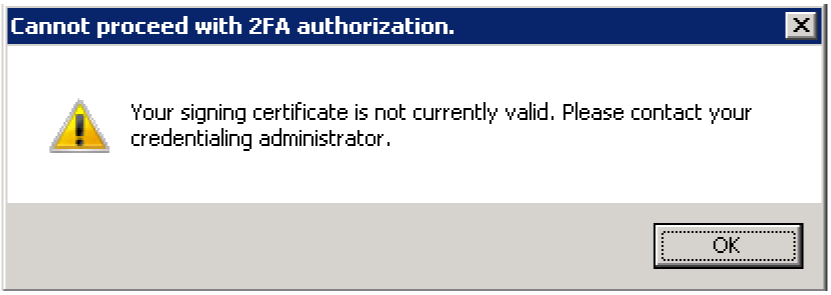
Cannot proceed with 2FA authorization.

Your signing certificate is expired as of 9/29/2018. Please contact your Credentialing administrator.
Your signing certificate is not currently valid. Please contact your credentialing administrator.

Figure 3-42: Signing certificate is expired

3.3.4.8 Not Marked as Valid

This error occurs when the status field in the BEH EPCS CERTIFICATE STATUS file is not set to “Valid.” This may occur when the certificate status has not been checked, or if the certificate has been revoked by the certificate issuing authority. It is resolved when the certificate status check returns a status of Valid. If the certificate has been revoked, the provider must obtain a new certificate according to the process outlined by the token issuer (see *bepc010o_EPCS_Token_Provisioning_Guide* for details), or through the IHS policy and procedure for PIV certificates. In both cases, if the certificate is renewed or re-issued, the new certificate must be loaded to the token or PIV and associated with the user profile through the EPCS Credentialing component. The edited profile must be verified before the user can digitally sign with the new certificate.



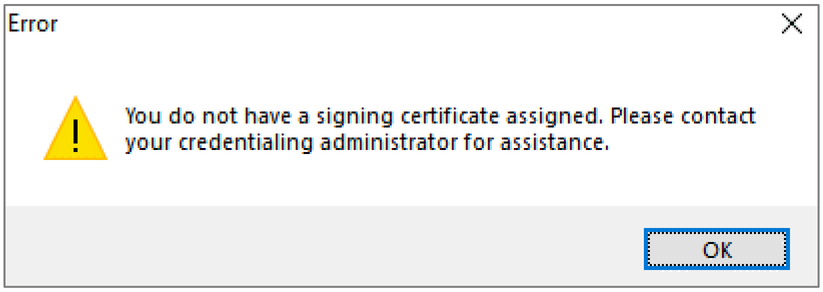
Cannot proceed with 2FA authorization.

Your signing certificate is not currently valid. Please contact your credentialing administrator.

Figure 3-43: Signing certificate is not currently valid

3.3.4.9 Certificate Not Assigned

This error occurs when the provider’s certificate is missing from the BEH EPCS CERTIFICATE STATUS file after having been assigned to the provider during credentialing. It is resolved by reassigning the certificate to the provider via the EPCS Credentialing component, then verifying the changes.



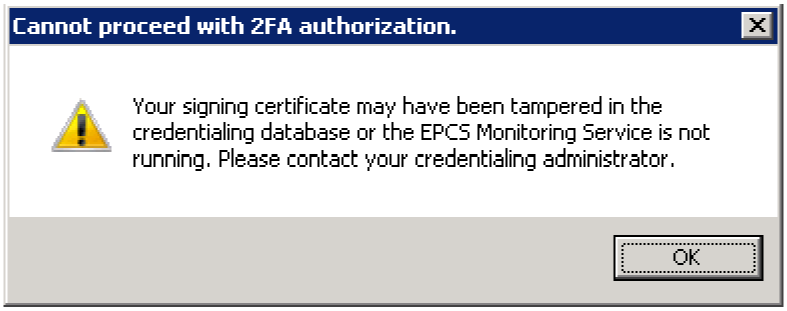
Error

You do not have a signing certificate assigned. Please contact your credentialing administrator for assistance.

Figure 3-44: The active user does not have a certificate assigned

3.3.4.10 Tampering/Monitoring Service Not Running

This error occurs when the certificate entry in the BEH EPCS CERTIFICATE STATUS file has been altered, or if the EPCS Monitoring service is not running. It may be resolved by restarting the monitoring service, or by reassigning the certificate to the provider via the EPCS Credentialing component, then verifying the changes. Users should only have the certificate reassigned if an investigation determines the alterations were not deliberate tampering of the certificate or file.



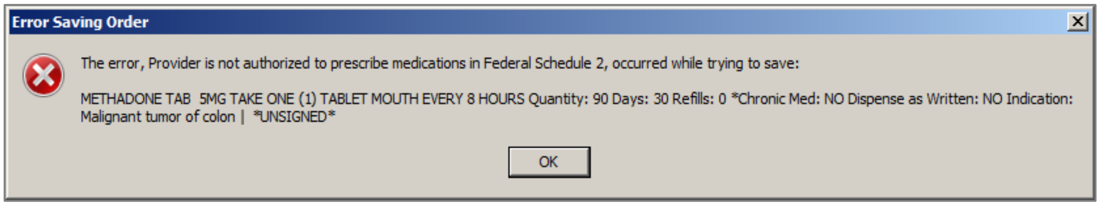
Cannot proceed with 2FA authorization.

Your signing certificate may have been tampered in the credentialing database or the EPCS Monitoring Service is not running. Please contact your credentialing administrator.

Figure 3-45: Signing certificate tampered or monitoring service not running

3.3.4.11 Unable to Sign Order

During the signing process, the same elements that were checked at the time the order was written are checked again. If the provider is not allowed to write the order, they will not be allowed to sign the order, either. The error messages are very similar to those seen when writing orders. These errors most often occur when the provider is attempting to sign orders that were written by another provider and does not have sufficient privileges for the medication being ordered. It may also occur if the provider’s privileges have changed between writing the order and signing the order.

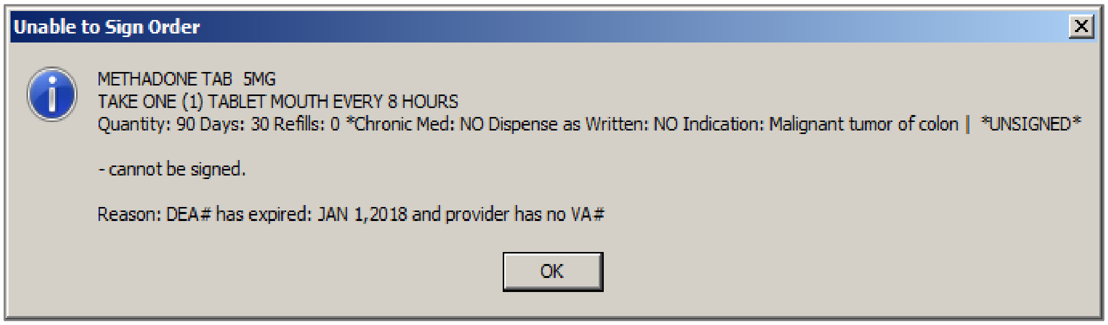


Error Saving Order

The error, Provider is not authorized to prescribe medications in Federal Schedule 2, occurred while trying to save:

METHADONE TAB 5MG TAKE ONE (1) TABLET MOUTH EVERY 8 HOURS Quantity: 90 Days: 30 Refills: 0 *Chronic Med: NO Dispense as Written: NO Indication: Malignant tumor of colon | *UNSIGNED*

Figure 3-46: Provider not authorized to prescribe schedule 2 orders



METHADONE TAB 5MG
TAKE ONE (1) TABLET MOUTH EVERY 8 HOURS
Quantity: 90 Days: 30 Refills: 0 *Chronic Med: NO Dispense as Written: NO Indication: Malignant tumor of colon | *UNSIGNED*

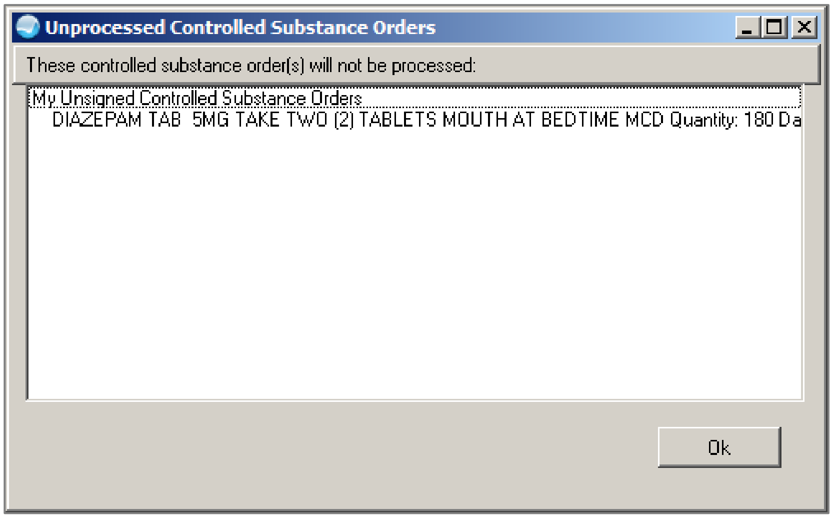
- cannot be signed.

Reason: DEA# has expired: JAN 1,2018 and provider has no VA#

Figure 3-47: Provider does not have a VA number and DEA is expired

3.3.4.12 Unprocessed Controlled Substance Order

If the provider chooses not to sign the order or it cannot be signed for any reason, a dialog will display to inform the provider that the order is unsigned.



These controlled substance order(s) will not be processed:

My Unsigned Controlled Substance Orders
DIAZEPAM TAB 5MG TAKE TWO (2) TABLETS MOUTH AT BEDTIME MCD Quantity: 180 Da

Figure 3-48: Unprocessed Controlled Substance Orders dialog

3.4 Printing an Order

A provider may need to print an order or copy for a variety of reasons. The RPMS-EHR system has several safeguards in place to prevent diversion and fraudulent orders. In general, printing an order will be the same as it was prior to the release of EPCS; however, there are a few additional safeguards and formats delivered with EPCS. A hardcopy, printed, signed-in-ink copy is required if the provider or site is not enabled for EPCS, or if the provider has access to and selects the **Force hardcopy** check box when signing. The provider may also print a copy when a Surescripts transmission has failed.

3.4.1 Print Formats

Several new print formats are delivered with the EPCS software, including:

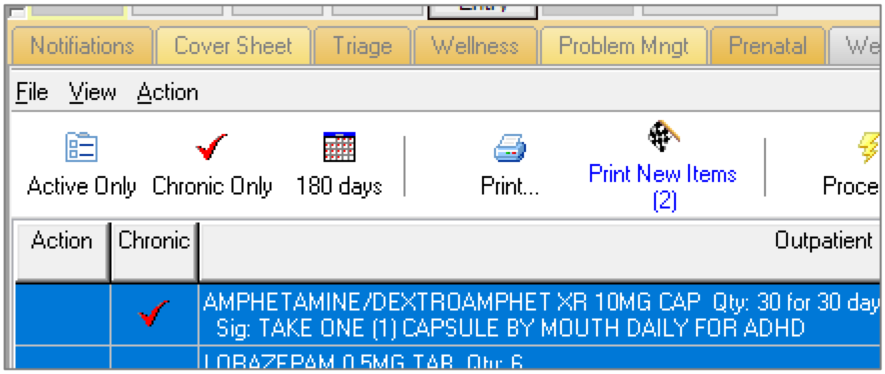
- Prescription CII EPCS
- Prescription CII EPCS SPVSR
- Prescription C3-5 EPCS
- Prescription C3-5 EPCS SPVSR
- Order for Signature CII EPCS
- Order for Signature CII EPCS SPVSR
- Order for Signature C3-5 EPCS
- Order for Signature C3-5 EPCS SPVSR

These formats are optimized for the EPCS rules and regulations. Sites who prefer to customize their formats should consider adjusting the EPCS formats, rather than trying to adjust current formats to include EPCS fields and requirements. The Reprint and DEA fields ***must*** be added to all formats per EPCS requirements. Other items, such as clinical indication (for detoxification and gamma-hydroxybutyrate (GHB) medications), Earliest Fill Date (CII only), and DEA X, are not removable per regulations and must be added to any existing formats if these types of order might be issued by providers at your site.

The formats labeled SPVSR are designed to include the supervisor information required by some states for certain providers such as mid-level providers. On these print formats, the Supervisor and Supervisor DEA number are also not removable per DEA regulations. Sites may set a parameter to identify those users requiring a supervisor (see *apsp0700.23o_EPCS_Supplemental_User_Guide* for more information). The Supervisor information comes from the Service/Section assigned to the user. For steps to set up these files, see Appendix C.

3.4.2 Print Queue

All CS orders requiring a hard copy, either for internal processing or to an external pharmacy, will show in the Print Queue regardless of site settings. The Print Queue otherwise functions as it did pre-EPCS. There are new print formats for EPCS, and sites should check the default formats and set them appropriately. See Section 3.4.1 for more information of the new print formats.

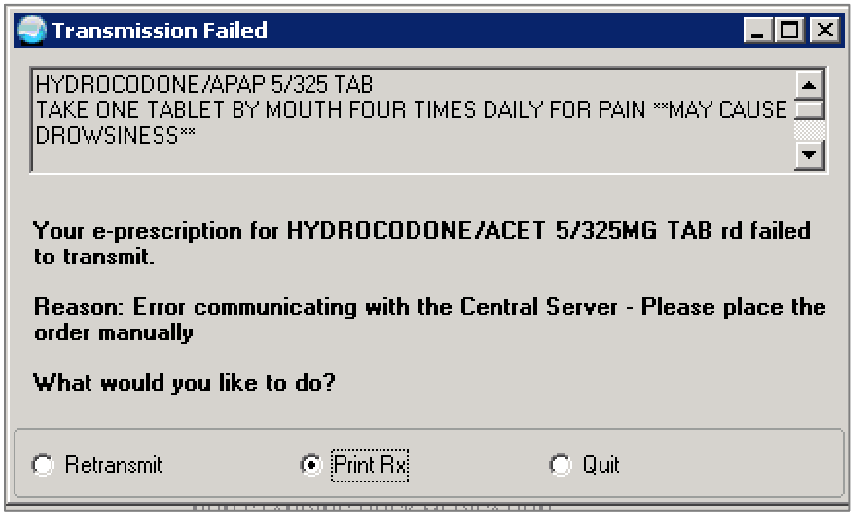


AMPHETAMINE/DEXTROAMPHET XR 10MG CAP Qty: 30 for 30 day
Sig: TAKE ONE (1) CAPSULE BY MOUTH DAILY FOR ADHD
LORAZEPAM 0.5MG TAB Qty: 6

Figure 3-49: The Print Queue shows 2 items awaiting action

3.4.3 Failed Transmission

When a Surescripts CS transmission fails, a notification will be sent to the provider in the same way providers currently receive them for Non-CS orders. Processing the Notification results in a dialog allowing the provider to choose to retransmit, print, or do nothing (quit).



HYDROCODONE/APAP 5/325 TAB
TAKE ONE TABLET BY MOUTH FOUR TIMES DAILY FOR PAIN **MAY CAUSE DROWSINESS**

Your e-prescription for HYDROCODONE/ACET 5/325MG TAB rd failed to transmit.

Reason: Error communicating with the Central Server - Please place the order manually

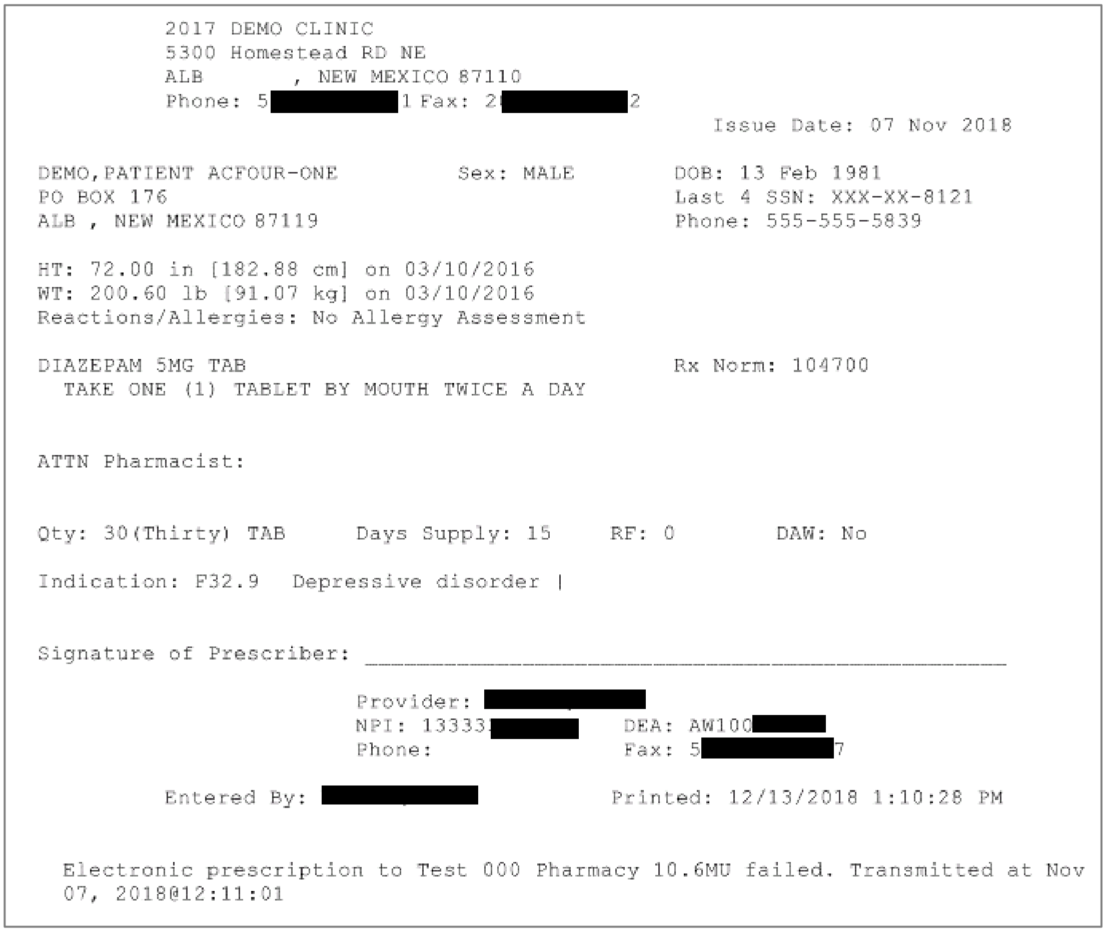
What would you like to do?

○ Retransmit ● Print Rx ○ Quit

Figure 3-50: Transmission Failed dialog for a Surescripts order

When **Print Rx** is selected, the prescription is printed, and the provider checks the information and manually signs the printed copy. When signing the printed copy, the provider should ensure that the printed copy contains the following information:

- Transmission Failed
- Target Pharmacy name
- Date and Time of the attempted transmission



```
          2017 DEMO CLINIC
          5300 Homestead RD NE
          ALB       , NEW MEXICO 87110
          Phone: 5[redacted]1 Fax: 2[redacted]2
                                                  Issue Date: 07 Nov 2018

DEMO,PATIENT ACFOUR-ONE         Sex: MALE        DOB: 13 Feb 1981
PO BOX 176                                       Last 4 SSN: XXX-XX-8121
ALB , NEW MEXICO 87119                           Phone: 555-555-5839

HT: 72.00 in [182.88 cm] on 03/10/2016
WT: 200.60 lb [91.07 kg] on 03/10/2016
Reactions/Allergies: No Allergy Assessment

DIAZEPAM 5MG TAB                                 Rx Norm: 104700
  TAKE ONE (1) TABLET BY MOUTH TWICE A DAY


ATTN Pharmacist:


Qty: 30(Thirty) TAB     Days Supply: 15    RF: 0       DAW: No

Indication: F32.9  Depressive disorder |


Signature of Prescriber: __________________________________________________

                        Provider: [redacted]
                        NPI: 13333[redacted]     DEA: AW100[redacted]
                        Phone:                    Fax: 5[redacted]7

          Entered By: [redacted]            Printed: 12/13/2018 1:10:28 PM


  Electronic prescription to Test 000 Pharmacy 10.6MU failed. Transmitted at Nov
  07, 2018@12:11:01
```

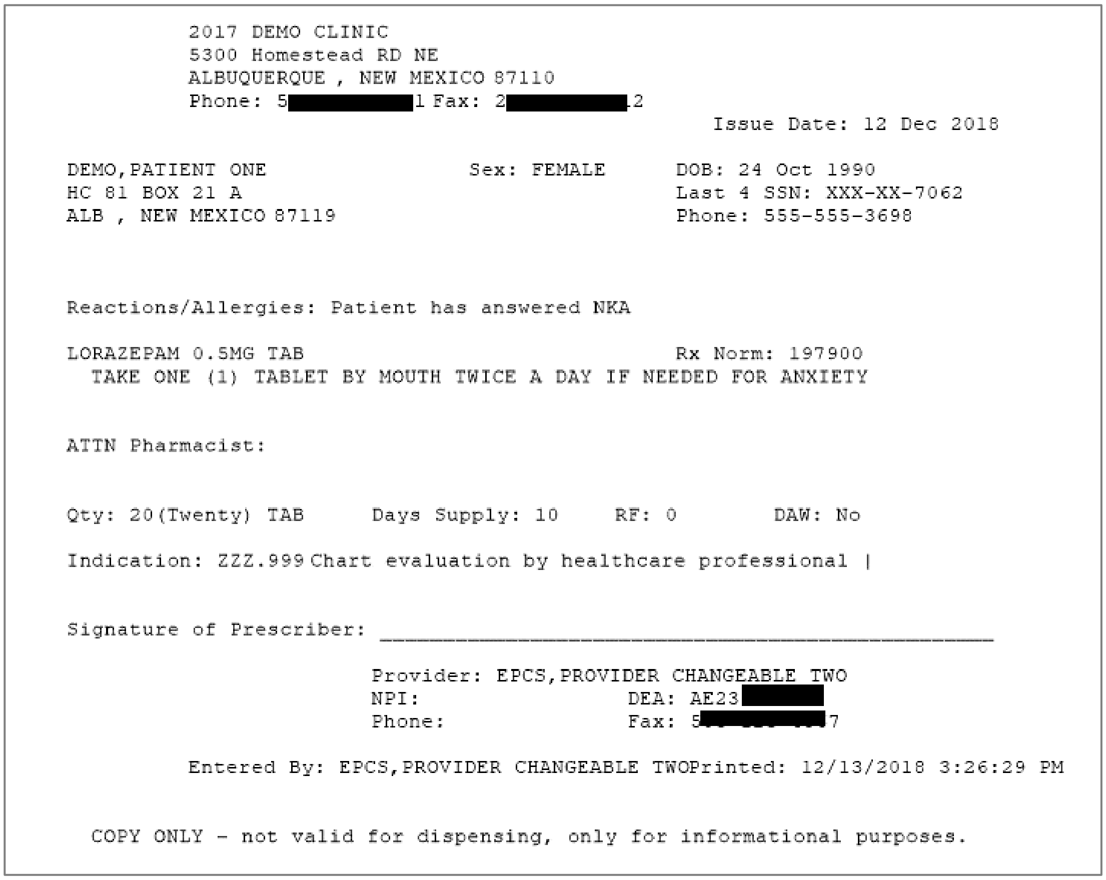
Figure 3-51: Failed Transmission printed for ink signature

3.4.4 Reprinting

The system has safeguards to track and identify orders and prescriptions that are reprinted to prevent diversion and fraudulent fillings.

3.4.4.1 Internal Pharmacy

Reprinting a digitally signed order transmitted to the internal pharmacy is no longer allowed. Reprinting a processed internal prescription is allowed but will show the **Copy Only** statement as shown in Figure 3-52. This statement may not be removed from a print template.

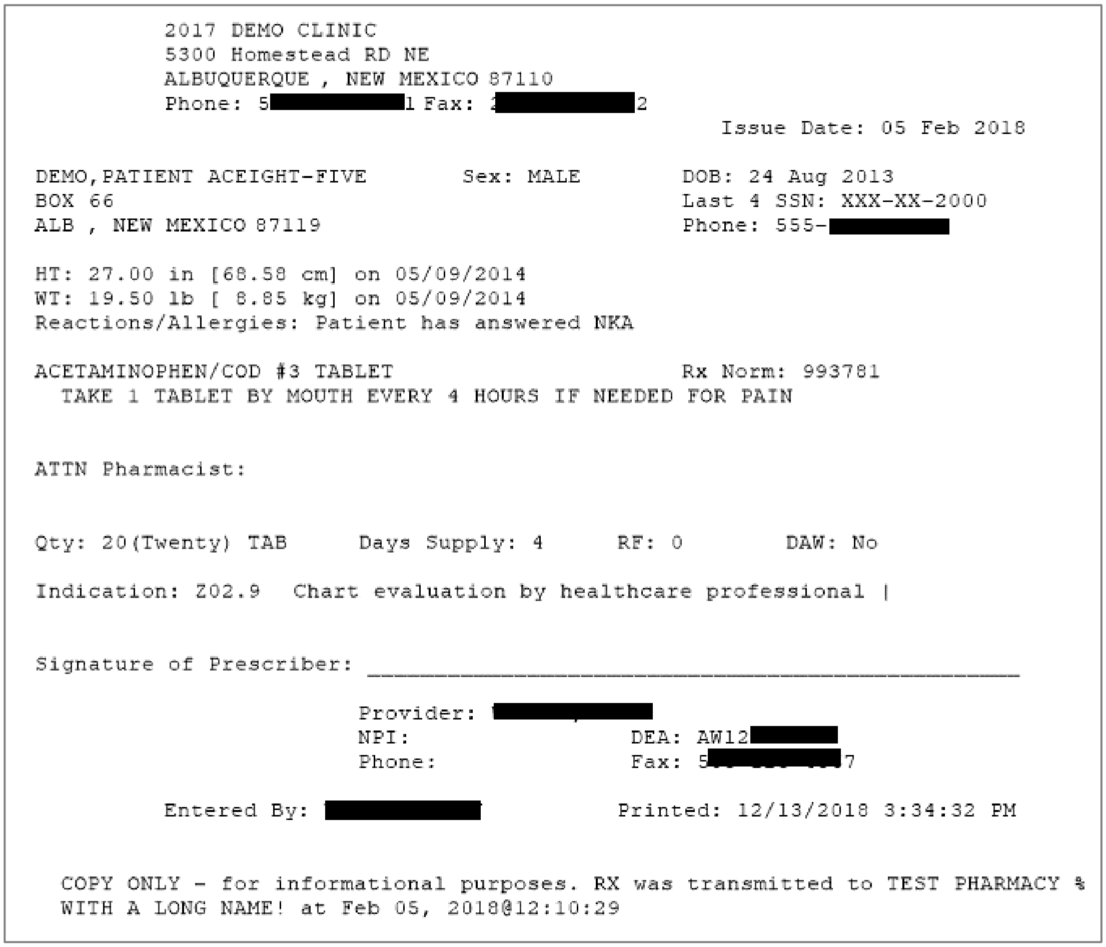


```
          2017 DEMO CLINIC
          5300 Homestead RD NE
          ALBUQUERQUE , NEW MEXICO 87110
          Phone: 5[redacted]1 Fax: 2[redacted]2
                                               Issue Date: 12 Dec 2018

DEMO,PATIENT ONE               Sex: FEMALE      DOB: 24 Oct 1990
HC 81 BOX 21 A                                  Last 4 SSN: XXX-XX-7062
ALB , NEW MEXICO 87119                          Phone: 555-555-3698


Reactions/Allergies: Patient has answered NKA

LORAZEPAM 0.5MG TAB                             Rx Norm: 197900
  TAKE ONE (1) TABLET BY MOUTH TWICE A DAY IF NEEDED FOR ANXIETY


ATTN Pharmacist:


Qty: 20(Twenty) TAB     Days Supply: 10    RF: 0       DAW: No

Indication: ZZZ.999 Chart evaluation by healthcare professional |


Signature of Prescriber: __________________________________________________

                         Provider: EPCS,PROVIDER CHANGEABLE TWO
                         NPI:                DEA: AE23[redacted]
                         Phone:              Fax: 5[redacted]7

          Entered By: EPCS,PROVIDER CHANGEABLE TWOPrinted: 12/13/2018 3:26:29 PM


  COPY ONLY - not valid for dispensing, only for informational purposes.
```

Figure 3-52: Reprint – internal pharmacy CS prescription

3.4.4.2 External Pharmacy

A print or reprint of a prescription successfully sent to Surescripts must state that is it a copy and is not intended for filling, along with the date/time of the transmission and where it was sent as shown in Figure 3-53. This statement may not be removed from a print template.

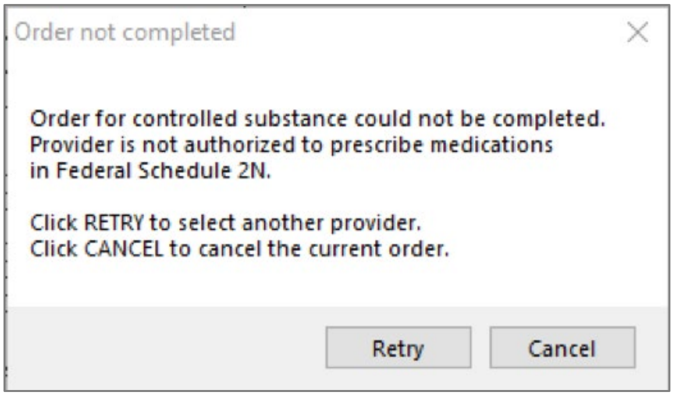


```
          2017 DEMO CLINIC
          5300 Homestead RD NE
          ALBUQUERQUE , NEW MEXICO 87110
          Phone: 5[redacted]1 Fax: [redacted]2
                                                  Issue Date: 05 Feb 2018

DEMO,PATIENT ACEIGHT-FIVE       Sex: MALE       DOB: 24 Aug 2013
BOX 66                                          Last 4 SSN: XXX-XX-2000
ALB , NEW MEXICO 87119                          Phone: 555-[redacted]

HT: 27.00 in [68.58 cm] on 05/09/2014
WT: 19.50 lb [ 8.85 kg] on 05/09/2014
Reactions/Allergies: Patient has answered NKA

ACETAMINOPHEN/COD #3 TABLET                     Rx Norm: 993781
  TAKE 1 TABLET BY MOUTH EVERY 4 HOURS IF NEEDED FOR PAIN


ATTN Pharmacist:


Qty: 20(Twenty) TAB     Days Supply: 4     RF: 0       DAW: No

Indication: Z02.9  Chart evaluation by healthcare professional |


Signature of Prescriber: __________________________________________________

                          Provider: [redacted]
                          NPI:                    DEA: AW12[redacted]
                          Phone:                  Fax: 5[redacted]7

          Entered By: [redacted]         Printed: 12/13/2018 3:34:32 PM


  COPY ONLY - for informational purposes. RX was transmitted to TEST PHARMACY %
  WITH A LONG NAME! at Feb 05, 2018@12:10:29
```

Figure 3-53: Print of an eRx prescription

3.5 Create an Inpatient Order

The basic method for creating an inpatient order for a CS medication has not changed, and EPCS does not apply to inpatient medications. However, there is now an internal check on the ordering provider's authorized schedules for inpatient medications. If the prescriber is not authorized for the scheduled drug being ordered, RPMS EHR will now provide an error message indicating that the prescriber is not authorized to order that schedule CS medication as shown in Figure 3-54.



Order for controlled substance could not be completed. Provider is not authorized to prescribe medications in Federal Schedule 2N.

Click RETRY to select another provider.
Click CANCEL to cancel the current order.

Figure 3-54: **Order not completed** warning for provider not authorized for schedule selected

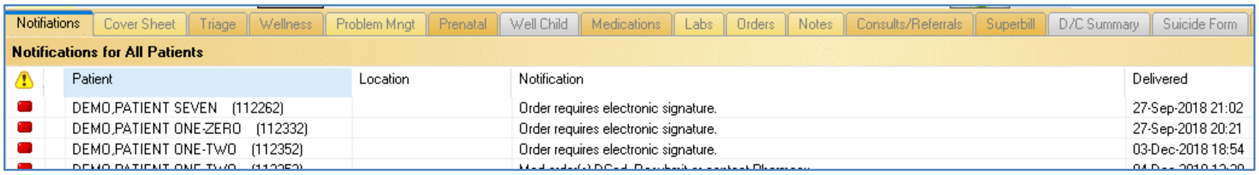
3.6 Notifications

The user may receive notifications regarding CS orders and the EPCS system. Some of these notifications are required and cannot be turned off by the user or any other personnel at the site. Other notifications are only received if the user is a member of a particular MailMan group.

The EPCS notifications for providers include the existing unsigned orders, and new monthly CS order reports and order discontinued.

3.6.1 Unsigned Order

This notification is not new but may become more common with EPCS if sites use scribes or ancillary personnel to enter orders on behalf of the provider. If an order for a CS medication is entered but not digitally signed by the provider, the provider will receive a notification indicating the order requires an electronic signature as illustrated in Figure 3-55. After the provider processes the medication order, this notification is automatically deleted from the Notifications screen.



Notifications for All Patients

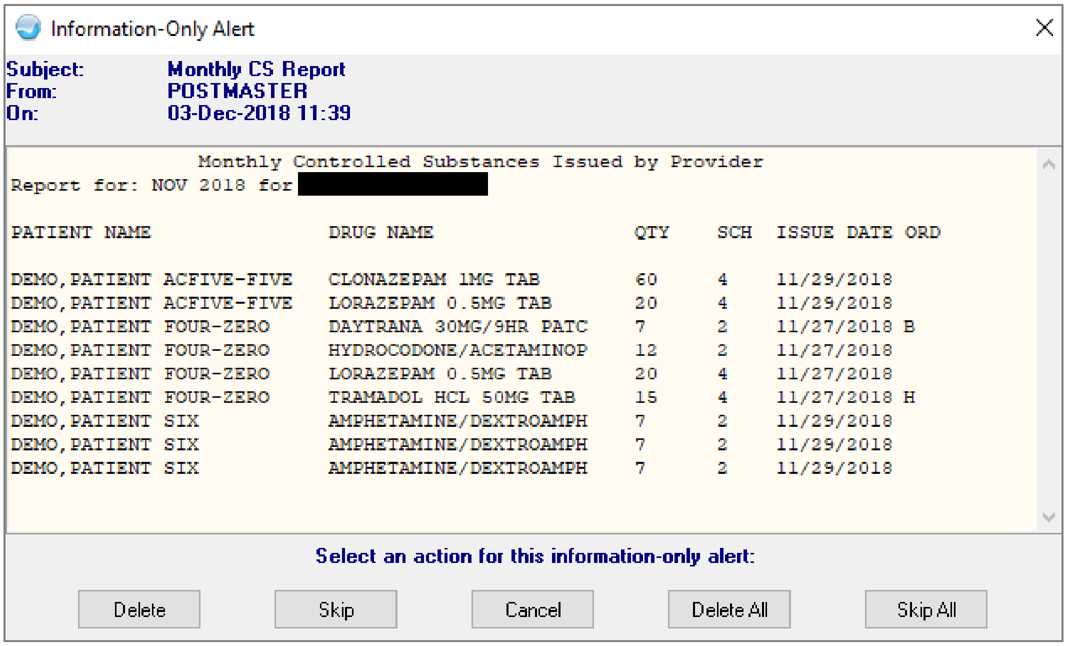
⚠	Patient	Location	Notification	Delivered
🟥	DEMO,PATIENT SEVEN (112262)		Order requires electronic signature.	27-Sep-2018 21:02
🟥	DEMO,PATIENT ONE-ZERO (112332)		Order requires electronic signature.	27-Sep-2018 20:21
🟥	DEMO,PATIENT ONE-TWO (112352)		Order requires electronic signature.	03-Dec-2018 18:54

Figure 3-55: Unsigned Order notification

3.6.2 Monthly CS Report

The required monthly CS Report is delivered to the provider as a notification. This report is generated automatically by the system when EPCS is properly set up. The report will contain all the orders written by the provider in the previous calendar month and will be delivered no later than seven (7) calendar days after the end of the previous month. If no CS medications were ordered by a provider during the previous calendar month, this report is not generated. This report may also be generated on demand for any date range. See *apsp0700.23o_EPCS_Supplemental_User_Guide* for details on running this report on demand.

The report contains the patient name, drug name, quantity, schedule, issue date, and an indication of an order that was not digitally signed. In this example, the **B** signifies that the order was entered directly in the pharmacy package as a “backdoor” order and the **H** signifies a hardcopy order.



Subject: Monthly CS Report
From: POSTMASTER
On: 03-Dec-2018 11:39

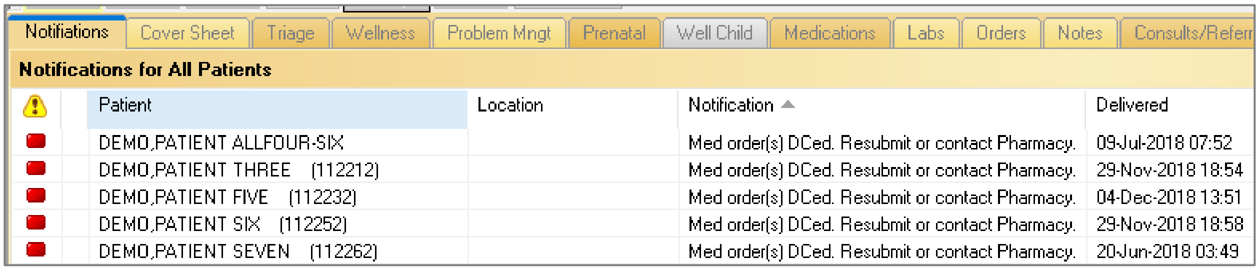
```
                Monthly Controlled Substances Issued by Provider
Report for: NOV 2018 for [redacted]

PATIENT NAME              DRUG NAME                 QTY    SCH  ISSUE DATE ORD

DEMO,PATIENT ACFIVE-FIVE  CLONAZEPAM 1MG TAB        60     4    11/29/2018
DEMO,PATIENT ACFIVE-FIVE  LORAZEPAM 0.5MG TAB       20     4    11/29/2018
DEMO,PATIENT FOUR-ZERO    DAYTRANA 30MG/9HR PATC    7      2    11/27/2018 B
DEMO,PATIENT FOUR-ZERO    HYDROCODONE/ACETAMINOP    12     2    11/27/2018
DEMO,PATIENT FOUR-ZERO    LORAZEPAM 0.5MG TAB       20     4    11/27/2018
DEMO,PATIENT FOUR-ZERO    TRAMADOL HCL 50MG TAB     15     4    11/27/2018 H
DEMO,PATIENT SIX          AMPHETAMINE/DEXTROAMPH    7      2    11/29/2018
DEMO,PATIENT SIX          AMPHETAMINE/DEXTROAMPH    7      2    11/29/2018
DEMO,PATIENT SIX          AMPHETAMINE/DEXTROAMPH    7      2    11/29/2018
```

Select an action for this information-only alert:

Figure 3-56: Monthly CS Report Notification

3.6.3 Med Order Discontinued

While anticipated to be rare, an order may be automatically discontinued if the order hash does not match when it arrives in the pharmacy for processing. This may occur by deliberate tampering or by accidental corruption in transmission. When this occurs, a notification is sent to the ordering provider and to the local EPCS incident response team. The provider notification is actionable, allowing the provider to reorder the medication if desired.



Notifications for All Patients

⚠		Patient	Location	Notification	Delivered
🟥		DEMO,PATIENT ALLFOUR-SIX		Med order(s) DCed. Resubmit or contact Pharmacy.	09-Jul-2018 07:52
🟥		DEMO,PATIENT THREE (112212)		Med order(s) DCed. Resubmit or contact Pharmacy.	29-Nov-2018 18:54
🟥		DEMO,PATIENT FIVE (112232)		Med order(s) DCed. Resubmit or contact Pharmacy.	04-Dec-2018 13:51
🟥		DEMO,PATIENT SIX (112252)		Med order(s) DCed. Resubmit or contact Pharmacy.	29-Nov-2018 18:58
🟥		DEMO,PATIENT SEVEN (112262)		Med order(s) DCed. Resubmit or contact Pharmacy.	20-Jun-2018 03:49

Figure 3-57: Med orders discontinued notifications

Appendix A: EPCS Troubleshooting

This section contains a partial listing of the various error messages or blocking situations a user may encounter when attempting to verify a provider profile or create and sign a CS order. The list is not all-inclusive.

A.1 Ordering

A.1.1 Message: “Electronic Prescribing for Controlled Substances (EPCS) is not currently enabled for you. You will be required to print and sign hardcopy Controlled Substance prescriptions.”

Causes:

- The user is not enabled for EPCS.
- The Division that the user is logged into is not enabled for EPCS.
- The hash check for the provider profile has failed. Note that the message window title will be different from the above reasons, though the message text will be the same.

Resolutions:

- Credential the user for EPCS.
- Turn on the Division for EPCS.
- Investigate the hash mismatch, and if authorized to do so, re-credential the provider.

A.1.2 Message: “Order for controlled substance could not be completed. Provider is not authorized to prescribe medications in Federal Schedule <schedule number>.”

Cause:

- The provider’s profile does not have the listed schedule authorized.

Resolution:

- Set up the provider in the EPCS Credentialing component to order the appropriate schedules based on their DEA licensure, and verify the changes.

A.1.3 Message: “Order for controlled substance could not be completed. Provider does not have a current, valid DEA# on record and is ineligible to sign the order.

Cause:

- The provider does not have a valid DEA or VA number assigned.

Resolution:

- Add the provider’s DEA# (if present) or VA# (if provider is eligible to prescribe under the institutional DEA) to the provider profile and verify the changes.

A.1.4 Message: “Order for controlled substance could not be completed. Provider’s DEA# expired <date> and no VA# is assigned. Provider is ineligible to sign the order.

Cause:

- The provider has a DEA assigned but the expiration date is in the past, and the provider does not have a VA# assigned.

Resolution:

- Update the provider’s DEA# expiration date (if present and appropriately renewed) or VA# (if provider is eligible to prescribe under the institutional DEA) to the provider profile and verify the changes.

A.1.5 Situation: eRx button grayed out

Causes:

- The division/site where the provider is ordering the medication is not EPCS enabled.
- The provider is not EPCS enabled and credentialed.
- The provider does not have a valid SPI number.

> **Note**: The site may set the parameter APSP AUTO RX ELECTRONIC to allow the button to show, but without a valid SPI number the prescription will be rejected by Surescripts.

- The site is not approved to send controlled substances to Surescripts.
- The provider is not enabled for CS medications on the Surescripts side.

- The Surescripts parameters (APSP AUTO RX, APSP AUTO RX SCHEDULE RESTRICT, APSP AUTO RX ERX OF CS II) are not set to allow sending of controlled substances externally.

Resolutions:

- Correct the underlying defect. Note that eRx deployment and approval for transmission of CS medications is not automatic with install of EPCS patches.

A.2 Digital Signing

A.2.1 Message: “Your signing certificate's status has not updated recently and cannot be validated.”

Cause:

- The signing certificate has not been validated within the last eight hours.

Resolutions:

- Check that the BMX Listener is running
  - BMXMENU > VIEW to see status
  - BMXMENU > STRT to start
- Stop/restart EPCS Monitoring Service
  - net stop "BEH EPCS Monitoring Service" then
  - net start "BEH EPCS Monitoring Service"

A.2.2 Message: “Your signing certificate is not currently valid.”

Causes:

- The certificate is revoked.
- The user is newly credentialed and the certificate was not validated yet.

Resolutions:

- The provider works with appropriate vendor to get a new certificate.
- Ensure that the BMX Listener is running:
  - BMXMENU > VIEW to see status
  - BMXMENU > STRT to start
- Stop/restart the EPCS Monitoring Service
  - net stop "BEH EPCS Monitoring Service" and then
  - net start "BEH EPCS Monitoring Service"

A.2.3 Message: “Your signing certificate could not be located. Please insert the device containing your signing certificate and try again.”

Causes:

- The token or PIV has never been inserted in the computer being used to digitally sign.
- The driver for the token or card reader has not been installed on the computer being used to digitally sign.

Resolutions:

- Plug token/PIV into the computer and attempt to sign again.
- Install the appropriate drivers on the computer.

A.2.4 Message: “The maximum number of unsuccessful PIN entry attempts has been exceeded and your signing certificate is locked.”

Cause:

- The user has entered the PIN incorrectly too many times. Note that this is cumulative for all uses of the token or PIV and may not have occurred strictly from use with EPCS functions.

Resolutions:

- Process depends on if the locked device is a PIV or a token:
  - If PIV, contact IHS Help Desk about unlocking/resetting PIV card.
  - If token, follow vendor instructions for unlocking device. See section 2.9 for details.

A.2.5 Message: “The device containing the certificate was removed before validation could complete.”

Causes:

- The device was physically removed.
- Windows reset the driver after the process of checking the PIN started and before it completed.

Resolution:

- Plug the token/PIV back in (or unplug and replug) and attempt to sign again.

A.2.6 Message: “There was a problem locating your signing certificate. Please remove your signing token/smart card, re-insert it, and try again.”

Cause:

- The certificate is present in the Windows Certificate Store, but the hardware device containing your certificate is not present.

Resolution:

- Remove the token/PIV, plug the token/PIV back in, and attempt to sign again.

A.2.7 Message: “Your signing certificate has been modified and is no longer valid.”

Cause:

- The certificate has been modified (meaning the thumbprint has been changed). This should not happen unless someone is intentionally tampering with their certificate, e.g. to change expiration date.

Resolution:

- Investigate the situation. If the modification is determined not to be intentional tampering, the certificate can be re-associated with the user’s profile and the changes verified.

A.2.8 Message: “Your signing certificate will not become active until {Date cert becomes active}.”

Cause:

- The certificate has been post-dated by the issuing certificate authority. This should not happen as the certificate authorities should not post-date certificates.

Resolutions:

- Contact issuing organization and get a non-post-dated certificate.
- Wait until the date specified.

A.2.9 Message: “Your signing certificate is expired as of {Date cert expired}.”

Cause:

- The signing certificate has expired.

Resolution:

- Obtain a new signing certificate from the issuing organization (e.g., IHS or IdenTrust), update the certificate assigned to the provider profile, and verify the changes.

A.2.10 Message: “You do not have a certificate assigned. Please contact your credentialing administrator for assistance.”

Cause:

- The user has not had their signing certificate assigned to their EPCS profile.

Resolution:

- Add the user’s signing certificate to their EPCS profile and verify the changes.

Appendix B: EHR Configuration

For complete EPCS system configuration information, please see the EPCS Configuration Guide. This section gives an overview of the set-up of the EHR component only.

The EPCS system utilizes an EHR component for the credentialing process. The component must be added to an EHR GUI Template in order for users to access the component. However, best practice is that the new EPCS Credentialing component should ***not*** be available on all EHR templates. A new template may be created for those who will be credentialing providers and are given the keys to perform these functions. The principle of least access suggests regular providers should not have access to this component unless their job duties require it. Likewise, a Provider Profile user should not have access to the patient care portions of the EHR unless their job duties require it.

To add the component to an EHR template, a user with access to design mode should perform the following steps:

1. Log into the EHR and select or create an appropriate template for the EPCS Provider Profile users.

2. If not already in design mode, right-click on the title bar and select **Design Mode** from the contextual menu. Alternately, press Control-Alt-D to enter design mode.

3. Select a location for the component. It should ***not*** be part of the patient chart/patient care areas of the EHR template if such items are present. In the example shown in Figure B-1 for an EHR GUI utilizing tabs, a new tab was created on the main portion of the EHR GUI Template. For sites using templates with Group Bars or Tree Views, add the object to an appropriate location outside the patient care portions of the EHR template.

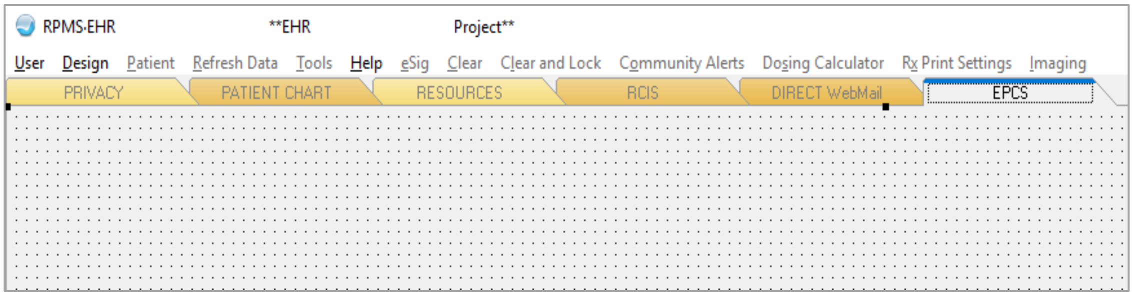


Figure B-1: EHR tab created for EPCS Credentialing component, currently empty

4. Right-click in the new tab and select **Add Object** as shown in Figure B-2.

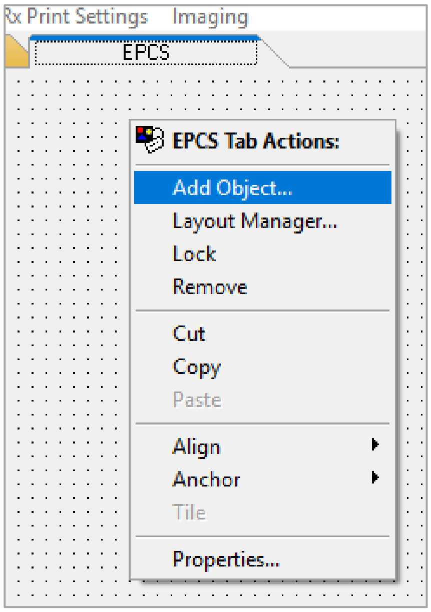


Figure B-2: Context menu in design mode

5. In the resulting pop-up dialog, open the Name folder and select the **EPCS Credentialing** component, then click **Add**.

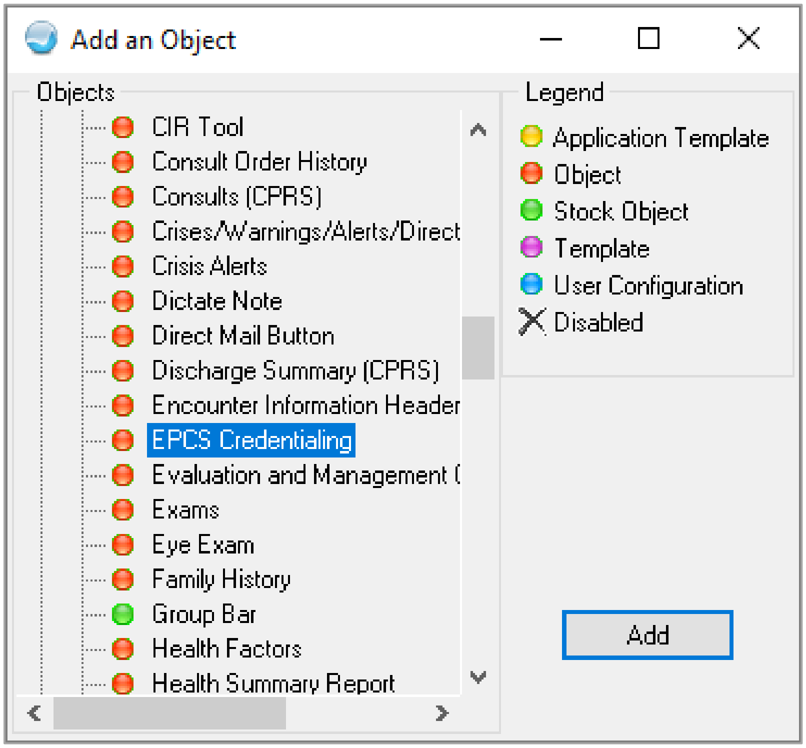


Figure B-3: Selecting EPCS Credentialing component

6. By default, the component will be added in a small size. Double-click on the component to expand it to fit the full tab area.

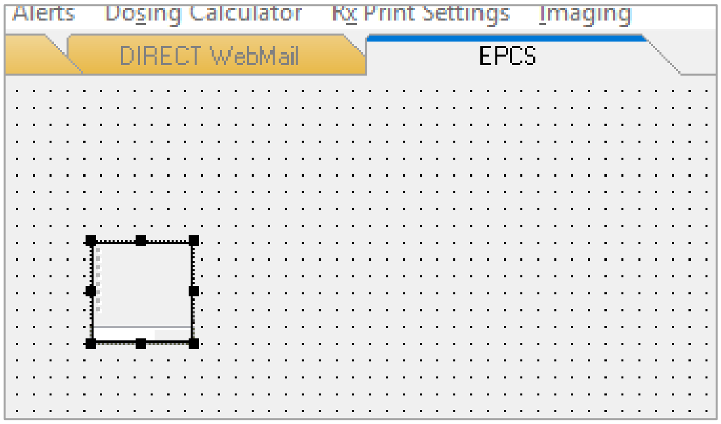


Figure B-4: Component added in small size

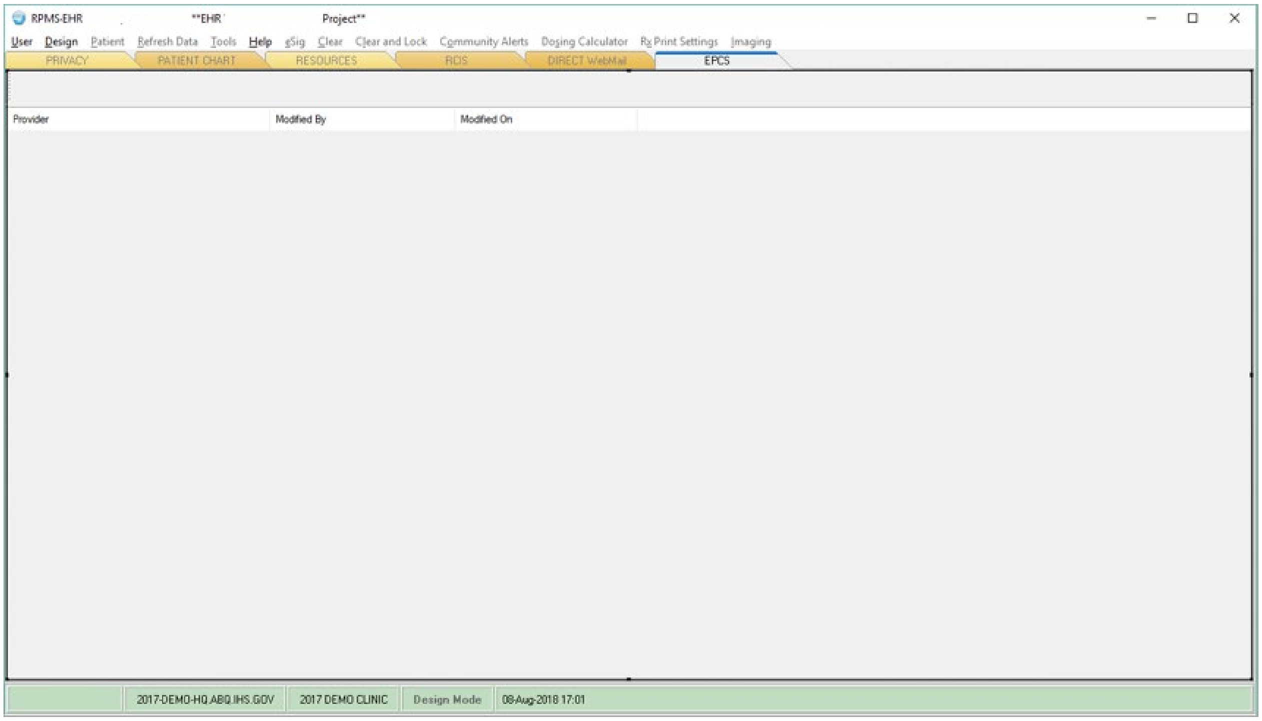


Figure B-5: Component expanded after double-clicking on it

7. Click the **Design** menu option and select **Save as Template**.

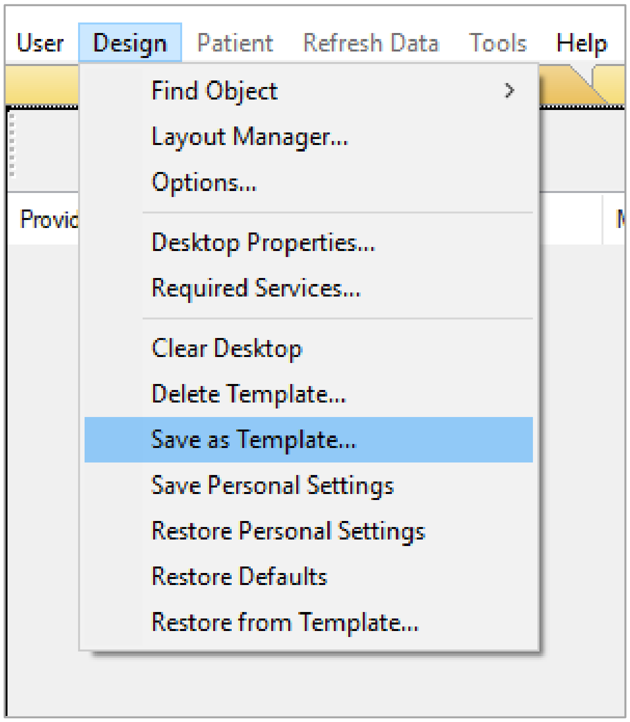
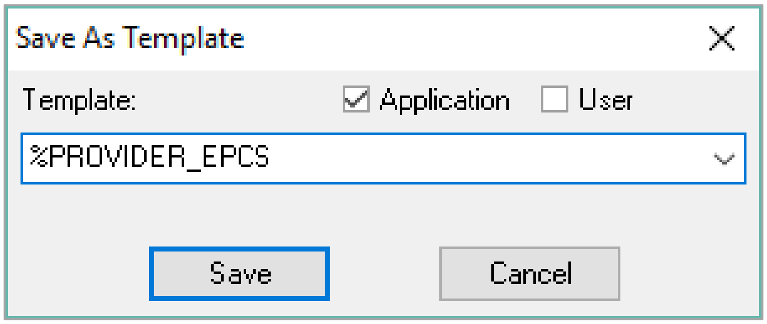


Figure B-6: Design menu, Save as Template

8. In the resulting pop-up dialog, name the template as desired, ensure that **Application** is checked, and then click **Save**. The template will be saved and can be assigned to users as normal. Remember that users will not see the new component until the template has been assigned to the appropriate personnel (if a new template is created).


Save As Template

Template: ☑ Application □ User

%PROVIDER_EPCS

Figure B-7: Save As Template dialog

Appendix C: Setting Up a Supervisor

C.1 Setting Up the SERVICE/SECTION File

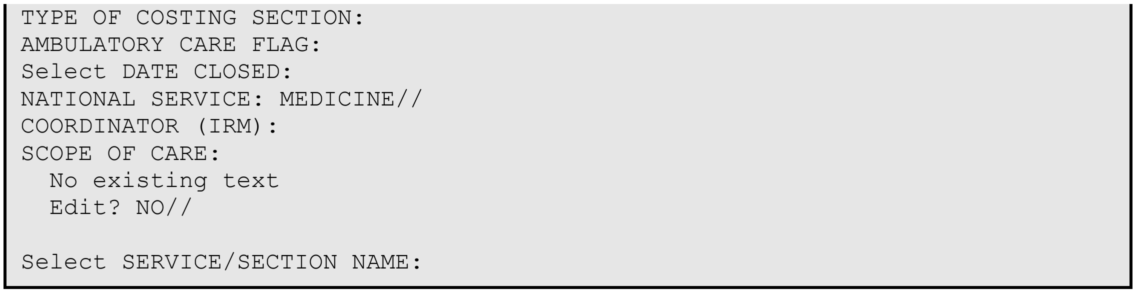
When setting up a new user, the user is assigned a Service/Section. The SERVICE/SECTION file (#49) was historically not well set up within IHS facilities, but it has become more useful with the release of the RPMS-EHR. For EPCS, it is where the supervisor information will be pulled when a user is required to have medical supervisor information on a CS medication order. It is therefore also important that this file be reviewed regularly and maintained appropriately as personnel changes occur.

Sites may use a single Service/Section for all providers requiring a medical supervisor or may set up specialized entries for more complex configurations. For example, if a site has three mid-level providers who are all supervised by the same person, a single Service/Section may be used for all three. However, if the three mid-level providers are each supervised by a different provider, the site may wish to set up individual Service/Section entries for each mid-level provider.

The **CHIEF** field should hold the person who is the medical supervisor of the user. This field is a pointer to the NEW PERSON file, so must be filled with a user currently set up in the RPMS system.

The file is usually edited from the FileMan menu. This file should only be edited by a user with the appropriate permissions and knowledge. An example of editing this file is shown in Figure C-1.

```
Select VA FileMan <TEST ACCOUNT> Option: ENTER or Edit File Entries

INPUT TO WHAT FILE: DRUG// 49  SERVICE/SECTION  (6 entries)
EDIT WHICH FIELD: ALL//

Select SERVICE/SECTION NAME: MEDICINE       MED
NAME: MEDICINE//
ABBREVIATION: MED//
DESCRIPTION:
  No existing text
  Edit? NO//
MAIL SYMBOL:
PARENT SERVICE:
TYPE OF SERVICE: PATIENT CARE//
CHIEF: EPCS,EDS
     1   EPCS,PROVIDER EDSCII-V       PE
     2   EPCS,PROVIDER EDSCIII-V       PE
     3   EPCS,PROVIDER EDSCIV-V       PE
CHOOSE 1-3: 1  EPCS,PROVIDER EDSCII-V     PE
Select CHIEF PHONE:
ASST CHIEF:
Select ASST CHIEF PHONE:
LOCATION:
MIS COSTING CODE:
COST CENTER:
```



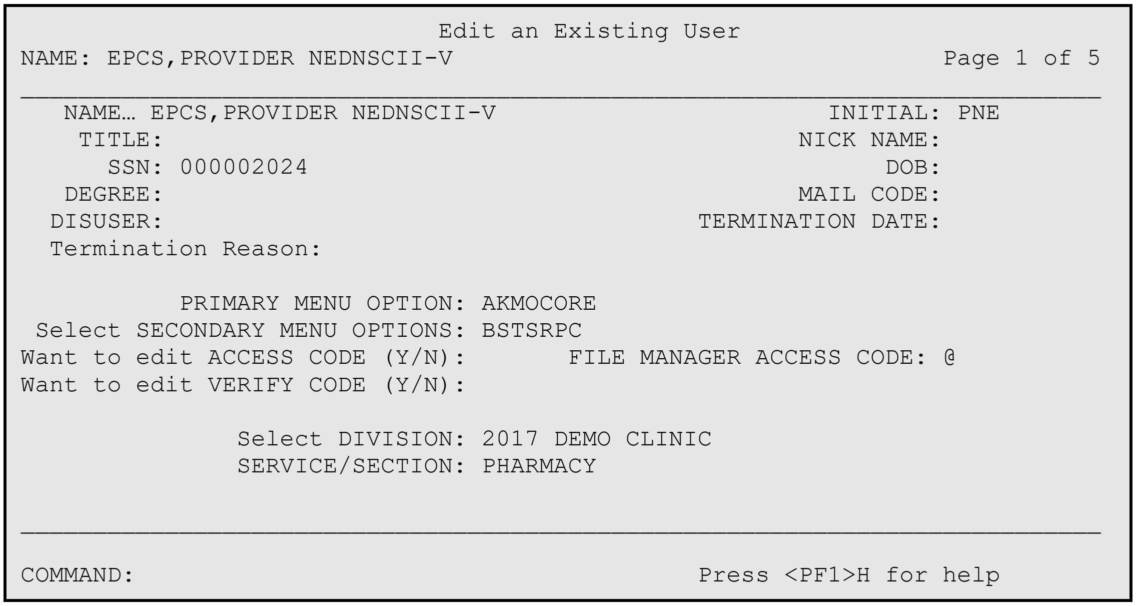
```
TYPE OF COSTING SECTION:
AMBULATORY CARE FLAG:
Select DATE CLOSED:
NATIONAL SERVICE: MEDICINE//
COORDINATOR (IRM):
SCOPE OF CARE:
  No existing text
  Edit? NO//

Select SERVICE/SECTION NAME:
```

Figure C-1: Editing the Service/Section file

C.2 Assigning a Service/Section to a User

When the SERVICE/SECTION file is set up, the Service/Section may be assigned to a user. This may be changed by editing an existing user in the User Management options. An example of this is shown in the following figures:

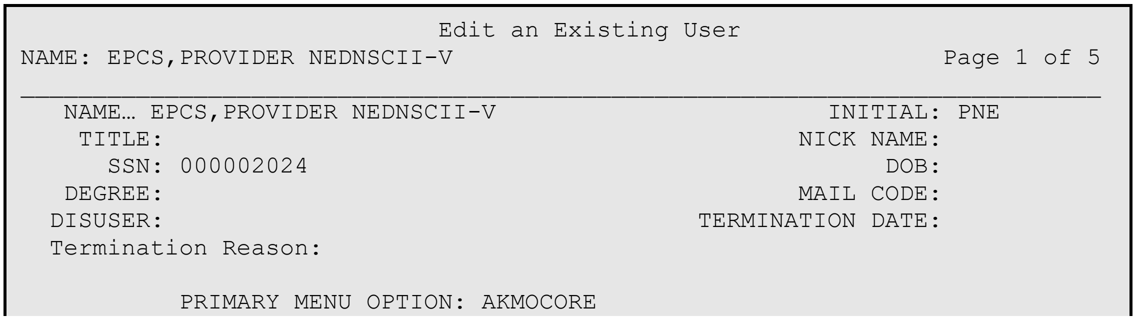
Before editing:



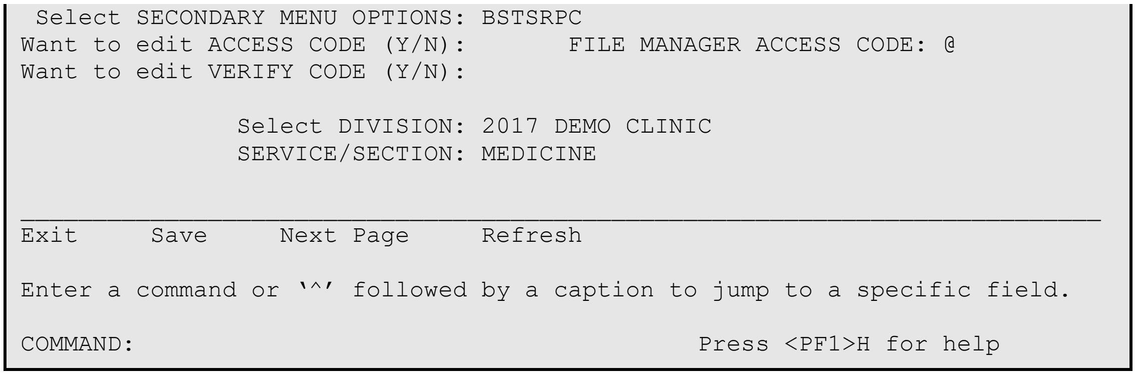
```
                             Edit an Existing User
NAME: EPCS,PROVIDER NEDNSCII-V                                  Page 1 of 5
___________________________________________________________________________
   NAME… EPCS,PROVIDER NEDNSCII-V                           INITIAL: PNE
    TITLE:                                                NICK NAME:
      SSN: 000002024                                            DOB:
   DEGREE:                                                MAIL CODE:
  DISUSER:                                         TERMINATION DATE:
  Termination Reason:

           PRIMARY MENU OPTION: AKMOCORE
 Select SECONDARY MENU OPTIONS: BSTSRPC
Want to edit ACCESS CODE (Y/N):       FILE MANAGER ACCESS CODE: @
Want to edit VERIFY CODE (Y/N):

               Select DIVISION: 2017 DEMO CLINIC
               SERVICE/SECTION: PHARMACY


___________________________________________________________________________

COMMAND:                                       Press <PF1>H for help
```

Figure C-2: Edit an Existing User showing Service/Section

After editing:



```
                             Edit an Existing User
NAME: EPCS,PROVIDER NEDNSCII-V                                  Page 1 of 5
___________________________________________________________________________
   NAME… EPCS,PROVIDER NEDNSCII-V                           INITIAL: PNE
    TITLE:                                                NICK NAME:
      SSN: 000002024                                            DOB:
   DEGREE:                                                MAIL CODE:
  DISUSER:                                         TERMINATION DATE:
  Termination Reason:

           PRIMARY MENU OPTION: AKMOCORE
```



```
 Select SECONDARY MENU OPTIONS: BSTSRPC
Want to edit ACCESS CODE (Y/N):       FILE MANAGER ACCESS CODE: @
Want to edit VERIFY CODE (Y/N):

               Select DIVISION: 2017 DEMO CLINIC
               SERVICE/SECTION: MEDICINE

___________________________________________________________________________
Exit     Save     Next Page     Refresh

Enter a command or '^' followed by a caption to jump to a specific field.

COMMAND:                                       Press <PF1>H for help
```

Figure C-3: Edit an Existing User with the Service/Section changed

Appendix D: Practitioner Responsibilities

The EPCS regulations specify the Practitioner responsibilities in sections 1311.102, 1311.125, 1311.130, 1311.150, and 1311.305. The relevant text of each of these sections follows:

§1311.102 Practitioner responsibilities:

(a) The practitioner must retain sole possession of the hard token, where applicable, and must not share the password or other knowledge factor, or biometric information, 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. Failure by the practitioner to secure the hard token, knowledge factor, or biometric information may provide a basis for revocation or suspension of registration pursuant to section 304(a)(4) of the Act (21 U.S.C. 824(a)(4)).

(b) The practitioner must notify the individuals designated under Section 1311.125 or Section 1311.130 within one business day of discovery that the hard token has been lost, stolen, or compromised or the authentication protocol has been otherwise compromised. A practitioner who fails to comply with this provision may be held responsible for any controlled substance prescriptions written using his two-factor authentication credential.

(c) If the practitioner is notified by an intermediary or pharmacy that an electronic prescription was not successfully delivered, as provided in Section 1311.170, he must ensure that any paper or oral prescription (where permitted) issued as a replacement of the original electronic prescription indicates that the prescription was originally transmitted electronically to a particular pharmacy and that the transmission failed.

(d) Before initially using an electronic prescription application to sign and transmit controlled substance prescriptions, the practitioner must determine that the third-party auditor or certification organization has found that the electronic prescription application records, stores, and transmits the following accurately and consistently:

(1) The information required for a prescription under Section 1306.05(a) of this chapter.

(2) The indication of signing as required by Section 1311.120(b)(17) or the digital signature created by the practitioner's private key.

(3) The number of refills as required by Section 1306.22 of this chapter.

(e) If the third-party auditor or certification organization has found that an electronic prescription application does not accurately and consistently record, store, and transmit other information required for prescriptions under this chapter, the practitioner must not create, sign, and transmit electronic prescriptions for controlled substances that are subject to the additional information requirements.

(f) The practitioner must not use the electronic prescription application to sign and transmit electronic controlled substance prescriptions if any of the functions of the application required by this subpart have been disabled or appear to be functioning improperly.

(g) If an electronic prescription application provider notifies an individual practitioner that a third-party audit or certification report indicates that the application or the application provider no longer meets the requirements of this part or notifies him that the application provider has identified an issue that makes the application non-compliant, the practitioner must do the following:

(1) Immediately cease to issue electronic controlled substance prescriptions using the application.

(2) Ensure, for an installed electronic prescription application at an individual practitioner's practice, that the individuals designated under Section 1311.125 terminate access for signing controlled substance prescriptions.

(h) If an electronic prescription application provider notifies an institutional practitioner that a third-party audit or certification report indicates that the application or the application provider no longer meets the requirements of this part or notifies it that the application provider has identified an issue that makes the application non-compliant, the institutional practitioner must ensure that the individuals designated under Section 1311.130 terminate access for signing controlled substance prescriptions.

(i) An individual practitioner or institutional practitioner that receives a notification that the electronic prescription application is not in compliance with the requirements of this part must not use the application to issue electronic controlled substance prescriptions until it is notified that the application is again compliant and all relevant updates to the application have been installed.

(j) The practitioner must notify both the individuals designated under Section 1311.125 or Section 1311.130 and the Administration within one business day of discovery that one or more prescriptions that were issued under a DEA registration held by that practitioner were prescriptions the practitioner had not signed or were not consistent with the prescriptions he signed.

(k) The practitioner has the same responsibilities when issuing prescriptions for controlled substances via electronic means as when issuing a paper or oral prescription. Nothing in this subpart relieves a practitioner of his responsibility to dispense controlled substances only for a legitimate medical purpose while acting in the usual course of his professional practice. If an agent enters information at the practitioner's direction prior to the practitioner reviewing and approving the information and signing and authorizing the transmission of that information, the practitioner is responsible in case the prescription does not conform in all essential respects to the law and regulations.

§1311.125 Requirements for establishing logical access control—Individual practitioner:

(a) At each registered location where one or more individual practitioners wish to use an electronic prescription application meeting the requirements of this subpart to issue controlled substance prescriptions, the registrant(s) must designate at least two individuals to manage access control to the application. At least one of the designated individuals must be a registrant who is authorized to issue controlled substance prescriptions and who has obtained a two-factor authentication credential as provided in Section 1311.105.

(b) At least one of the individuals designated under paragraph (a) of this section must verify that the DEA registration and State authorization(s) to practice and, where applicable, State authorization(s) to dispense controlled substances of each registrant being granted permission to sign electronic prescriptions for controlled substances are current and in good standing.

(c) After one individual designated under paragraph (a) of this section enters data that grants permission for individual practitioners to have access to the prescription functions that indicate readiness for signature and signing or revokes such authorization, a second individual designated under paragraph (a) of this section must use his two-factor authentication credential to satisfy the logical access controls. The second individual must be a DEA registrant.

(d) A registrant's permission to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions must be revoked whenever any of the following occurs, on the date the occurrence is discovered:

(1) A hard token or any other authentication factor required by the two-factor authentication protocol is lost, stolen, or compromised. Such access must be terminated immediately upon receiving notification from the individual practitioner.

(2) The individual practitioner's DEA registration expires, unless the registration has been renewed.

(3) The individual practitioner's DEA registration is terminated, revoked, or suspended.

(4) The individual practitioner is no longer authorized to use the electronic prescription application (e.g., when the individual practitioner leaves the practice).

§1311.130 Requirements for establishing logical access control—Institutional practitioner:

(a) The entity within an institutional practitioner that conducts the identity proofing under Section 1311.110 must develop a list of individual practitioners who are permitted to use the institutional practitioner's electronic prescription application to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions. The list must be approved by two individuals.

(b) After the list is approved, it must be sent to a separate entity within the institutional practitioner that enters permissions for logical access controls into the application. The institutional practitioner must authorize at least two individuals or a role filled by at least two individuals to enter the logical access control data. One individual in the separate entity must authenticate to the application and enter the data to grant permissions to individual practitioners to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions. A second individual must authenticate to the application to execute the logical access controls.

(c) The institutional practitioner must retain a record of the individuals or roles that are authorized to conduct identity proofing and logical access control data entry and execution.

(d) Permission to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions must be revoked whenever any of the following occurs, on the date the occurrence is discovered:

(1) An individual practitioner's hard token or any other authentication factor required by the practitioner's two-factor authentication protocol is lost, stolen, or compromised. Such access must be terminated immediately upon receiving notification from the individual practitioner.

(2) The institutional practitioner's or, where applicable, individual practitioner's DEA registration expires, unless the registration has been renewed.

(3) The institutional practitioner's or, where applicable, individual practitioner's DEA registration is terminated, revoked, or suspended.

(4) An individual practitioner is no longer authorized to use the institutional practitioner's electronic prescription application (e.g., when the individual practitioner is no longer associated with the institutional practitioner.)

§1311.150 Additional requirements for internal application audits:

(c) Any person designated to set logical access controls under Section Section 1311.125 or 1311.130 must determine whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescription records. Any such incidents must be reported to the electronic prescription application provider and the Administration within one business day.

§1311.305 Recordkeeping:

(f) If a registrant changes application providers, the registrant must ensure that any records subject to this part are migrated to the new application or are stored in a format that can be retrieved, displayed, and printed in a readable format.

(g) If a registrant transfers its electronic prescription files to another registrant, both registrants must ensure that the records are migrated to the new application or are stored in a format that can be retrieved, displayed, and printed in a readable format.

Appendix E: Rules of Behavior

The Resource and Patient Management System (RPMS) is a United States Department of Health and Human Services (HHS), Indian Health Service (IHS) information system that is ***for official use only***. The RPMS system is subject to monitoring; therefore, no expectation of privacy shall be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

All users (Contractors and IHS Employees) of RPMS will be provided a copy of the Rules of Behavior (ROB) and must acknowledge that they have received and read them prior to being granted access to a RPMS system, in accordance to IHS policy.

For a listing of general ROB for all users, see the most recent edition of *IHS General User Security Handbook* (SOP 06-11a).

For a listing of system administrators/managers rules, see the most recent edition of the *IHS Technical and Managerial Handbook* (SOP 06-11b).

Both documents are available at this IHS website: http://security.ihs.gov/.

The ROB listed in the following sections are specific to RPMS.

E.1 All RPMS Users

In addition to these rules, each application may include additional ROBs that may be defined within the documentation of that application (e.g., Dental, Pharmacy).

E.1.1 Access

RPMS users shall

- Only use data for which you have been granted authorization.
- Only give information to personnel who have access authority and have a need to know.
- Always verify a caller’s identification and job purpose with your supervisor or the entity provided as employer before providing any type of information system access, sensitive information, or nonpublic agency information.
- Be aware that personal use of information resources is authorized on a limited basis within the provisions *Indian Health Manual* Part 8, “Information Resources Management,” Chapter 6, “Limited Personal Use of Information Technology Resources.”

RPMS users shall not

- Retrieve information for someone who does not have authority to access the information.
- Access, research, or change any user account, file, directory, table, or record not required to perform their *official* duties.
- Store sensitive files on a PC hard drive, or portable devices or media, if access to the PC or files cannot be physically or technically limited.
- Exceed their authorized access limits in RPMS by changing information or searching databases beyond the responsibilities of their jobs or by divulging information to anyone not authorized to know that information.

E.1.2 Information Accessibility

RPMS shall restrict access to information based on the type and identity of the user. However, regardless of the type of user, access shall be restricted to the minimum level necessary to perform the job.

RPMS users shall

- Access only those documents they created and those other documents to which they have a valid need-to-know and to which they have specifically granted access through an RPMS application based on their menus (job roles), keys, and FileMan access codes. Some users may be afforded additional privileges based on the functions they perform, such as system administrator or application administrator.
- Acquire a written preauthorization in accordance with IHS policies and procedures prior to interconnection to or transferring data from RPMS.

E.1.3 Accountability

RPMS users shall

- Behave in an ethical, technically proficient, informed, and trustworthy manner.
- Log out of the system whenever they leave the vicinity of their personal computers (PCs).
- Be alert to threats and vulnerabilities in the security of the system.
- Report all security incidents to their local Information System Security Officer (ISSO)
- Differentiate tasks and functions to ensure that no one person has sole access to or control over important resources.
- Protect all sensitive data entrusted to them as part of their government employment.

- Abide by all Department and Agency policies and procedures and guidelines related to ethics, conduct, behavior, and information technology (IT) information processes.

E.1.4 Confidentiality

RPMS users shall

- Be aware of the sensitivity of electronic and hard copy information, and protect it accordingly.
- Store hard copy reports/storage media containing confidential information in a locked room or cabinet.
- Erase sensitive data on storage media prior to reusing or disposing of the media.
- Protect all RPMS terminals from public viewing at all times.
- Abide by all Health Insurance Portability and Accountability Act (HIPAA) regulations to ensure patient confidentiality.

RPMS users shall not

- Allow confidential information to remain on the PC screen when someone who is not authorized to that data is in the vicinity.
- Store sensitive files on a portable device or media without encrypting.

E.1.5 Integrity

RPMS users shall

- Protect their systems against viruses and similar malicious programs.
- Observe all software license agreements.
- Follow industry standard procedures for maintaining and managing RPMS hardware, operating system software, application software, and/or database software and database tables.
- Comply with all copyright regulations and license agreements associated with RPMS software.

RPMS users shall not

- Violate federal copyright laws.
- Install or use unauthorized software within the system libraries or folders.
- Use freeware, shareware, or public domain software on/with the system without their manager’s written permission and without scanning it for viruses first.

E.1.6 System Logon

RPMS users shall

- Have a unique User Identification/Account name and password.
- Be granted access based on authenticating the account name and password entered.
- Be locked out of an account after five successive failed login attempts within a specified time period (e.g., one hour).

E.1.7 Passwords and Second Factor Tokens

RPMS users shall

- Change passwords a minimum of every 90 days.
- Create passwords with a minimum of eight characters.
- If the system allows, use a combination of alpha-numeric characters for passwords, with at least one uppercase letter, one lower case letter, and one number. It is recommended, if possible, that a special character also be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or store them in a safe place (do not store passwords in login scripts or batch files).
- Change passwords immediately if password has been seen, guessed, or otherwise compromised, and report the compromise or suspected compromise to their ISSO.
- Keep user identifications (IDs) and passwords confidential.
- Maintain and store second factor hard tokens, phones, and other devices securely.

RPMS users shall not

- Use common words found in any dictionary as a password.
- Use obvious readable passwords or passwords that incorporate personal data elements (e.g., user’s name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Share passwords/IDs/Tokens with anyone or accept the use of another’s password/ID, even if offered.
- Reuse passwords. A new password must contain no more than five characters per eight characters from the previous password.
- Post passwords.

- Keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.
- Give a password out over the phone.

E.1.8 Backups

RPMS users shall

- Plan for contingencies such as physical disasters, loss of processing, and disclosure of information by preparing alternate work strategies and system recovery mechanisms.
- Make backups of systems and files on a regular, defined basis.
- If possible, store backups away from the system in a secure environment.

E.1.9 Reporting

RPMS users shall

- Contact and inform their ISSO that they have identified an IT security incident and begin the reporting process by providing an IT Incident Reporting Form regarding this incident.
- Report security incidents as detailed in the *IHS Incident Handling Guide* (SOP 05-03).

RPMS users shall not

- Assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident gets reported more than once.

E.1.10 Session Timeouts

RPMS system implements system-based timeouts that back users out of a prompt after no more than 5 minutes of inactivity.

RPMS users shall

- Utilize a screen saver with password protection set to suspend operations at no greater than 10 minutes of inactivity. This will prevent inappropriate access and viewing of any material displayed on the screen after some period of inactivity.

E.1.11 Hardware

RPMS users shall

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).

- Keep an inventory of all system equipment.
- Keep records of maintenance/repairs performed on system equipment.

RPMS users shall not

- Eat or drink near system equipment.

E.1.12 Awareness

RPMS users shall

- Participate in organization-wide security training as required.
- Read and adhere to security information pertaining to system hardware and software.
- Take the annual information security awareness.
- Read all applicable RPMS manuals for the applications used in their jobs.

E.1.13 Remote Access

Each subscriber organization establishes its own policies for determining which employees may work at home or in other remote workplace locations. Any remote work arrangement should include policies that

- Are in writing.
- Provide authentication of the remote user through the use of ID and password or other acceptable technical means.
- Outline the work requirements and the security safeguards and procedures the employee is expected to follow.
- Ensure adequate storage of files, removal, and nonrecovery of temporary files created in processing sensitive data, virus protection, and intrusion detection, and provide physical security for government equipment and sensitive data.
- Establish mechanisms to back up data created and/or stored at alternate work locations.

Remote RPMS users shall

- Remotely access RPMS through a virtual private network (VPN) whenever possible. Use of direct dial in access must be justified and approved in writing and its use secured in accordance with industry best practices or government procedures.

Remote RPMS users shall not

- Disable any encryption established for network, internet, and Web browser communications.

E.2 RPMS Developers

RPMS developers shall

- Always be mindful of protecting the confidentiality, availability, and integrity of RPMS when writing or revising code.
- Always follow the IHS RPMS Programming Standards and Conventions (SAC) when developing for RPMS.
- Only access information or code within the namespaces for which they have been assigned as part of their duties.
- Remember that all RPMS code is the property of the U.S. Government, not the developer.
- Not access live production systems without obtaining appropriate written access, and shall only retain that access for the shortest period possible to accomplish the task that requires the access.
- Observe separation of duties policies and procedures to the fullest extent possible.
- Document or comment all changes to any RPMS software at the time the change or update is made. Documentation shall include the programmer’s initials, date of change, and reason for the change.
- Use checksums or other integrity mechanism when releasing their certified applications to assure the integrity of the routines within their RPMS applications.
- Follow industry best standards for systems they are assigned to develop or maintain and abide by all Department and Agency policies and procedures.
- Document and implement security processes whenever available.

RPMS developers shall not

- Write any code that adversely impacts RPMS, such as backdoor access, “Easter eggs,” time bombs, or any other malicious code or make inappropriate comments within the code, manuals, or help frames.
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

E.3 Privileged Users

Personnel who have significant access to processes and data in RPMS, such as, system security administrators, systems administrators, and database administrators, have added responsibilities to ensure the secure operation of RPMS.

Privileged RPMS users shall

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government personnel and contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance.
- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to RPMS that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to RPMS.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the ISSO, Chief Information Security Officer (CISO), and systems owner.
- Protect the supervisor, superuser, or system administrator passwords.
- Avoid instances where the same individual has responsibility for several functions (i.e., transaction entry and transaction approval).
- Watch for unscheduled, unusual, and unauthorized programs.
- Help train system users on the appropriate use and security of the system.
- Establish protective controls to ensure the accountability, integrity, confidentiality, and availability of the system.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible from the time that the user is no longer authorized system. Passwords forgotten by their owner should be replaced, not reissued.
- Terminate user accounts when a user transfers or has been terminated. If the user has authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel logon IDs and passwords and delete or reassign related active and backup files.

- Use a suspend program to prevent an unauthorized user from logging on with the current user's ID if the system is left on and unattended.
- Verify the identity of the user when resetting passwords. This can be done either in person or having the user answer a question that can be compared to one in the administrator’s database.
- Shall follow industry best standards for systems they are assigned to, and abide by all Department and Agency policies and procedures.

Privileged RPMS users shall not

- Access any files, records, systems, etc., that are not explicitly needed to perform their duties
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

Acronym List

Acronym	Meaning
2FA	Two-Factor Authentication
CIR	Clinical Information Reconciliation Tool
CISO	Chief Information Security Officer
CS	Controlled Substance
DEA	Drug Enforcement Administration
DC	Discontinued
EHR	Electronic Health Record
EPCS	Electronic Prescribing of Controlled Substances
eRx	Electronic Prescription
FDA	U.S. Food and Drug Administration
FPKI	Federal Public Key Infrastructure
GHB	Gamma-hydroxybutyrate
GUI	Graphical User Interface
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IDs	Identifications
IHS	Indian Health Service
ISSO	Information System Security Officer
IT	Information Technology
ITAC	Information Technology Access Control
NADEAN	Narcotic Addiction DEA Number
ONC	Office of the National Coordinator
PAA	EPCS Provider Access Admin
PC	Personal Computer
PIV	Personal Identity Verification
PPA	EPCS Provider Profile Admin
ROB	Rules of Behavior
RPMS	Resource and Patient Management System
SAC	Standards and Conventions
SPI	Surescripts Provider Identifier
SSN	Social Security Number
USB	Universal Serial Bus
VA	U.S. Department of Veterans Affairs
VPN	Virtual Private Network

Contact Information

If you have any questions or comments regarding this distribution, please contact the OIT Help Desk (IHS).

Phone: (888) 830-7280 (toll free)

Web: http://www.ihs.gov/helpdesk/

Email: support@ihs.gov