RESOURCE AND PATIENT MANAGEMENT SYSTEM

Electronic Prescribing of Controlled Substances

(BEPC)

Implementation Plan

Version 1.0
August 2019

Office of Information Technology
Division of Information Resource Management

Table of Contents

Document Revision History

Version	Date	Author	Description	Sections
1.0	8/2019	GDIT SESS team	Initial Release	All

1.0 Introduction

1.1 Purpose of Implementation Planning

The Electronic Prescribing of Controlled Substances (EPCS) project implements the Drug Enforcement Administration (DEA) regulations that give providers the ability to electronically prescribe outpatient controlled substances, whether the orders are sent to the Outpatient Pharmacy at the site or electronically transmitted to Surescripts. The regulations require each provider to be individually configured with specific information, such as the number that gives them the authority to prescribe controlled substances (DEA or Veterans Administration [VA] number), any schedules for which they can or cannot prescribe, and the authorization to do electronic prescribing of controlled substances.

In addition, two-factor authentication for both provider credentialing and the digital signing of controlled substances must be instituted at the site. This configuration should be done prior to enabling the site for EPCS.

If the site transmits prescriptions to Surescripts, the provider shall have an active Surescripts Provider Identifier (SPI) number and the site must have the ability to send different classes of controlled substances through Surescripts.

The intended audience of the EPCS Implementation Plan is the Business Sponsor and the Integrated Project Team which must include information technology (IT) personnel, the Clinical Application Coordinator (CAC), pharmacists, and providers.

1.2 Implementation Objectives

The Indian Health Service (IHS) must meet the DEA regulations and the Department of Health and Human Services (HHS) Office of National Coordinator (ONC) 2014 certification requirements for the IHS mandated project Electronic Prescribing of Controlled Substance (EPCS). The requirements for EPCS in ONC 2014 are largely met by the e-prescribing functionality already implemented in the Resource and Patient Management System (RPMS). The Office of Information Technology (OIT) seeks to develop critical enhancements to the existing e-Prescription (e-Rx) process within RPMS to allow for secure electronic prescription of Controlled Substances as required by law.

The following considerations must be addressed in this enhancement:

- U.S. Drug Enforcement Administration (DEA) – Compliance with “Electronic Prescriptions for Controlled Substances” (2010) provides the option of writing prescriptions for controlled substances electronically.
- Compliance with Tribal and State Laws:

  - New York State requires all prescriptions to be sent electronically, including controlled substances.
  - Starting July 1, 2017, Maine requires all prescriptions for opioids to be sent electronically.
- Authorization of users to prescribe controlled substances under EPCS
- Secure Two-Factor Authentication
- Digital Signing of electronic controlled substances
- Integration with existing RPMS e-Prescribing functionality

This implementation plan includes the following in support of the business objectives:

- This Implementation Plan covers establishing connectivity to time.nist.gov and to the certificate revocation list (CRL) of the certificate authority (CA) that issued the digital signing certificates. These connections are necessary to ensure the EPCS Monitoring Service is able to assess compliance with the DEA regulations regarding system time and certificate revocations.
- This Implementation Plan covers the patching of a site's RPMS server to implement the EPCS functionality. This not only covers the multi-factor authentication and digital signing, but also includes updates to the Surescripts messaging to support sending controlled substances medication orders to community pharmacies.
- This Implementation Plan covers establishing the process to identity proof and authorize the providers that will conduct EPCS.
- This Implementation Plan covers establishing the process to provision providers that have been authorized to conduct EPCS. This includes the process to issue the provider a cryptographic token and digital signing certificate. It also covers the process to establish a provider's EPCS profile in the RPMS server and to activate the ability to electronically prescribe controlled substance medications.
- This Implementation Plan also covers establishing the processes required for the continued operation and maintenance of the EPCS functionality.

The following objectives are designed so that the transition once EPCS is enabled for the site will flow as easily as possible:

- Understand what KIDS builds must be installed.
- Understand what pharmacists can and cannot do with a digitally signed order and the role of the PSDRPH key.
- Understand how providers should be credentialed to do EPCS and get the setup done before the site goes live.
- Understand how two-factor authentication will be implemented at the sites.

- Make sure that all users have the necessary hardware and software to do two-factor authentication when EPCS is enabled for the site.
- If the site intends to do electronic prescribing of controlled substances to Surescripts, understand the changes required.
- Establish local implementation team.

1.3 Assumptions

For the software to be installed, some assumptions must be made:

- The site is up to date with all required patches.
- The software has been approved for EPCS by the DEA and Surescripts.
- The two-factor authentication software is available to users.
- The scope of the EPCS project is only for writing, signing, and transmitting Controlled Substance (CS) orders to either:
  - Local on-site pharmacy.
  - "Community" pharmacies outside of the IHS, tribal and urban sites and who will receive the order via Surescripts.
- Maintain current paper CS for non-EPCS enabled sites and providers.
- The physician's electronic signature code will be used as the first required authentication types.
- PIV and/or USB cryptographic tokens will be used as the second authenticator.
- The EPCS solution will use the provider's signing certificate that will be on the provider's PIV or USB cryptographic token.

1.4 Constraints

The following constraints have been identified for the EPCS solution:

- The deployment approach may require adjustment as the project progresses through the different phases in response to emerging needs.
- Current legacy processes / workflows will be continuously refined based on feedback collected during retrospectives.

1.4.1 Modification and Recertification

This patch contains modifications required for EPCS. EPCS has been certified by the Drug Enforcement Administration and in accordance with Title 21 CFR Subpart 1311 should not be modified without recertification.

1.4.2 EPCS and Child Divisions

The main division at a site shall implement EPCS before any child divisions implement EPCS. If the main site does not plan to implement EPCS, any child divisions that want to implement EPCS will not be able to do so unless they establish their own RPMS database.

2.0 Planning

The Electronic Prescribing for Controlled Substances Implementation Plan provides an outline of activities necessary to ensure that the EPCS product is available for use by end-users as originally planned.

The site should spend time fully planning for this release as it will impact patient's ability to receive medications in a timely fashion.

The site must plan for dealing with attempted breaches or tampering of provider's credentials, system security, or the ordering of controlled substances. Policies shall be implemented when responding to reports and alerts that indicate an alleged breach of security in these areas.

The impact of tampered credentials is that providers will not be able to digitally sign orders and/or orders already signed will be automatically discontinued. This can affect patient care.

Sites also shall become familiar with the software for two-factor authentication and learn how to use it properly.

Pharmacists shall learn processing of digitally signed orders.

2.1 Roles and Responsibilities

The main role changes involve dealing with tampering of credentials or orders. This is a new responsibility and may be split up among different users or departments depending on the size of the facility.

Several new reports and/or alerts will notify people of a tampered credential or order, but the new responsibility will be to determine what should be done after that to ensure system safety. These reports cannot be ignored. They must be run according to the DEA regulations and action taken when a breach has occurred.

2.1.1 Site Project Manager

The Site Project Manager is a member of the site workforce and is responsible for coordinating resources and schedules on behalf of the site.

2.1.2 Implementation Project Manager

The Implementation Project Manager is a member of the EPCS Development Team and is responsible for coordinating the external resources and schedules for the implementation of EPCS at a site.

2.1.3 Training Development

Responsible for developing the necessary pre- and post-implementation training content.

2.1.4 Site Trainer

Responsible for carrying out the training during a site implementation. This includes system administration, end user and train the trainer training.

2.1.5 Site Team

Members at the site that will implement the EPCS solution.

2.1.6 System Administration

Site members, such as IT Support Staff, CACs, etc., that will support the implementation process as well as support the ongoing operations and maintenance.

2.1.7 Support Team

Members of the EPCS Development Team, not on site, that will provide ad hoc support to the Site Team as needed.

2.2 Workforce Changes

It is not anticipated that there will be any reduction or relocation of workforce. It is anticipated that existing workforce members will be assigned EPCS/Pharmacy roles based on existing job functions. The site shall make an independent assessment to determine if additional workforce members will be required. The site shall ensure that each of the roles are appropriately covered during the implementation process.

Site Team Members can be considered a temporary workforce during the implementation. The Site Team Members and both Project Managers will coordinate the following:

2.2.1 Implementation Team

The EPCS functionality introduces task-based roles to be integrated into the workforce. The site shall plan for the assignment of these roles to appropriate individuals from local staff, Area Office staff, and possibly IHS OIT National Program staff. The site should consider separation of duties and least privileges when making these assignments. The site should also consider assigning backup individuals for each role to ensure adequate coverage in the event the primary individual is unavailable.

The following task-based roles are new for EPCS:

- **EPCS Provider Profile Admin**: See EPCS Credentialing under Section 2.4 for additional information.
- **EPCS Provider Access Admin**: See EPCS Credentialing under Section 2.4 for additional information.
- **EPCS Incident Responder Role**: See Incident Response under Section 2.4 for additional information.
- **BEHO EPCS Incident Response Mailman Group**: See Incident Response under Section 2.4 for additional information.

The following roles will have additional tasks related to EPCS functionality:

- **Site Administrator**: The Site Administrator will have additional settings to configure for EPCS enabled providers. The Site Administrator may also coordinate with providers authorized for EPCS to obtain their cryptographic token and digital signing certificate from the third-party credential service provider.
- **Pharmacy Manager**: The Pharmacy Manager will have additional settings to configure for EPCS enabled Pharmacists.
- **Credentialing Office**: Credentialing Office personnel will still conduct the vetting and background checks to determine whether a provider is allowed to practice at a site. The Credentialing Office personnel will have the additional task to specifically authorize a provider for EPCS and trigger the provisioning of the account, cryptographic token, and digital signing certificate. The Credentialing Office must also maintain a list of providers that have been authorized for the EPCS functionality.
- **Purchasing/Contracting Office**: If a site will be using USB cryptographic tokens, a site's purchasing/contracting office will have the additional task to manage the acquisition and payment for the Credential Service Provider team to obtain the cryptographic token and digital signing certificate for a provider. This includes the following:
  - The initial batch of providers as a site implements the EPCS functionality.
  - The renewal of a provider's certificate every two years.
  - Acquisition for new providers as they come on board.
- **Help Desk**: A site's Help Desk may update the workflow of existing help desk tickets or create tickets and workflows to accommodate the provisioning and de-provisioning of EPCS-enabled providers.

> **Note:** The terms Help Desk and Ticket are used as generic stand-ins for the process to request and track actions by certain groups. This could be a formal help desk program, or it could be an email or paper form. Each site will want to know or establish the process to request and track certain tasks needed to support EPCS.

2.3 Employee Transition

It is well known that change is difficult for many people, and changes in processes that have been done one way for over 10 years is the most difficult. Adding in another layer for signing of medications will be difficult for many people and therefore training will be required for providers and pharmacists.

It is only when employees know what is coming, why the change is being implemented, and receiving training on the changes that it will be accepted without a loss of morale.

2.3.1 Transition of Implementation Team

Sites will need to consider when the implementation team is formally activated.

2.3.2 Transition of Tasked Based Roles

The following are recommendations for when to assign and engage the roles related to EPCS functionality.

- **EPCS Provider Profile Admin**: Consider assigning and training early in the deployment process. Assignment and training shall occur early enough that the individuals can carry out the provisioning of providers when the EPCS functionality moves into operations. It is recommended to assign and train earlier so that the individuals can participate in the testing of the system prior to the move into operations.
- **EPCS Provider Access Admin**: Consider assigning and training early in the deployment process. Individuals assigned the Provider Profile Admin role require time to obtain a cryptographic token from the Credential Service provider. Assignment and training shall occur early enough that the individuals can carry out the provisioning of providers when the EPCS functionality moves into operations. It is recommended to assign and train earlier so that the individuals can participate in the testing of the system prior to the move into operations.

- **EPCS Incident Responder**: Consider assigning and training early in the deployment process. Assignment and training shall occur early enough to start the daily review of the EPCS and Pharmacy Incident Response reports once the EPCS functionality goes into operation. It is recommended to assign and train earlier so that the individual can participate in the testing of the system prior to the move into operations.
- **BEHO EPCS Incident Response Mailman Group**: The individual assigned the EPCS Incident Responder role shall be assigned as a member of the BEHO EPCS Incident Response Mailman group. Any additional members should be assigned and trained to start monitoring EPCS alerts around the time EPCS functionality goes into operation.
- **Site Administrator**: The Site Administrator should be engaged from the very beginning and undergo training as soon as possible. The Site Administrator is considered a key role in the implementation of EPCS.
- **Pharmacy Manager**: The Pharmacy Manager should obtain training early enough that the individual is ready to provision the Pharmacy staff once EPCS functionality goes into operations.
- **Credentialing Office**: The Credentialing Office Personnel should receive training early enough that they can complete the workflow changes to authorize providers prior to the EPCS functionality going into operations.
- **Purchasing/Contracting Office**: A site's Purchasing/Contracting Office shall be engaged early so that they can make a decision on which Credential Service Provider to use. This decision must be made early enough that cryptographic tokens can be obtained for the implantation and testing personnel. The Purchasing/Contracting Office shall have the bulk acquisition made in time to provision providers once EPCS functionality goes into operations.
- **Help Desk**: Entities responsible for a site's Help Desk functions shall be engaged early enough so that the workflows are established before the EPCS functionality goes into operations.
- **Providers**: The initial set of providers should be trained close to the time that the EPCS functionality goes into operations. There should not be a large lag between the time the training occurs and when the EPCS functionality goes into operations. Ongoing, new providers should receive EPCS training as part of the normal on-boarding processes.
- **Provider Agents**: The initial set of provider agents should be trained close to the time that the EPCS functionality goes into operations. There should not be a large lag between the time the training occurs and when the EPCS functionality goes into operations. Ongoing, new providers should receive EPCS training as part of the normal on-boarding processes.

- **Pharmacists**: The initial set of pharmacists should be trained close to the time that the EPCS functionality goes into operations. There should not be a large lag between the time the training occurs and when the EPCS functionality goes into operations. Ongoing, new providers should receive EPCS training as part of the normal on-boarding processes.

2.4 Business Process

In setting up EPCS, the process of credentialing providers for being able to order different classes of controlled substances and for being able to do EPCS will involve policy and procedural changes.

There will also be policy changes on what to do when a provider's credentials have been tampered with. In addition, policy changes on the tampering of medication orders, audit file tampering or unauthorized access to the database will be required.

The site shall first determine who and/or which department will be responsible for each type of tampering. The site manager or the area office may be responsible for unauthorized access to the system, while it may be the pharmacy that handles order tampering. For each type of tampering, official standards of actions to be taken shall be in place before EPCS goes live.

The site may implement Business Associates Agreement (BAA) or a Non-Disclosure Agreement (NDA).

The site may prepare standardized forms for business process such as:

- EPCS Authorization.
- Credential Assignment.

2.4.1 Policy and Procedure Review

Given the regulatory requirements of EPCS, a site should plan on reviewing its policies and procedures to determine if any modifications are required. Policy and procedure changes should be in place by the time the EPCS functionality goes into operation.

At a minimum, a site should look at policies that cover the following:

- Credentialing providers.
- Controlled substance medication ordering.
- Electronic prescribing.
- Daily backups of RPMS data.

The other business processes identified in this section may have corresponding procedures that a site should review.

2.4.2 Identity Proofing/Credentialing

EPCS has been set up around the hybrid Institutional and Individual Provider model outlined in the DEA regulations. Under this model, the individuals responsible for credentialing providers will conduct the vetting and identity proofing and authorization of a provider to conduct EPCS. Once approved an authorization is sent to the appropriate system administrators to provision the provider with an authentication token and to set up and activate the provider for EPCS in the RPMS system.

For federal sites, the user's PIV card would be registered. Non-federal sites will need to utilize a third-party credential service provider. Once authorized, the provider goes through the designated Credential Service Provider to undergo identity proofing and receive a cryptographic token with a digital signing certificate. Given the amount of time it takes to issue a PIV, a site may want to consider using a USB cryptographic token as an interim credential for EPCS.

2.4.3 Acquisition

For federal sites, a PIV will be used. Established identity proofing and issuance processes will be used.

For non-federal sites or federal sites that opt to use an interim token until the PIV is issued would need to obtain a USB cryptographic token from an authorized credential service provider. The EPCS functionality obtained DEA certification utilizing cryptographic tokens from the following Credential Service Providers (CSPs):

- IdenTrust
  IdenTrust
  6623 Dumbarton Circle
  Fremont, CA 94555
  (415) 486-2900
  https://identrust.com

- ORC
  WidePoint Cybersecurity Solutions Corporation (formerly ORC, Inc.)
  11250 Waples Mill Road
  South Tower, Ste 210
  Fairfax, VA 22030
  800-816-5548
  https://www.orc.com

See the *EPCS Token Provisioning Guide*.

A site shall plan for establishing a relationship with one of the listed CSPs in order to issue cryptographic tokens and the digital signing certificates to providers.

Costs from the CSPs are on a per provider basis. Using the number of existing providers and anticipated turnover determined from capacity planning, the site should plan and budget for the acquisition of initial cryptographic tokens for a provider. Budgeting should also take into account the certificate renewals for a provider.

2.4.4 Pharmacy

Because the medication ordering and pharmacy sides are so tightly coupled, the archive on the order side serves as the archive for the pharmacy side. Otherwise there is only one substantial change on the pharmacy side related to EPCS.

When a provider issues a paper prescription to the internal pharmacy, the order is still electronically transmitted to the pharmacy without the prescription being digitally signed. To keep efficiencies and to reduce data entry errors, a pharmacist shall enter the electronic signature code to attest that the paper prescription is being acted upon. Otherwise, the pharmacist would be required to reenter the prescription information into the system.

2.4.5 Controlled Substance Medication Ordering

When ordering a controlled substance medication, a provider will be required to use multifactor authentication to have the order digitally signed and transmitted.

Once the provider successfully authenticates, the controlled substance medication order will be digitally signed by an individual digital signing certificate stored on the provider's cryptographic token. The order, the provider's public certificate, and the signature are then archived in the RPMS system.

2.4.6 Surescripts

With the completion of EPCS and the associated Refill Request project, it will be feasible for the site to send controlled substance prescriptions to community pharmacies over Surescripts.

Procedures for controlled substance medication ordering should include a check to verify the community pharmacy will accept controlled substances electronically.

If a site uses Surescripts and intends to deploy to a test system prior to deploying to a production system, the test system requires a connection to the Surescripts staging server. A site should plan on submitting appropriate help desk tickets to provision the connection.

Sites currently not using the Surescripts portal but anticipate enabling because of EPCS should consider the timing of the EPCS and the Surescripts implementation. It is recommended that Surescripts either be implemented prior to implementing EPCS functionality or after EPCS functionality has been in operations for a while. This will simplify the deployment and simplify the troubleshooting of any issues that may arise during the implementation process.

2.4.7 Record Retention

EPCS has a specific retention requirement around the archive of the digitally signed medication orders and the EPCS audit logs. The DEA requires the archives and the audit logs to be retained for two years. Federal sites are also subject to National Archives and Records Administration (NARA) records retention requirements, which move retention out to six years.

2.4.8 Incident Response

DEA regulations require a daily review of the audit logs to look for issues. The EPCS application includes two daily EPCS Incident Reports, one for the ordering side and one for the pharmacy. These reports shall be reviewed on a daily basis and any anomalies identified, investigated and addressed.

The BUSA Audit Log is the central audit repository for EPCS audit events. The BUSA Audit Log is also the source of information used to generate the daily EPCS and Pharmacy Incident Reports.

The BUSA Audit Log will be used even if a site has not turned it on for Meaningful use or other purposes so there is no need to specifically turn BUSA on.

The following are incident types a site should consider when planning for incident response:

1. Time is out of synchronization with NIST time servers by more than five minutes. If this occurs e-Prescribing of controlled substances is out of compliance and use of the EPCS applications should be discontinued.

    a. The EPCS Background Monitoring Service will check to see if time is in synchronization. Alerts will be generated and sent to a designated individual if the checks do not occur or when time synchronization is out of synch more than three minutes. These events are captured in the BUSA audit log. Utilize the EPCS Audit Log Report in List view and filter for the Service event type. Review for time synchronization checks.

b. To trace the issue, review the time synchronization configuration of the local server and check the local operating system audit logs for any time synchronization issues. Check configuration to ensure correct upstream servers are being referenced and that correct time settings, such as UTC are being utilized. Audit log should identify if server is unable to connect to upstream time servers. If local server appears correct, repeat the process with the upstream time servers until the issue is identified. Another issue to consider, depending on the age of the server is whether the battery for the real-time clock is losing power.

c. Depending on the nature of the actual issue, consider the following responses:

- If the issue is with the upstream time servers, disable time synchronization and manually set the local time to match NIST time.
- If the issue is with the local clock, fall back to issuing hard copy prescriptions until the issue can be resolved.

2. Corruption or tampering of the provider profile.

a. A background job will run a daily check of the provider profile integrity. If integrity issues, mismatched hashes, are identified, the results are provided in the daily incident response report.

The integrity of a provider's profile is also checked at the time a controlled substance medication order is attempted. If the integrity is not valid, the order is stopped. An audit entry is generated, and alerts are sent to both the provider and the designated incident response individual.

b. To trace the issue, run the Provider Profile Integrity Check Report. This report will identify all provider profiles that have an issue. This report will also give an indication whether the issue is isolated to only one or two providers or is more widespread.

To help determine if the issue is related to corruption rather than tampering, review the local operating system logs housing the RPMS database. Look for issues indicating unexpected shutdowns or restarts. Also look for indications of storage issues such as disk failures or RAID array inconsistencies. Look into the CACHE audit logs to determine if there are any database issues or inconsistencies.

To help determine if the issue is related to tampering, look in the BUSA audit logs. Review the activity around provider profile and verification. Use the EPCS Audit Reporting tool and select **EPCS** and the event **Type: Provider Profile** for the filter. Review the BUSA audit logs for any FileMan changes on New Person and EPCS Provider Profile files. Also look at the local server operating system logs and CACHE logs to see if any anomalous activity occurred before and during the time period the tampering occurred.

c. Response should include fallback to contingency of paper prescriptions until the root cause can be found. Provider Profiles should be either restored from a known good backup or manually edited and verified based on the original authorizations on file with the credentialing office.

3. Corruption or tampering of the archived digitally signed electronic controlled substance medication orders (**ORDER DEA ARCHIVE INFO** and **PKI Digital Signatures**).

   a. A background job will run a daily check of the integrity of the **ORDER DEA ARCHIVE INFO** and **PKI Digital Signatures** files. If integrity issues, mismatched hashes, are identified, the results are provided in the daily incident response report.

   b. To help determine if the issue is related to corruption rather than tampering, review the local operating system logs housing the RPMS database. Look for issues indicating unexpected shutdowns or restarts. Also look for indications of storage issues such as disk failures or RAID array inconsistencies. Look into the CACHE audit logs to determine if there are any database issues or inconsistencies.

      To help determine if the issue is related to tampering, look in the BUSA audit logs. Review the activity around controlled substance medication orders. Use the EPCS Audit Reporting tool and select **EPCS** and the **Rx event type** for the filter. Review the BUSA audit logs for any FileMan changes in **ORDER DEA ARCHIVE INFO** or **PKI Digital Signatures**. Also check the local server operating system logs and CACHE logs to see if any anomalous activity occurred before and during the time period the tampering occurred.

   c. Response should include fallback to contingency of paper prescriptions until the root cause can be found. The **ORDER DEA ARCHIVE INFO** and **PKI Digital Signature** file should be either restored from a known good backup.

4. Corruption or tampering of BUSA audit records.

   a. A daily background job will run a daily check of the integrity of the EPCS related audit entries in the BUSA audit log. If integrity issues, mismatched hashes, are identified, the results are provided in the daily incident response report.

   b. To help determine if the issue is related to corruption rather than tampering, review the local operating system logs housing the RPMS database. Look for issues indicating unexpected shutdowns or restarts. Also look for indications of storage issues such as disk failures or RAID array inconsistencies. Look into the CACHE audit logs to determine if there are any database issues or inconsistencies.

To help determine if the issue is related to tampering, run the EPCS Audit Log Report in List mode. The List mode report includes a real-time check of the integrity of the audit record. Reverse sort the report on the Hash column. This will bring all the audit records with a mismatched hash to the top of the report. Review the BUSA audit logs for any FileMan changes on BUSA audit log file. Also look at the local server operating system logs and CACHE logs to see if any anomalous activity occurred before and during the time period the tampering occurred.

c. Response should include fallback to contingency of paper prescriptions until the root cause can be found. It is not recommended to restore the BUSA audit log from a file. Set aside the last known good backup of that BUSA audit log. Stop all activity and create an archive backup of the current BUSA audit log that has the issues, documenting the issues. These need to be retained for at least two years to meet Drug Enforcement Agency retention requirements and for at least six years to meet HHS/NARA incident response retention requirements.

5. Audit log exceeds storage capacity. If the system is not able to retain an audit trail of EPCS medication ordering for pharmacy activity, the applications are considered out of compliance and use should discontinue until the application can be brought back into compliance.

   a. The monitoring of storage space for the audit logs is inherited from the site running RPMS.

   b. The site will need to review logs of the system being used to monitor the capacity of the storage holding the audit logs. Local operating systems utilities, such as diskmanager may also be used to determine the current available storage capacity.

   c. Response should include fallback to contingency of paper prescriptions until the root cause can be found and corrected.

6. Denial of service due to lost, stolen cryptographic token or expired or revoked digital signing certificate. A provider will be unable to conduct the multifactor authentication necessary to authorize the digital signing and release of a controlled substance medication order.

   a. An expired token will generate an audit event and alert the provider when an attempt to authenticate with the token is conducted. The provider will need to alert the site administrator.

      A lost or stolen token will not generate any audit events. It is up to the provider to follow site policy and appropriately report as an incident.

b. The Drug Enforcement Regulations do not account for the issuance of a temporary or emergency token. Due to the Level of Assurance 3 requirement, the response is effectively to disable the original token and issue a new token. Response should also include fallback to paper prescriptions for the impacted provider until a replacement token is issued.

   If a site opts to implement the contingency plan option where a provider obtains two cryptographic tokens. The provider would work with the EPCS Provider Profile Admin and EPCS Provider Access Admin to register the alternate token for use for EPCS.

2.4.9 Contingency Planning

The following are EPCS contingency types a site should consider in its planning:

- The EPCS functionality is rooted in RPMS. As such, EPCS will inherit the same threats and contingency planning from the site running RPMS. The primary contingency option for EPCS is to fall back to issuing paper prescriptions.
- A communications or outage related to the Central Ensemble/Surescripts server will prevent electronic transmission of prescriptions to community pharmacies. The EPCS functionality will inherit any telecommunications redundancy already established for eRx functionality at a site. The fallback is to issue paper prescriptions in the event the outage issue cannot be addressed by an alternate telecommunications path.
- Revoked or expired certificates prevent the digital signing of the controlled substance medication orders. The system will not complete medication orders if a provider's digital signing certificate is not valid. The fallback is to issue a paper prescription.
- If the order or pharmacy applications are no longer in DEA compliance, the site must discontinue use of EPCS. Some short-term compliance issues would be the system time more than five minutes out of sync with the NIST time server, audit logs not being captured. Long-term compliance issues include system compromise or failure to complete the two-year DEA recertification. The primary contingency option for EPCS is to fall back to issuing paper prescriptions.

2.4.10 Help Desk Support System

> **Note:** Help Desk is being used as a generic term to refer to the parties and processes used to request certain actions. It could be a submitting a ticket to a formal help desk system or it could be an email to a designated contact. The goal of this section is to determine those parties and processes.

It may be necessary for a site to submit Help Desk tickets to configure the firewall rules and proxy servers to establish the connections. A site shall determine the appropriate Help Desk System and ticket types for the following requests:

- A request for the site to configure site firewall/proxy rules to allow the EPCS Monitoring Service to reach time.nist.gov.
- A request for the site to configure site firewall/proxy rules to allow the EPCS Monitoring Service to reach the CRL Distribution Points for the digital signing certificates.

Document the Help Desk Systems and ticket types that shall be generated during the deployment process.

For each of the following ticket types note the following information:

- The Help Desk Support System used.
- One or more of the following as applicable:
  - Existing Ticket Type to use as is.
  - Existing Ticket Type to modify.
  - New Ticket Type to create.

Table 2-1: Help Desk tickets and systems

Ticket Type	**Help Desk System**	**Use Existing** (Note Ticket Type)	**Modify Existing** [Note Ticket Type and Modifications]	**Create New**
Site Firewall/Proxy Change for time.nist.gov				
Site Firewall/Proxy Change for CRL Distribution Points				

A site may require assistance from various teams and roles to assist with any troubleshooting during the Site Deployment. The site shall know how to request that assistance.

The site shall establish its own Help Desk process to authorize and provision providers and to authorize and provision pharmacists for EPCS.

2.4.11 Capacity Planning

The site should identify and document the following information required to conduct the capacity assessment:

- Total Number of Divisions (count Parent as 1 Division).
  - Number of Divisions that are a separate independent site acting as a Division.

  - Number of providers in each Division that will be EPCS enabled.
  - Number of controlled substance medication orders per day for each Division.
- Number of Pharmacies supported by site.
  - Number of Pharmacists in each Pharmacy that will be EPCS enabled.
  - Number of controlled substance medication orders processed per day for each Pharmacy.
- Site RPMS Server Information

> **Note:** The Site RPMS Server Information should be gathered after the RPMS System has been brought up to the minimum patch levels.

  - OS Type and Version.
  - Disk Space.
  - Site Bandwidth.

Use the EPCS Capacity Plan to determine the impacts EPCS will have on the RPMS System. If any issues are identified, note the ones that shall be addressed prior to deploying EPCS.

2.4.12 Compliance Related Planning

This patch contains modifications required for EPCS. EPCS has been certified by the Drug Enforcement Administration and in accordance with Title 21 CFR Subpart 1311 should not be modified without recertification.

2.4.12.1 Retention

Order DEA Archive Info

Title 21, Section 1311.120(b)(15) requires the EPCS application to electronically archive the digitally signed controlled substance medication order. Title 21, Section 1311.120(b)(28) requires that such records be retained for at least two years.

This information is also covered by NARA General Records Schedule GRS 3.2-031: "System access records. Systems requiring special accountability for access," which requires the information to be retained for six years.

The **ORDER DEA ARCHIVE INFO** file is used to archive the record. The corresponding digital signature is stored in the file PKI Digital Signature. The EPCS software does not automatically purge records. The site shall ensure that proper retention schedules are maintained by keeping data according to retention or by moving and retaining the data in an offline archive.

If moving to an offline archive, records from **ORDER DEA ARCHIVE INFO** and **PKI Digital Signature** should be moved as a set.

PKI Digital Signature

The **PKI Digital Signature** file contains the corresponding digital signature for the records in ORDER DEA ARCHIVE. The digital signature is linked by the Digital Signature Hash field in the corresponding DEA ARCHIVE INFO file.

As noted above, DEA regulations require that records be retained for two years and the NARA records retention schedule require that the records be retained for six year.

The EPCS software does not automatically purge records. The site shall ensure that proper retention schedules are maintained by keeping data according to retention or by moving and retaining the data in an offline archive.

If moving to an offline archive, ensure that records from PKI Digital Signature are moved as a set with the corresponding DEA ARCHIVE INFO file.

BUSA Audit Log

Title 21, Section 1311.120(b)(23) requires the EPCS application to maintain an audit log. Title 21, Section 1311.120(b)(28) requires that audit records be retained for at least two years.

Title 21, Section 1311.205(b)(13) requires the Pharmacy application to maintain an audit log. Title 21, Section 1311.205(b)(18) requires that audit records be retained for at least two years.

Audit records are also covered by NARA General Records Schedule GRS 3.2-031, "System access records. Systems requiring special accountability for access," which requires the information to be retained for 6 years.

Audit records generated within RPMS are stored in BUSA. BUSA does not automatically purge records. The site shall ensure that proper retention schedules are maintained by keeping data according to retention or by moving and retaining the data in an offline archive.

2.4.13 Incident Response

Incident response planning shall incorporate responses to the following types of incidents related to EPCS:

- Time is out of synchronization with NIST time servers by more than five minutes.
- Corruption or tampering of a provider's EPCS profile.
- Corruption or tampering of the archived digitally signed electronic controlled substance medication orders (ORDER DEA ARCHIVE INFO).
- Corruption or tampering of BUSA audit records.
- Audit log exceeds storage capacity.

- Denial of service due to lost, stolen, revoked, or expired authentication token.

2.4.14 Future System Changes

Similar to Meaningful Use (MU), future system or operational changes shall be evaluated to determine the impact on EPCS certification.

If it is unclear whether a change will impact the EPCS certification or whether it is absolutely clear a change will impact the EPCS certification, it is recommended to contact the DEA Certification Assessor. The Assessor will be able to determine the actual impact of the change to the certification and make a determination of the level of testing required to maintain the certification.

The set of patches identified in Section 2.5.2 RPMS Related Software contain the modifications required for EPCS. EPCS has been certified by the Drug Enforcement Administration and in accordance with Title 21 CFR Subpart 1311 should not be modified without recertification.

2.4.15 Operations and Maintenance Planning

This section describes the maintenance and operations activities for the EPCS solution.

2.4.15.1 Digital Signing Certificates

The site shall plan for ongoing certificate operations.

Renewing Digital Signing Certificates

The digital certificates on the tokens have a limited lifespan and must be renewed. For federal sites utilizing PIV, the renewal process will follow the existing card and certificate renewal processes. IndenTrust certificates must be renewed every two years. ORC certificates must be renewed every year. The site shall establish processes and procedures for providers to renew their certificates in a timely manner. Additional information can be found in the *EPCS Token Provisioning Guide*.

Revoking Digital Signing Certificates

Digital signing certificates may be revoked in the event a token is lost or compromised. The certificates shall be revoked if a site intends to reclaim the token if a provider leaves the organization. Federal sites will use existing processes to revoke a PIV card. Sites utilizing USB cryptographic tokens shall establish process and procedures to revoke a provider's certificate when needed. Additional information can be found in the *EPCS Token Provisioning Guide*.

Cryptographic Tokens

The site shall plan for the ongoing issuance of tokens for new providers. The site shall plan for obtaining replacements for lost or damaged tokens. This process should include how a site will handle emergency tokens (Section 2.4.9).

The site shall address how they will handle multi-site providers. A token issued from another site can be used, as long as both sites support the same type of token. For example, a provider who works at more than one federal site could use a PIV at those sites. A provider with a USB cryptographic token could work at multiple non-federal sites and federal sites that opt to use USB cryptographic tokens as an interim credential. However, a provider with a PIV only would need to obtain a USB cryptographic token to work at a non-federal site. A provider with a USB cryptographic token would need to obtain a PIV to work at a federal site that allows a PIV only.

2.4.15.2 Patching/Hot Fixes

The site shall plan for the ongoing monitoring and prompt installation of EPCS patches. Such patches will likely be needed to address issues or updates to DEA regulations and would be necessary to keep the system in compliance.

2.4.15.3 On-Boarding

New Personnel

The site shall plan on incorporating the credentialing and provisioning of new providers and pharmacists that will be EPCS enabled.

Multi-Site Providers

Similar to new personnel, the site shall identity proof and authorize a provider from another site. However, it may not be necessary to provision a new cryptographic token. (See **Cryptographic Tokens** in Section 2.4.15.1) The cryptographic token issued by the provider's primary site can be used. The site shall plan on incorporating a process to register the token for a provider that operates at multiple sites.

2.5 Technology Requirements

- Workstations for Site Team.
- Provision Accounts during install.

2.5.1 Deployment Architecture Diagram

2.5.1.1 Information Flow Diagram

The Information Flow Diagram highlights the high-level components and how they communicate with each other. There are three high-level components for EPCS.

RPMS Server

The RPMS server houses the components to conduct the multifactor authentication. The electronic signature code component verifies the provider's electronic signature code. The electronic signature code component then makes a call using the BEH2FA component to validate the personal identification number (PIN) for the cryptographic token entered by the provider. The component calls the token driver on the workstation to interact with the cryptographic token.

Once multifactor authentication is completed successfully, the digital signing component assembles the elements of the controlled substance medication order, creates a digest, and submits to the cryptographic token to digitally sign.

Multifactor authentication is also used by the Provider Access Admin to activate a provider for EPCS. The EPCS Credentialing Service will use the electronic signature code component to unlock the cryptographic token and verify the certificate.

If the site uses Surescripts for external pharmacies, the RPMS server maintains a connection to the Central Ensemble, which is responsible for transmitting the prescription. This functionality is essentially unchanged. HL7 messages have been updated to comply with Surescripts handling of controlled substance medication orders.

The RPMS server provides an RPC listener. In relation to EPCS, this provides the communication point for the Electronic Health Record (EHR) graphical user interface (GUI). This functionality is essentially unchanged.

The RPMS server provides an EPCS Monitoring Service. This service is used to conduct two different checks to ensure the EPCS application is incompliance with the DEA regulations.

- The monitoring service conducts a check to verify that the system time is within five minutes of NIST time sources. This call is only a check. It does not adjust the local system time. The site will still need to ensure proper configuration to use the site's designated time servers.
- The Monitoring Service makes a call to time.nist.gov using NTP. The site shall allow the service access to the Internet using a designated firewall/proxy.

- The monitoring service conducts a check to verify the status of the digital signing certificates. The Monitoring Service makes a call to the Certificate Revocation List Distribution Points of the Certificate Authority that issued the certificate using HTTP. The site shall allow the service access to the Internet using a designated firewall/proxy.

DEA regulations require auditing of EPCS activities. The BUSA audit log has been designated as the central repository for EPCS audit events. Several components will feed audit events as EPCS activities are carried out.

Workstation

The Pharmacy application users will still use a roll and scroll terminal connection to connect to the RPMS server.

Providers will use the RPMS EHR GUI to carry out controlled substance medication ordering. The RPMS EHR GUI will also act as the user interface to enter the PIN to unlock the cryptographic token when the provider carries out the multifactor authentication.

Providers shall use a web browser to connect to the Credential Service Provider portal to conduct remote identity proofing and to activate the cryptographic token once it is received.

Cryptographic Token

The cryptographic token is a PIV card or USB-connected device. The device supports PIN operations to lock and unlock the token. The device also contains a certificate store and the capability to conduct certificate operations such as digital signing. The device is accessed using a token driver that is loaded onto the workstation.

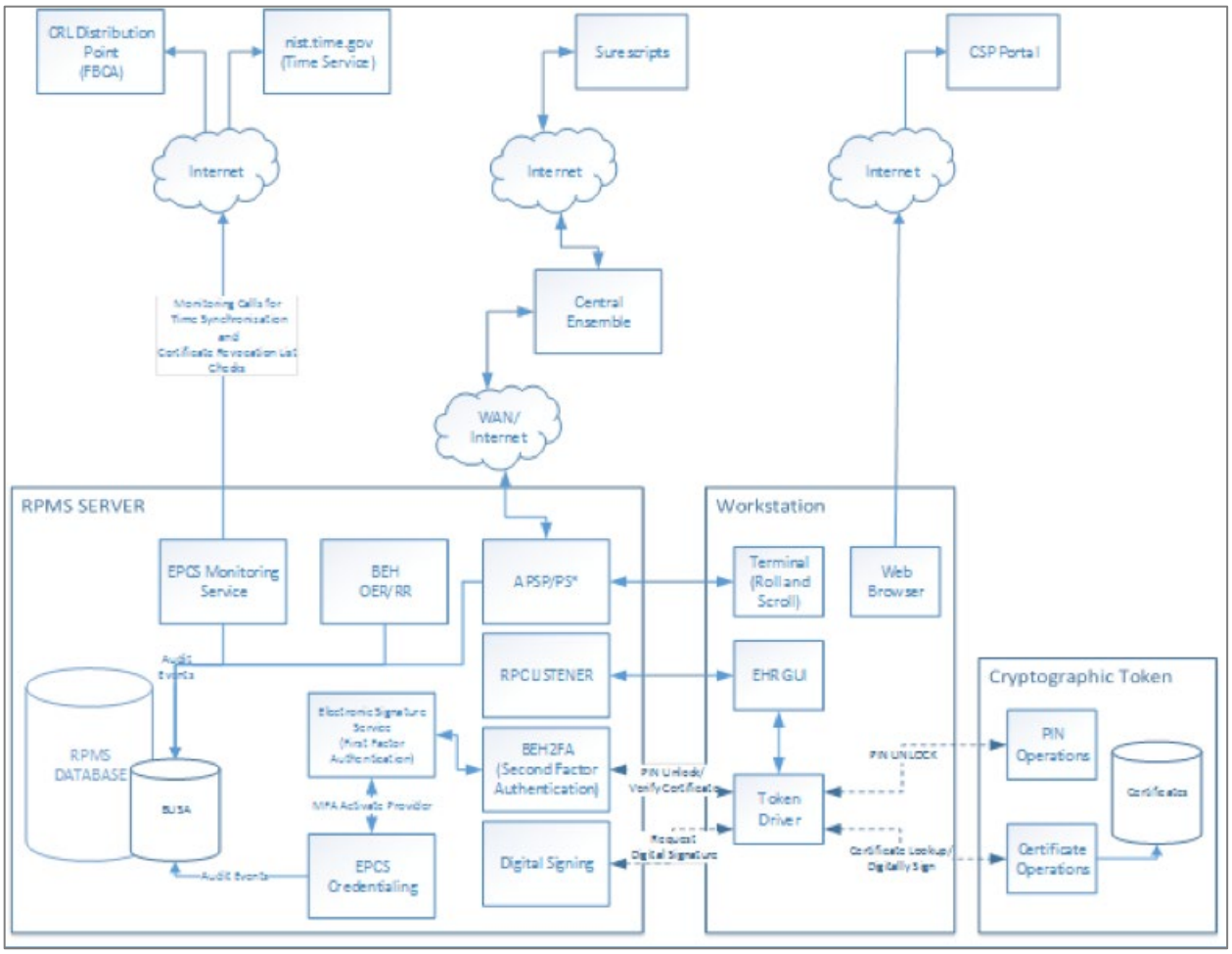

Figure 2-1: EPCS information flow diagram

The cryptographic token in the lower right corner can be one of three devices.

1. An ActivKey SIM with certificates issued by IdenTrust IDG.
2. An ActivKey SIM with certificates issued by ORC ECA.
3. A PIV card with certificates issued through HHS.

The ActivKey SIM is a USB cryptographic token device that combines the smart card reader and smart card. PIV cards would require a separate smart card reader on the workstation. From an application standpoint, all three of the devices operate in an identical fashion. From a Windows device manager point of view the devices look like a smart card reader and smart card pair.

Note:	In further discussions, references to a cryptographic token would apply to both the USB cryptographic token and the PIV smart card reader combination.

2.5.1.2 RPMS EHR Access directly from Workstation

The RPMS EHR application shall be able to access the USB cryptographic token. If the RPMS EHR is running directly from a workstation, the workstation shall have a USB port available to connect the USB token.

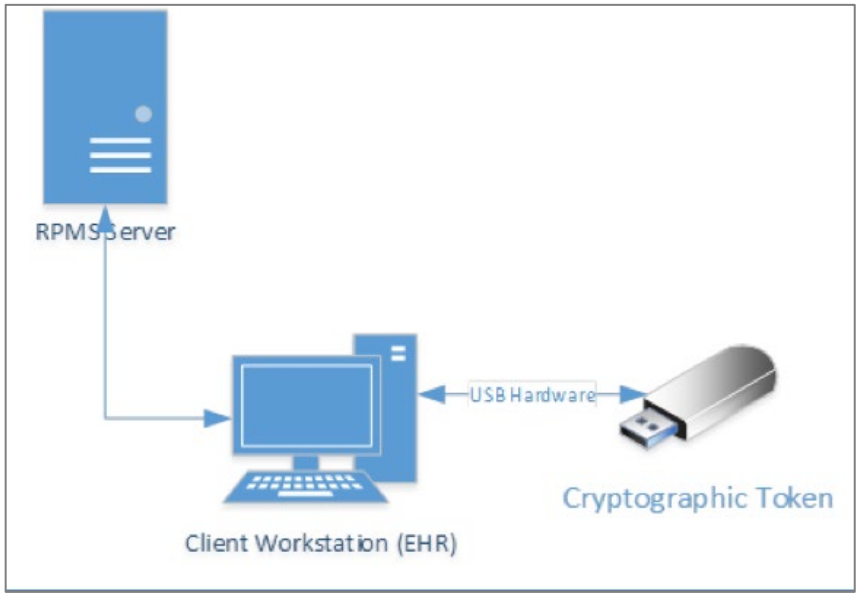

Figure 2-2: RPMS EHR run from a client workstation

2.5.1.3 RPMS EHR Access from Remote Desktop/Thin Client

The RPMS EHR application shall be able to access the USB cryptographic token. If the RPMS EHR is running on a remote desktop from a workstation thin client, the remote desktop the ability to access the certificates on the USB cryptographic token or smart card.

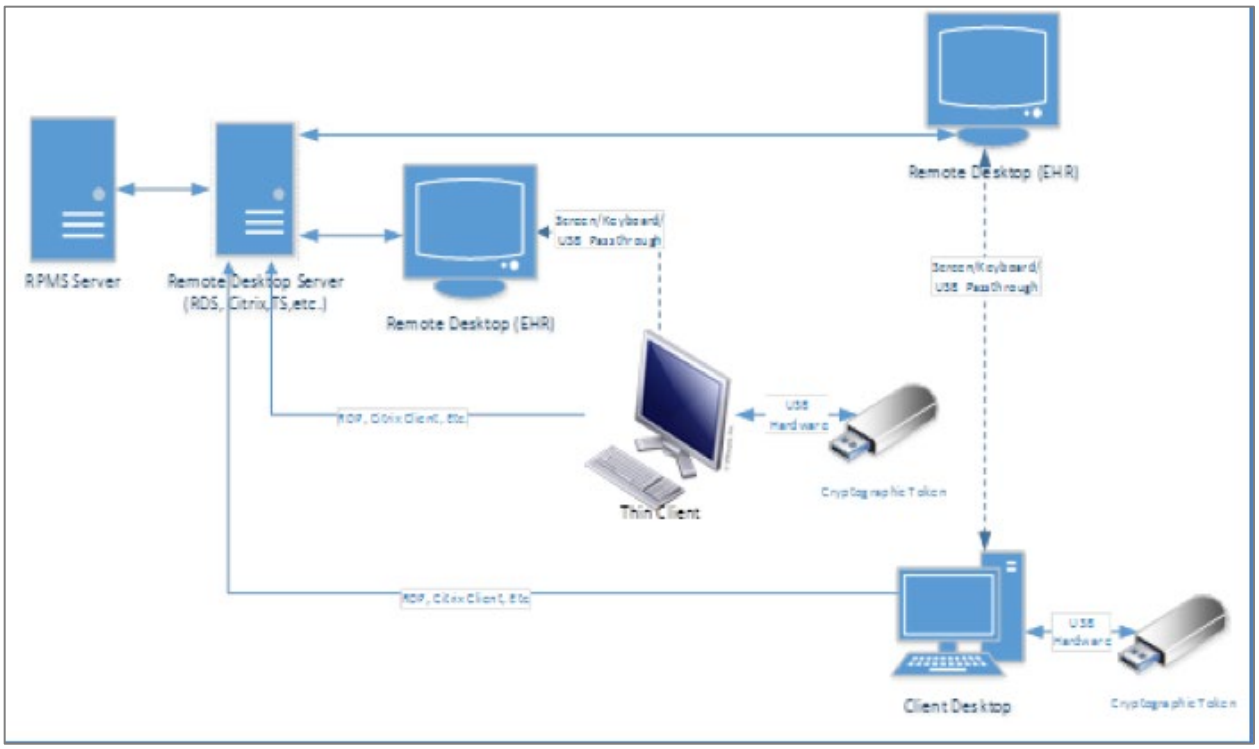

Figure 2-3: EHR run from remote desktop or thin client

2.5.2 RPMS-Related Software

The EPCS requires certain patches to be installed and at a certain patch level prior to installing the EPCS related patches. A site should verify that the following patches are installed and at the appropriate level. Please refer to the *Electronic Prescribing of Controlled Substances (BEPC) Installation Guide and Release Notes* for additional information.

Table 2-2: EPCS installation package requirements

Module	Minimum Version
HL7	Version 1.6 Patch 1006
BUSA	Version 1.0
Kernel	Version 8.0 Patch 1018
EHR	Version 1.1 Patch 24
APSP	Version 1.1 Patch 22
AVA	Version 93.2 Patch 24
BEPR	Version 2.0
PSD	Version 3.0 Patch 67
FileMan	Version 22

The EPCS release contains a number of application patches that need to be installed in order for the EPCS functionality to operate properly. The following patches are all required for EPCS. The patches have been listed according to the order in which they should be installed. Please refer to the Electronic Prescribing of Controlled Substances (BEPC) Installation Guide and Release Notes for additional information.

- E-PRESCRIBING (BEPR) v2.0 Patch 1 (XML): This patch should only be installed if the site is using e-prescribing.
- HEALTH LEVEL SEVEN (HL) v1.6 Patch 1007 (KIDS): A regular KIDS build containing HL7-related changes.
- KERNEL (XU) v8.0 Patch 1019 (KIDS): A KIDS multi-build containing kernel-related changes.
- IHS USER SECURITY AUDIT (BUSA) v1.0 Patch 1 (KIDS): A regular KIDS build containing BUSA-related changes. Includes the install for the EPCS ZEN reporting utility.
- CONTROLLED SUBSTANCES (PSD) v3.0 Patch 23 (KIDS): A KIDS multi-build containing the VA changes to the PSD application.
- IHS PHARMACY MODIFICATIONS (APSP) v7.0 Patch 1023 (KIDS): A regular KIDS build containing pharmacy-related changes.
- RPMS EHR v1.1 Patch 25 (repository updater): This is an install package containing GUI changes for the EHR.
- RPMS EHR v1.1 Patch 25 (KIDS): This is a KIDS multi-build containing order-related changes.
- RPMS EHR v1.1 Patch 25 (EPCS Monitoring Service): This is the install package for the EPCS Monitoring Service. See additional considerations in Section 2.5.3.

The site shall plan for and designate a staging location for the patch files. The designated location shall be accessible from the RPMS instance that will be updated. Additionally, a site should plan out the process to move the patch files to the designated staging location.

The site shall ensure that the RPMS instance has the required patches to install EPCS. The site should plan for time to review the EPCS Installation Guide and the associated patch notes to determine the required patches. The site may consider using the XUQuery utility to determine the current patch levels.

2.5.3 EPCS Monitoring Service

The EPCS Monitoring Service is a Windows service that is primarily used to verify time synchronization and the status of digital signing certificates. There are three considerations a site shall plan for during the installation of the EPCS Monitoring Service.

2.5.3.1 EPCS Monitoring Service Installation Approach

The EPCS Monitoring Service takes into account that more than one RPMS database instance may be running on a server. A single installation of the EPCS Monitoring Service may handle more than one RPMS database where EPCS functionality will be installed. This could be a single site with test and production databases or multiple sites sharing the same server.

The site shall plan for the installation and/or configuration based on one of the three following scenarios:

- The EPCS Monitoring Service needs to be installed and will support only one RPMS database instance with EPCS functionality.
- A new EPCS Monitoring Service is being installed that will support multiple RPMS database instances. The site will want to incorporate into capacity planning to determine how many database instances the service is able to support.
- A new RPMS database instance with EPCS functionality is being added to an existing installation of the EPCS Monitoring Service. Instead of installing the service, the site shall gather the information for the existing service.

2.5.3.2 EPCS Monitoring Service Installation Location

The EPCS Monitoring Service requires a Windows operating system. While it is recommended to run on the same server as the RPMS database instance for Windows RPMS servers, or the associated application server for AIX RPMS servers, this is not mandatory.

If a site intends to run the EPCS Monitoring Service on a different server from the RPMS database server, the site shall plan for the configuration of the connections between the service and the RPMS database server.

2.5.3.3 EPCS Monitoring Service Connection

The server at the site running EPCS Monitoring Service will require Internet access to make two calls.

- The first call is to obtain the current time from time.nist.gov time servers using NTP. Given that time.nist.gov is a global name for multiple servers, the site shall account for the different IP addresses that may be returned.
- The second call is to check the CRL Distribution Points of the issuing Certificate Authority to verify the digital signing certificates are still valid. This call is made over HTTP.

The site shall plan for the Internet proxy servers to use for these connections and the firewall and proxy server configuration changes that will be needed to allow the calls to go through.

2.5.4 Cryptographic Token

The Provider Access Admin role will require a cryptographic USB token or a PIV card to activate a provider for EPCS functionality. Providers will require a cryptographic USB token or a PIV card to conduct the multifactor authentication and digitally sign an electronic controlled substance prescription.

The EPCS functionality has gone through certification using the following credential service providers:

- IdenTrust
- ORC
- PIV cards issued through IHS

A site shall select the vendor it wishes to use. The site shall work with the CSP to set up its portal and determine how the providers will pay for the tokens. Existing issuance processes would be used for PIV cards.

2.6 Communication Approach

Communication to staff is generally best done if it occurs in multiple ways. Communication of EPCS changes should occur via the documentation that will be sent with the software but also through training. Staff should be made aware from the highest levels at the site that this change will be occurring long before the implementation date. Conversely, training should occur as close to implementation as possible.

2.6.1 Acquiring Cryptographic Tokens

The vendors for cryptographic tokens will provide generic documentation that outline how individuals acquire a cryptographic token. Sites will want to consider planning for the customization of the generic documentation. Customization would include the site-specific URL provided by the portal, site branding, and any other site-specific information.

2.7 Data Conversion Approach

While there is not a data conversion associated with this project, the following data activities may be required.

First the drug file must be in a proper state to support prescribing of controlled substances. If controlled substances are not properly designated, the file shall be updated as part of the site preparation.

During implementation, the provider's DEA profiles will be updated and verified. The site shall determine how it wishes to address providers that are not being granted EPCS capabilities to ensure their profiles are in line with the EPCS updates. This activity would need to occur as part of the post-implementation processes.

2.8 Verification and Validation

The site shall plan for the verification and validation of the EPCS application once it is installed.

- IT staff should determine that the software installed correctly.
- IT Staff should determine that the EPCS Monitoring Service is installed and running correctly.
- The EPCS Provider Profile Admin and EPCS Provider Access Admin should verify the credentialing software works.
- Providers should be able to enter orders with two-factor authentication.
- Pharmacists shall test the processing of digitally signed orders.
- EPCS Incident Responder should verify that the incident response reports are properly scheduled and generated.

3.0 Preparation

The Electronic Prescribing of Controlled Substances Implementation Plan Preparation section provides an outline of activities and steps that should be completed prior to actual deployment.

3.1 Roles and Responsibilities

3.1.1 Site Administrator

While other roles may be delegated tasks, the Site Administrator would be the most appropriate resource to carry out or coordinate the activities to establish site connectivity.

3.1.2 Authorizers (Credentialing Office)

One or more individuals shall be assigned the responsibility of making the final determination to authorize a provider to prescribe controlled substances at a facility. This individual will review information gathered by the Primary Authorizer and make a formal authorization determination. The Secondary Authorizer forwards approved providers to the system administration team to conduct provisioning.

3.1.3 Credential Service Provider

A selected credential service provider will be responsible for issuing cryptographic tokens.

3.1.4 EPCS Provider Profile Admin

The EPCS Profile Provider Admin role is responsible for entering the appropriate information in RPMS to grant logical access to EPCS functionality. This role takes the information provided in the authorization and edits the Provider Profile with items such as DEA registration number and allowed drug schedules.

3.1.5 EPCS Provider Access Admin

The EPCS Provider Access Admin activates the logical access that grants the provider EPCS functionality. This role reviews the information provided in the authorization and the entry made by the EPCS Provider Profile Admin. If correct, the EPCS Provider Access Admin uses multifactor authentication to activate the provider for EPCS functionality.

> **Note:** An individual can act as either an EPCS Provider Profile Admin or EPCS Provider Access Admin but cannot act as both for the same provider.

3.1.6 Pharmacy Manager

The Pharmacy Manager provisions pharmacy personnel.

3.1.7 Incident Response Monitors – EPCS

One or more individuals shall be assigned the responsibility for monitoring and responding to the daily EPCS incident report. The EPCS incident report identifies potential security issues related to EPCS activity.

3.1.8 Incident Response Monitors – Pharmacy

One or more individuals shall be assigned the responsibility for monitoring and responding to the daily Pharmacy incident report.

3.1.9 System Authorizer – EPCS

The site shall assign a sponsor or executive that is responsible for reviewing and accepting the certification of the EPCS system. This role is also responsible for signing off that the EPCS implementation was completed in line with the EPCS system certification in order to place the system in operation.

3.1.10 System Authorizer – Pharmacy

The site shall assign a sponsor or executive who is responsible for reviewing and accepting the certification of the Pharmacy system. This role is also responsible for signing off on verification that the EPCS implementation was completed in line with the Pharmacy system certification to place the system in operation.

3.1.11 Information Technology/Site Manager

- Load the software as documented in Section 2.5.2.
- Enable EPCS for the site and appropriate divisions.
- Install and configure software related to two-factor authentication.
- Give the credentialing keys to the appropriate people.
- Give the PSDRPH key to the appropriate people.

3.1.12 Credentialing

- Determine who is responsible for provider tampering.

- Create policies and procedures for dealing with provider tampering.
- Set up providers with proper credentials.

3.1.13 Clinical Applications Coordinator

- Make appropriate changes to the EPCS-related configuration for e-Prescribing.
- Train providers on two-factor authentication.

3.1.14 Pharmacy

- Train pharmacy staff on changes in software.
- Set up rules for order or audit log tampering.

3.2 Workforce Changes

3.2.1 Assign EPCS Provider Profile and Access Admin Roles

Once installed, EPCS does not need to be turned on to start provisioning providers. Provisioning of providers does require that the EPCS Provider Profile Admin and the EPCS Provider Access Admin roles are assigned and provisioned. The provisioning of these two roles is carried out by the Site Administrator. There is also a prerequisite that the EPCS Provider Access Admin has a cryptographic token.

3.2.1.1 Steps

Follow the steps below so that the EPCS Provider Profile Admin and EPCS Provider Access Admin are ready to proceed with credentialing providers once the EPCS application is installed:

- Formally assign and document the EPCS Provider Profile and EPCS Provider Access Roles.
- Authorize individuals holding the EPCS Provider Access Admin role to obtain a cryptographic token to use for multi-factor authentication when activating a provider’s EPCS profile.
- Formally authorize the Site Administrator to provision the individual's assigned roles.
- Initiate the training appropriate for the roles.

> **Note:** If the EPCS Provider Access Admin will also be an EPCS enabled provider:
>
> The same cryptographic token may be used for both purposes. It is not necessary to obtain separate tokens.
>
> Ensure there is at least one other individual assigned the EPCS Provider Access Admin Role. An individual is not able to activate their own EPCS provider profile.

3.2.1.2 Prerequisites

- A site has identified or established the process and procedures it will use to assign the EPCS Provider Profile Admin and EPCS Provider Access Admin Roles and authorize the Site Administrator to provision the accounts.
- A site has selected and established a relationship with a designated Credential Service Provider.

3.2.2 Providers

While the authorization of providers for EPCS can be done after EPCS has been installed, it is recommended to start the authorization process early. Providers should also start the process of obtaining a cryptographic token. This will allow the EPCS Provider Profile Admin and EPCS Provider Access Admin to start provisioning once the EPCS application has been installed. It will also allow providers to process EPCS orders once EPCS has been enabled for the site.

3.2.2.1 Steps

1. Credentialing Office personnel to establish a list of providers that will be EPCS enabled.
2. Credentialing Office personnel formally authorizes provider for EPCS.
3. Credentialing Office personnel authorize provider to obtain a cryptographic token from the designated credential service provider.
4. Authorized providers obtain cryptographic tokens.

> **Note:** While the authorizations have been made, the EPCS Provider Profile Admin and EPCS Provider Access Admin will not act upon them until the EPCS application has been installed.

3.2.2.2 Prerequisites

- A site has identified or established the process and procedures it will use to authorize a provider for EPCS.
- A site has identified or established the process and procedures it will use to authorize the EPCS Provider Profile Admin and EPCS Provider Access Admin to provision a provider for EPCS.
- A site has selected and established a relationship with a designated Credential Service Provider.
- A site has established the process and procedures it will use to authorize a provider to obtain a cryptographic token.

3.3 Employee Transition

- Make employees aware that this change is coming.
- Make sure that everyone that needs two-factor authentication has it ready.
- Provide training.

3.3.1 Acquire Cryptographic Tokens

The site shall acquire a sufficient number of cryptographic tokens to handle the number of providers identified during capacity planning. Additional tokens may also be needed for individuals assigned the Provider Access Admin Role.

If a site is taking the approach of deploying to a test environment prior to deploying to a production environment, the site shall initially acquire sufficient tokens to cover the test deployment. Additional tokens can be acquired prior to deploying to the production environment. The tokens used in the test environment can be used by the same individuals in the production environment.

> **Note:** Tokens cannot be reissued to a different individual. Tokens used during testing can be used by the same individual in production. However, a token issued to an individual during testing cannot be transferred to another individual to use in production.

3.3.2 Training Sessions

The site project management team should start the process for holding and scheduling the training sessions for each of the roles.

Sites should consider training the EPCS Provider Profile Admin and EPCS Provider Access Admin roles during the preparation phase so that they are prepared to provision providers once the EPCS application is installed.

3.4 Business Process

Sites should consider establishing the process and procedures to support the implementation and ongoing operations for EPCS.

3.4.1 Process to Obtain USB Cryptographic Tokens

The process to obtain a PIV will remain the same. The following is for non-federal sites or federal sites that have opted to use the USB cryptographic token as an interim credential.

Once a site has designated the credential service provider it will use to issue cryptographic tokens, the site shall establish the process and procedures to engage the provider or EPCS Provider Access Admin with the credential service provider.

This process should accomplish the following:

- Document the authorization for an individual to acquire a cryptographic token.
- Convey instructions to the individual on how to acquire the cryptographic token. If providers are to purchase their own tokens, this should cover:
  - How to contact the vendor to start the process.
  - Instructions on how to handle payment for the cryptographic token.

Please see the *EPCS Token Provisioning Guide* for additional information.

> **Note:** For other processes referring to this process, a site will want to include a check to determine if the individual already has a cryptographic token. Individuals assigned the EPCS Provider Access Admin Role can use the cryptographic token obtained as an EPCS enabled provider, and vice versa. It is not necessary to obtain a separate cryptographic token for each role.

3.4.2 Process to Authorize EPCS Provider Profile and Access Admins

The site shall identify existing or establish new business processes to authorize the assignment of the EPCS Provider Profile Admin and EPCS Provider Access Admin Roles. This could include the modification of existing Help Desk tickets or the creation of new Help Desk tickets.

The process should accomplish the following:

- Document the assignment of the roles by an appropriate official in the organization.
- Provide authorization for individuals assigned the EPCS Provider Access Admin role to obtain a cryptographic token. (Optional if individual does not already have a cryptographic token.)

- Provide authorization for the Site Administrator to provision the roles in RPMS.

> **Note:** In general, retention periods for the assignment of privileged roles typically starts when an individual relinquishes a role. The site shall look at policies to ensure the assignment records are retained for the appropriate length of time. (See also Section 2.4.12: Compliance Related Planning.)

3.4.3 Process to Authorize a Provider for EPCS

The site shall identify existing or establish new business process to authorize a provider for EPCS functionality. This could include the modification of existing Help Desk tickets or the creation of new Help Desk tickets.

The process should accomplish the following:

- Vetting and authorization for a provider to practice at a facility. This is likely a well-established process. For the purposes of EPCS, the key elements are as follows:
  - Validating the DEA Registration Number or institutional DEA Number (VA Number).
  - Validating the detoxification number (aka, DEA X, NADEAN), if applicable.
  - Establishing the schedules of the controlled substance medications the provider will be allowed to order.
- Authorizing the provider to obtain a cryptographic token and proceed with the Process to Obtain Cryptographic Token.
- Authorize and convey information needed for the EPCS Provider Profile Admin and EPCS Provider Access Admin to enter and activate the designated provider's profile in EPCS. The step has a dependency on the provider obtaining the cryptographic token.

3.5 Technology Requirements

3.5.1 Address any Capacity Issues Identified

With the completion of Capacity Planning, it is possible that short-term or longer-term capacity issues may be identified. Any short-term capacity issues should be addressed prior to proceeding with deployment.

Consider a capacity issue short-term if:

- The issue prevents successful deployment of the EPCS functionality.

- Once in operation, the issue would cause the EPCS functionality to go out of compliance before it could be addressed.

3.5.2 Prepare Site for Selected Tokens

There are steps that a site can do ahead of the formal implementation. These steps prepare the site to use the token selected to carry out two-factor authentication. These steps cover:

1. Preparing the workstations providers and EPCS Provider Access Admins will use to provision their token. (Applicable to USB cryptographic tokens.)
2. Preparing the workstations the EPCS Provider Access Admins will use to credential providers.
3. Preparing the workstations the providers will use to digitally sign controlled substance medication orders.

The process to acquire different tokens and to prepare a site for their use addressed in the EPCS Tokens Guide.

3.6 Data Conversion

No data conversion is required. Sites should update the drug file and ensure that controlled substances are properly designated as described in the Pharmacy Data Management documentation.

3.7 Implementation Readiness Verification

The following checklist items will help determine if a site is ready to start implementation.

3.7.1 Site Connection Readiness

The EPCS Monitoring Service is able to connect to the NIST time services and to the certificate revocation lists of the selected credential service provider.

3.7.2 Site Readiness

- Capacity issues have been identified and resolved.
- The EPCS Provider Profile Admin and EPCS Provider Access Admin have been designated.
- The site has selected a Credential Service Provider.
- The drug file has been reviewed and brought into compliance.
- Release files have been obtained and staged.

- Training sessions have been established.
- Process for individuals to obtain tokens is in place.
- Personnel have been notified of pending change.

3.7.3 Surescripts Readiness

If a site will connect to Surescripts prior to EPCS, the Surescripts implementation is completed and verified.

4.0 Implementing

The Electronic Prescribing of Controlled Substances Implementation Plan provides an outline of activities and steps that are necessary to ensure that the EPCS product is available for use by end-users as planned.

4.1 Roles and Responsibilities

> **Note:** While this section appears similar to the previous Roles and Responsibilities, this section is highlighting the actual assignment of a role to an individual and have them start carrying out the associated responsibilities.

4.1.1 Authorizer (Credentialing Office)

One or more individuals shall be assigned the responsibility of gathering and reviewing credentials of a provider. This is to make a determination on whether to authorize the ability to prescribe controlled substances at a facility.

4.1.2 Secondary Authorizer (Credentialing Office)

One or more individuals shall be assigned the responsibility of making the final determination to authorize a provider to prescribe controlled substances at a facility. This individual will review information gathered by the Primary Authorizer and make a formal authorization determination. The Secondary Authorizer forwards approved providers to the system administration team to conduct provisioning.

4.1.3 Credential Service Provider

The site shall designate a credential service provider to issue tokens.

4.1.4 EPCS Provider Profile Admin

The EPCS Provider Profile Provider Admin role is responsible for entering the appropriate information in RPMS to grant logical access to EPCS functionality. This role takes the information provided in the authorization and edits the Provider Profile with items such as DEA registration number and allowed drug schedules.

4.1.5 EPCS Provider Access Admin

The EPCS Provider Access Admin activates the logical access that grants the provider EPCS functionality. This role reviews the information provided in the authorization and the entry made by the EPCS Provider Profile Admin. If correct, the EPCS Provider Access Admin uses multifactor authentication to activate the provider for EPCS functionality.

> **Note:** An individual can act as either an EPCS Provider Profile Admin or Provider Access Admin but cannot act as both for the same provider.

4.1.6 Pharmacy Authorizer (Pharmacy Manager)

This is the pharmacy individual that is capable of authorizing other pharmacy personnel for EPCS.

4.1.7 Incident Response Monitors – EPCS

One or more individuals shall be assigned the responsibility for monitoring and responding to the daily EPCS incident report.

4.1.8 Incident Response Monitors – Pharmacy

One or more individuals shall be assigned the responsibility for monitoring and responding to the daily Pharmacy incident report.

4.1.9 System Authorizer – EPCS

The site shall assign a sponsor or executive that is responsible for reviewing and accepting the certification of the EPCS system. This role is also responsible for signing off that the EPCS implementation was completed in line with the EPCS system certification in order to place the system in operation.

4.1.10 System Authorizer – Pharmacy

The site shall assign a sponsor or executive that is responsible for reviewing and accepting the certification of the Pharmacy system. This role is also responsible for signing off that the EPCS implementation was completed in line with the Pharmacy system certification in order to place the system in operation.

4.1.11 Information Technology/Site Manager

- Load the software as documented in Section 2.5.2.
- Enable EPCS for the site and appropriate divisions.
- Install and configure Two Factor Authentication related software.
- Give the credentialing keys to the appropriate people.
- Give the PSDRPH key to the appropriate people.

4.1.12 Credentialing

- Determine who is responsible for monitoring provider tampering.

- Create policies and procedures for dealing with provider tampering.
- Set up providers with proper credentials.

4.1.13 Clinical Applications Coordinator

- Make appropriate changes to EPCS related configuration for e-prescribing.
- Train providers on two-factor authentication.

4.1.14 Pharmacy

- Train pharmacy staff on changes in software.
- Set up rules for order or audit log tampering.

4.2 Workforce Changes

- Credentialing users will now need to finish the process by using the RPMS EHR Credentialing component. This is a change in workflow.
- What happens when a provider's credentials fail and who is responsible for investigating this problem is a change?

4.2.1 Providers

- Signing a controlled substance order will take an extra step.
- The user must have the second factor (USB cryptographic token) with them when ordering or the order may be delayed.

While this may increase work time for ordering a bit, especially at first, the amount of time should decrease as users become familiar with the process.

4.2.2 Pharmacy

- Pharmacy users will notice an extra step of needing to verify a hardcopy-controlled substance request if the provider is not EPCS enabled.
- Pharmacists shall verify all digitally signed orders for pharmacy users who do not have the PSDRPH key. This key is not intended for pharmacy technicians.
- Pharmacists shall handle auto-discontinued orders if the order hash has been tampered.
- Pharmacists may be called in for investigation on what happened when an order or the controlled substance audit log has been tampered.
- Pharmacy shall run more reports to meet DEA regulations on controlled substances.

4.3 Employee Transition

There are two stages of employee transition. The first transition occurs once the EPCS functionality has been installed, but not turned on. The second transition occurs when the EPCS functionality is turned on for the site.

4.3.1 EPCS Installed but not Turned on

If a site has not carried out the process to authorize providers and have providers obtain their cryptographic tokens, that process should be completed at this time (Sections 3.2.2 and 3.3.1).

Once providers have been authorized and acquired their tokens, the EPCS Provider Profile Admins and EPCS Provider Access Admins can process the authorizations and update and activate the provider's EPCS profile. This will allow a provider to electronically order controlled substance medications once EPCS is turned on for the site. (See the *EPCS Configuration Manual*).

4.3.2 EPCS Turned On

Once EPCS is turned on, providers will be required to use multi-factor authentication to digitally sign controlled substance medication orders. Sites will want to ensure that appropriate communications and training have been carried out so that providers are prepared for the change.

4.3.2.1 Multi-Divisional Sites

For multi-divisional sites, sites should consider a staged implementation of EPCS for the different divisions. If a site chooses to stage turning on EPCS, the main division shall be turned on before EPCS is turned on for any of the child divisions.

4.3.2.2 Independent Site Acting as a Child Division of another site

If an independent site is operating as a division under another site as opposed to operating its own RPMS instance, the staging mentioned in the previous section apply. The main division would have to have EPCS installed and turned on before turning on EPCS for the independent site. Otherwise, the independent site shall establish its own RPMS instance.

4.4 Business Process

- Determine who will handle provider credentialing.
- Determine who will be responsible for monitoring the tampering of provider credentials.
- Determine who will run the required DEA reports on controlled substances.

- Determine who will be responsible for security breaches.
- Determine who will be responsible for investigating order tampering.
- Determine who will be responsible for audit log tampering.
- Tailor sample forms.
- Dry run workflows:
  - Provider credentialing changes
  - Provisioning multifactor authenticators
  - Provisioning EPCS access
  - Pharmacy: Electronic signing for in-house paper prescriptions
  - EPCS: Daily Incident Response Report review
  - Pharmacy: Daily Incident Response review
  - Pharmacy: Daily prescription reviews
- Credentialing Office: Authorizing providers.
- Credentials Issuance: one-time password (OTP).
- Granting Logical Access.
- Termination.
- Renewal.
- System Monitoring.
- Incident Response.

4.5 Technology Requirements

4.5.1 Install EPCS Applications

Sites will proceed with the installation of the EPCS Patches and EPCS Monitoring Services. These processes are addressed in the *EPCS Installation Guide* and *EPCS Configuration Guide*.

- Install prerequisite patches.
- Install the releases as documented in Section 2.5.2.
- Configure site settings:
  - Establish Mailman mail groups.
  - Enable Sites/Divisions
- Establish Automated Tasks:
  - Profile integration check.

  - Backup/archive.
  - Report delivery.
  - Certificate revocation checks.
- XPAR Parameters.
- Credential Providers for EPCS.

4.5.2 Prepare Workstations to Support EPCS

If the site did not carry out the steps to prepare the designated workstation noted in Section 3.5.3 Prepare Site for Selected Tokens, the following will need to be completed:

1. Prepare the workstations providers and EPCS Provider Access Admins will use to provision their token. (Applicable to USB cryptographic tokens.)
2. Prepare the workstations the EPCS Provider Access Admins will use to credential providers.
3. Prepare the workstations the providers will use to digitally sign controlled substance medication orders.

The process to acquire different tokens and to prepare a site for their use addressed in the EPCS Tokens Guide.

4.6 Data Conversion

There is no data conversion.

Users should be off the system when the software is loaded.

It is recommended that all users are off the system and that pharmacy order processing is current when the site is turned on for EPCS to eliminate issues related to processing of controlled substances. This could be after hours for an outpatient site or in the evening for an inpatient site.

After the software is installed, all controlled substance orders will require a hardcopy until which time the facility has been EPCS enabled and the ordering provider credentialed.

4.7 Verification and Validation

If the site has a training environment, the patch should be installed there first and validated with a small number of users.

When the patch is installed, the site will be turned off for EPCS. Everything should function the way it is currently for medication ordering except:

- All controlled substances for non-EPCS providers will now require a hardcopy order to be sent to pharmacy. New print formats shall be installed to follow the rules for controlled substances.
- Providers will be informed they need to send a hardcopy to pharmacy.
- Pharmacy will be required to electronically sign that they have this hardcopy before processing the order.
- Sites can choose to either setup all providers and then turn on the site for everyone or turn the site on and then add providers one at a time depending on how the providers have been trained.
- Credentialing users will need special keys to perform the functions.
- Pharmacy shall assign the PSDRPH key to pharmacists only to be able to release controlled substances.

5.0 Transitioning

For providers and pharmacists, the changes will be evident as soon as the software is installed, even if EPCS is not enabled for the site immediately.

If EPCS is not enabled immediately, providers shall revert to paper prescriptions of controlled substances until the site is enabled. Until the site or division enables EPCS, any controlled substance orders will require a hardcopy of the order to be signed with ink.

Providers can be individually designated as an EPCS provider.

Sending controlled substance prescriptions to Surescripts will be handled by the e-Prescribing Implementation Group. Providers shall be authorized by Surescripts to send EPCS prescriptions.

5.1 Training

Role-based training is available for users and administrators of the EPCS applications. This training will be offered as both live and recorded sessions. The training sessions will be scheduled as part of the rollout activities. Sites should incorporate this training into onboarding activities for future staff joining the site.

5.1.1 Pharmacist Training

- Assignment of the PSDRPH security key.
- What the pharmacist can and cannot do with the new key.
- What a digitally signed order looks like and how to process it.
- How to process a hardcopy of controlled substance for a non-EPCS provider.
- What happens when an order has been tampered?
- New reports and who should receive them.

5.1.2 Provider Training

- How to use the USB cryptographic token.
- How to process/sign two-factor authentication orders.
- What the new warning messages mean.

5.1.3 Site Administrator

- General installation notes of EPCS components.

- Overview of new keys and menus.

5.1.4 Credentialing Office Personnel

General process and procedure for authorizing a provider for EPCS.

5.1.5 CS Provider Profile Admin

Steps to create and modify a provider's EPCS profile.

5.1.6 EPCS Provider Access Admin

- Steps to verify and activate a provider's EPCS profile.
- Steps to manage cryptographic token used in multi-factor authentication to activate a provider's profile.

5.1.7 EPCS Incident Responder

- How to review and respond to daily EPCS Incident Response reports.
- How to review EPCS audit logs using the EPCS Reporting tool.

5.1.8 EPCS Incident Response Group

Awareness of expectations for individual that receive EPCS incident response notifications.

5.1.9 EPCS Auditor

How to review EPCS audit logs using the EPCS Reporting tool.

5.2 Technical Document

Please refer to the Technical Manual(s) for specific technical changes to the EPCS applications.

5.3 Operations and Maintenance

Sites should now be ready to carry out the ongoing operations and maintenance identified in the previous sections.

5.3.1 Cryptographic Tokens

The site shall operationalize the ongoing management of tokens and certificates. federal site utilizing PIV will continue to use established processes.

5.3.1.1 Managing Token Inventory

If a site has selected ORC as the credential service provider and opts to bulk buy tokens to issue to providers, the site shall establish process and procedures for storing the blank tokens and for storing the activation information that would be given to a provider. The processes should include maintaining the inventory and periodic checks to verify tokens are accounted for as they are issued.

If a site has selected IdenTrust as the credential service provider and opts to bulk buy vouchers to issue providers, the site shall establish process and procedures for storing the vouchers. The processes should include maintaining the inventory and periodic checks to verify vouchers are accounted for as they are issued.

5.3.1.2 Contingency Planning for Emergency Tokens

Due to the issuance process and DEA requirement for tying a token to an individual, keeping a few spare tokens to use in case a token is lost or forgotten is not feasible. An individual would need to go through the process of obtaining a new token through the selected credential service provider.

The initial fallback is to revert to paper prescriptions until a provider finds or replaces the token. A potential alternative is to have the providers obtain two cryptographic tokens. Keep one for primary use and keep the other in a secure location.

Regardless of whether using a new token or a backup token, the provider shall work with the EPCS Provider Profile Admin and EPCS Provider Access Admin to register and activate the new token in the provider's EPCS profile.

This is also addressed in Section 2.4.9 Contingency Planning.

5.3.1.3 Multi-Site Providers

If a site uses a provider that works at multiple sites, it may not be necessary for the provider to obtain a new cryptographic token. If a provider was issued a token for use at a different site, the same token may be registered and used at the site. The process for credentialing a multi-site provider should include checks to determine if the provider already has a cryptographic token that was issued by one of the approved credential service providers.

5.3.1.4 Revoking Cryptographic Tokens

There are two scenarios where a site should consider revoking a provider's cryptographic token. Revoking a token involves contacting the credential service provider and notifying them the cryptographic token cannot be used.

Incident Response Scenario

In the event a token is compromised, lost, or stolen and deemed not recoverable, the token should be revoked. A site's incident response plan should be activated, and the credential service provider notified to revoke the token. See Section 2.4.8 Incident Response.

Separation from Organization Scenario

The cryptographic tokens are not transferrable or reusable. If a site has deemed that it will retrieve the token from a provider when they leave the organization, the token shall be revoked. The token is no longer in the possession of the individual it was tied to and needs to be rendered unusable.

5.3.2 Patching

The site shall ensure it is keeping up on EPCS patches. It is possible that a patch is required to keep the EPCS application in compliance. Failure to patch the EPCS application in a timely manner could result in the need to disable EPCS until the patches are installed.

5.3.3 Incident Response Management

DEA regulations require that the incident response reports be monitored daily. The site shall be prepared to carry out that monitoring and address any incidents that are identified.

Glossary

Audit Trail

Record showing who has accessed an information technology application and what operations the user performed during a given period.

Authentication

Verifying the identity of the user as a prerequisite to allowing access to the information application.

Authentication Protocol

Well-specified message exchange process that verifies possession of a token to remotely authenticate a person to an application.

Cache

Download and store information on a local server or hard drive.

Certification Policy

Named set of rules that sets forth the applicability of the specific digital certificate to a particular community or class of application with common security requirements.

Certification Revocation List

List of revoked, but unexpired certificates issued by a certification authority.

Certification Authority

Organization that is responsible for verifying the identity of applicants, authorizing and issuing a digital certificate, maintaining a directory of public keys, and maintaining a Certificate Revocation List.

Credential

Object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.

Credential Service Provider

Trusted entity that issues or registers tokens and issues electronic credentials to individuals. The CSP may be an independent third party or may issue credentials for its own use.

Digital Certificate

Data record that, at a minimum:

- Identifies the certification authority issuing it;

- Names or otherwise identifies the certificate holder;
- Contains a public key that corresponds to a private key under the sole control of the certificate holder;
- Identifies the operational period;
- Contains a serial number and is digitally signed by the certification authority issuing it.

Digital Signature

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. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed.

Digitally Sign

Affix a digital signature to a data file.

Electronic Prescription

Prescription that is generated on an electronic application and transmitted as an electronic data file.

Electronic Prescription Application

Entity that develops or markets electronic prescription software either as a stand-alone application or as a module in an electronic health record application.

Electronic Signature

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.

FIPS

Federal Information Processing Standards. These federal standards, as incorporated by reference in § 1311.08 of this chapter, prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, etc.

FIPS 140-2

As incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ‘‘Security Requirements for Cryptographic Modules,’’ a federal standard for security requirements for cryptographic modules.

FIPS 180-2

As incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ‘‘Secure Hash Standard,’’ a federal secure hash standard.

FIPS 180-3

As incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ‘‘Secure Hash Standard (SHS),’’ a federal secure hash standard.

FIPS 186-2

As incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ‘‘Digital Signature Standard,’’ a federal standard for applications used to generate and rely upon digital applications used to generate and rely upon digital signatures.

FIPS 186–3

As incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ‘‘Digital Signature Standard (DSS),’’applications used to generate and rely upon digital signatures.

Hard Token

Cryptographic key stored on a special hardware device (e.g., a PDA, cell phone, smart card, USB drive, one-time password device) rather than on a general-purpose computer.

Identity Proofing

Process by which a credential service provider or certification authority validates sufficient information to uniquely identify a person.

Installed Electronic Prescription Application

Software that is used to create electronic prescriptions and that is installed on a practitioner’s computers and servers, where access and records are controlled by the practitioner.

Installed Pharmacy Application

Software that is used to process prescription information and that is installed on a pharmacy’s computers or servers and is controlled by the pharmacy.

Key Pair

Two mathematically related keys having the properties that:

- One key can be used to encrypt a message that can only be decrypted using the other key, and

- Even knowing one key, it is computationally infeasible to discover the other key

NIST SP 800–63–1

As incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled ‘‘Electronic Authentication Guideline,’’ a federal standard for electronic authentication.

Paper Prescription

Prescription created on paper or computer generated to be printed or transmitted via facsimile that meets the requirements, including a manual signature.

Password

Secret, typically a character string (letters, numbers, and other symbols), that a person memorizes and uses to authenticate his/her identity.

Pharmacy Application Provider

Entity that develops or markets software that manages the receipt and processing of electronic prescriptions.

Private Key

Key of a key pair that is used to create a digital signature.

Public Key

Key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair.

Public Key Infrastructure

Structure under which a certification authority verifies the identity of applicants; issues, renews, and revokes digital certificates; maintains a registry of public keys; and maintains an up-to-date certificate revocation list.

Resource and Patient Management System

A decentralized integrated solution for management of both clinical and administrative information in these healthcare facilities. Flexible hardware configurations, over 50 software applications, and network communication components combine to create a comprehensive clinical, financial, and administrative solution; a solution that can stand alone or function in concert with other components as needed. Professionals in American Indian, Alaska Native, and private sector health facilities use RPMS every day to efficiently manage programs, maximize revenue generation, and most important, to provide high-quality care for patients.

Signing Function

Keystroke or other action used to indicate that the practitioner has authorized for transmission and dispensing a controlled substance prescription. The signing function may occur simultaneously with or after the completion of the two-factor authentication protocol.

Token

Something a person possesses and controls (typically a key or password) used to authenticate the person's identity

Acronym List

Acronym	Meaning
2FA	Two Factor Authentication
AI	American Indian
AN	Alaska Native
CA	Certification Authority
CAC	Clinical Application Coordinator
CRL	Certification Revocation List
CS	Controlled Substance
CSP	Credential Service Provider
DEA	Drug Enforcement Administration
EHR	Electronic Health Record
EPCS	Electronic Prescribing of Controlled Substances
FIPS	Federal Information Processing Standard
IHS	Indian Health Service
IT	Information Technology
ITU (aka I/T/U)	IHS/Tribal/Urban
HSM	Hardware Security Module
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIT	Office of Information Technology
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RPMS	Resource and Patient Management System
SESS	Software Engineering Support Services
SPI	Surescripts Provider Identifier
USB	Universal Serial Bus

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: https://www.ihs.gov/helpdesk/

Email: support@ihs.gov