Pharmacy Operational Updates (POU)

PSO*7.0*529

Deployment, Installation, Back-Out, and Rollback Guide

April 2022

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
04/06/2022	1.0	Initial Version	Liberty IT Solutions

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Dependencies 1
1.3 Constraints 1
2 Roles and Responsibilities 2
3 Deployment 3
3.1 Timeline 3
3.2 Site Readiness Assessment 3
3.2.1 Deployment Topology (Targeted Architecture) 3
3.2.2 Site Information (Locations, Deployment Recipients) 4
3.2.3 Site Preparation 4
3.3 Resources 4
3.3.1 Hardware 4
3.3.2 Software 4
3.3.3 Communications 4
3.3.3.1 Deployment/Installation/Back-Out Checklist 4
4 Installation 5
4.1 Pre-installation and System Requirements 5
4.2 Platform Installation and Preparation 5
4.3 Download and Extract Files 5
4.4 Database Creation 5
4.5 Installation Scripts 5
4.6 Cron Scripts 5
4.7 Access Requirements and Skills Needed for the Installation 5
4.8 Installation Procedure 5
4.9 Installation Verification Procedure 7
4.10 System Configuration 7
4.11 Database Tuning 7
5 Back-Out Procedure 7
5.1 Back-Out Strategy 7
5.2 Back-Out Considerations 8
5.2.1 Load Testing 8
5.2.2 User Acceptance Testing 8
5.3 Back-Out Risks 8
5.4 Authority for Back-Out 8
5.5 Back-Out Procedure 8

5.6 Back-out Verification Procedure 10
6 Rollback Procedure 10
6.1 Rollback Considerations 10
6.2 Rollback Criteria 10
6.3 Rollback Risks 10
6.4 Authority for Rollback 10
6.5 Rollback Procedure 10
6.6 Rollback Verification Procedure 10

1 Introduction

This document describes how to install the Pharmacy Operational Updates (POU) project's VistA Patch PSO*7.0*529, as well as how to backout the patch and rollback to a previous version or data set. This patch, in conjunction with Outpatient Pharmacy patch PSO*7.0*529, implements enhancements to VistA Drug Enforcement Agency (DEA) functionality. This patch primarily contains updates to data dictionaries that store DEA related information.

1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the PSO*7.0*529 patch will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2 Dependencies

The following VistA patches must be installed at the site:

- PSO*7.0*630
- XU*8.0*688

1.3 Constraints

This patch is intended to be installed in a fully patched Veterans Health Information Systems and Technology Architecture (VistA) system.

2 Roles and Responsibilities

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	VA OIT, VA OIT Health Product Support, and PMO (Liberty)	Deployment	Plan and schedule deployment.	Planning
2	Health Product Support and Field Operations	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Planning
3	Field Testing (Initial Operating Capability-IOC), Health Product Support Testing & Veteran-Focused Integrated Process (VIP) Release Agent Approval	Deployment	Test for operational readiness	Testing
4	Health Product Support and Field Operations	Deployment	Execute deployment	Deployment

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
5	Individual Veterans Administration Medical Centers (VAMCs)	Installation	Plan and schedule installation	Deployment
6	Facility Chief Information Officer (CIO) and OIT support, which may be local or regional	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)	Deployment
7	VA OIT, VA OIT Product Support, and the Liberty Development Team	Post Deployment	Hardware, Software and System Support	Warranty

3 Deployment

The deployment is planned as a national general availability release. The scheduling of test/mirror installs, testing, and the deployment to production will be at the sites' discretion.

A national release is planned after testing has been successfully completed at initial operating capability (IOC) test sites.

Deployment will be performed by the local or regional OIT staff and supported by team members from these organizations: Field Operations (FO) and Enterprise Operations. Other teams may provide additional support.

3.1 Timeline

The deployment and installation is scheduled to run for 31 days, as depicted in the master deployment schedule for Pharmacy Operational Updates Optional Release 2.

Table 2:Timeline

Task	Start	Finish
National Release	4/15/22	4/15/22
Compliance Period	4/18/22	5/16/22

3.2 Site Readiness Assessment

This section discusses the locations that will install patch PSO*7.0*529.

3.2.1 Deployment Topology (Targeted Architecture)

This release is a patch intended for installation at local sites.

Health Product Support Patch Release of Products and Patches Guide: Health Product Support Release of Products and Patches Guide.

3.2.2 Site Information (Locations, Deployment Recipients)

The IOC sites are:

- Ann Arbor VA Medical Center (Ann Arbor, MI)
- Spark M. Matsunaga VA Medical Center (Honolulu, HI)

Upon national release, all VAMCs are expected to install this patch prior to or on the compliance date. The software will be distributed in Forum.

3.2.3 Site Preparation

The patch does not require any site preparations other than the prerequisite patch installations as described in the Patch Description and in the National Patch Module (NPM) in Forum.

3.3 Resources

The Pharmacy patch PSO*7.0*529 is a VistA patch and does not require any special or specific resources other than an existing and functional VistA system.

3.3.1 Hardware

There is no specific hardware required other than that which already hosts the VistA system. This is a software enhancement that will not require additional hardware.

3.3.2 Software

There is no specific software required other than that which already hosts the VistA system.

3.3.3 Communications

When VistA patches are nationally released from the Forum NPM, the patch is automatically sent to the targeted VistA systems nationwide. When VistA patches are installed at a site, a notification is sent back to the NPM to track which sites have and have not installed a patch. This is part of the standard VistA patch notifications and communications protocols.

3.3.3.1 Deployment/Installation/Back-Out Checklist

The Release Management team will deploy the patch PSO*7.0*529, which is tracked in the NPM in Forum, nationally to all VAMCs. Forum automatically tracks the patches as they are installed in the different VAMC production systems as described in the previous section. One can run a report in Forum to identify when the patch was installed in the VistA production at each site, and by whom. A report can also be run, to identify which sites have not installed the patch in their VistA production system as of that moment in time.

Therefore, this information does not need to be manually tracked. Table 3 is included below if manual tracking is desired and because it is part of the VIP document template.

Table 3: Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual Who Completed Task
Deploy	TBD	TBD	TBD

Activity	Day	Time	Individual Who Completed Task
Install	TBD	TBD	TBD
Back-Out	TBD	TBD	TBD

4 Installation

4.1 Pre-installation and System Requirements

This product is a VistA patch. The only pre-installation and system requirements for deployment and installation of this patch are the prerequisite patches which need to be installed before this patch can be installed.

4.2 Platform Installation and Preparation

This product is a VistA patch. Sites should install patches into the test/mirror/pre-prod accounts before the production account as is the normal VistA patch installation standard convention. When installing any VistA patch, sites should utilize the option "Backup a Transport Global" in order to create a backup message of any routines exported with this patch. Post-installation checksums are found in the Patch Description and in Forum NPM.

4.3 Download and Extract Files

Download and extract files are not applicable for this VistA patch.

4.4 Database Creation

Database creation is not applicable for this VistA patch.

4.5 Installation Scripts

Installation scripts are not applicable for this VistA patch.

4.6 Cron Scripts

Cron scripts are not applicable for this VistA patch.

4.7 Access Requirements and Skills Needed for the Installation

To install this VistA patch, the patch installer must be an active user on the VistA system and have access to the VistA menu option "Kernel Installation & Distribution System" [XPD MAIN] and have VistA security keys XUPROG and XUPROGMODE. Knowledge on how to install VistA patches using the items on this menu option is also a required skill.

4.8 Installation Procedure

This patch may be installed with users on the system although it is recommended that it be installed during non-peak hours to minimize potential disruption to users. This patch should take less than 5 minutes to install.

1. Choose the PackMan message containing this build. Then select the INSTALL/CHECK MESSAGE PackMan option to load the build.
2. From the Kernel Installation and Distribution System Menu, select the Installation Menu. From this menu:
    a. Select the Verify Checksums in Transport Global option to confirm the integrity of the routines that are in the transport global. When prompted for the INSTALL NAME enter the patch or build name PSO*7.0*529.
    b. Select the Backup a Transport Global option to create a backup message. You must use this option and specify what to backup; the entire Build or just Routines. The backup message can be used to restore the routines and components of the build to the pre-patch condition.
        i. At the Installation option menu, select Backup a Transport Global
        ii. At the Select INSTALL NAME prompt, enter build PSO*7.0*529.
        iii. When prompted for the following, enter "R" for Routines or "B" for Build.

            Select one of the following:

            B Build
            R Routines

            Enter response: Build

        iv. When prompted "Do you wish to secure this message? NO//", press <enter> and take the default response of "NO".
        v. When prompted with, "Send mail to: Last name, First Name", press <enter> to take default recipient. Add any additional recipients.
        vi. When prompted with "Select basket to send to: IN//", press <enter> and take the default IN mailbox or select a different mailbox.

    c. You may also elect to use the following options:
        i. Print Transport Global - This option will allow you to view the components of the KIDS build.
        ii. Compare Transport Global to Current System - This option will allow you to view all changes that will be made when this patch is installed. It compares all of the components of this patch, such as routines, DDs, templates, etc.
    d. Select the Install Package(s) option and choose the patch to install.
        i. If prompted 'Want KIDS to Rebuild Menu Trees Upon Completion of Install? NO//', answer NO.

ii. When prompted 'Want KIDS to INHIBIT LOGONs during the install? NO//', answer NO.

iii. When prompted 'Want to DISABLE Scheduled Options, Menu Options, and Protocols? NO//', answer NO.

1. When prompted 'Enter protocols you wish to mark as 'Out Of Order':', press the Enter key.
2. When prompted 'Delay Install (Minutes): (0 - 60): 0//', answer 0.^

4.9 Installation Verification Procedure

ATTENTION: The DEA migration process performed by the post-install routine may take up to 24 hours to complete. This time will vary depending on the number of entries in the NEW PERSON file containing DEA numbers. This process should have no effect on end users.

Verify completed installation by comparing the post-install routine checksums against the published checksums in the Patch Description and in Forum NPM.

Another verification method is to ensure that the build components as listed in the Patch Description have been correctly installed onto the target VistA system

4.10 System Configuration

System configuration is not applicable for this VistA patch.

4.11 Database Tuning

Database tuning is not applicable for this VistA patch.

5 Back-Out Procedure

Back-Out pertains to a return to the last known good operational state of the software and appropriate platform settings.

5.1 Back-Out Strategy

Prior to installing the updated KIDS package, the site/region should have saved a backup of the routines in a mail message using the Backup a Transport Global [XPD BACKUP] menu option. The message containing the backed-up routines can be loaded with the "Xtract PackMan" function at the Message Action prompt. The PackMan function INSTALL/CHECK MESSAGE is then used to install the backed-up routines onto the VistA system.

The development team recommends that sites log a ticket if it is a nationally released patch; otherwise, the site should contact the Enterprise Program Management Office (EPMO) directly for specific solutions to their unique problems.

Although it is unlikely due to care in collecting approved requirements, Software Quality Assurance (SQA) review and multiple testing stages (Unit testing, Component Integration Testing, User Acceptance Testing) a back-out decision due to major issues with this patch could occur during site Mirror Testing, Site Production Testing or after National Release to the Field. The strategy would depend on during which of these stages the decision is made. If during Site Production Testing, unless the patch produces catastrophic problems, the normal VistA response would be for a new version of the test patch correcting defects to be produced, retested and upon successfully passing development team testing would be resubmitted to the site for testing. If the defects were not discovered until after national release but during the 30 days support period, a new patch will be entered into the National Patch Module on Forum and go through all the necessary milestone reviews etc. as an emergency patch.

5.2 Back-Out Considerations

It is necessary to determine if a back-out of the patch PSO*7.0*529 is needed, or if issues may be adequately addressed via a new version of the patch (if prior to national release) or through a subsequent patch (if after national release).

A back-out of the patch will require a new test version (if prior to national release) or a subsequent patch (if after national release). If the back-out is post-release of patch PSO*7.0*529, patch PSO*7.0*529 should be assigned status of "Entered in Error" in Forum's NPM.

5.2.1 Load Testing

Load Testing is not applicable for this VistA patch.

5.2.2 User Acceptance Testing

User Acceptance *Testing is in progress.*

The decision to back-out this VistA patch will be made by Health Product Support, CPAC Revenue System Management staff, and the Development Team. Criteria to be determined based on separate and unique factors and will be evaluated upon post-patch installation use of the product.

5.3 Back-Out Risks

Back-out risks are not applicable for this VistA patch.

5.4 Authority for Back-Out

Any back-out decision should be a joint decision of the Business Owner (or their representative) and the Program Manager with input from theHealth Product Support (HPS) Application Coordinator, HPS Support, the project development team.

5.5 Back-Out Procedure

The back-out plan for VistA applications is complex and not a "one size fits all" solution. The general strategy for a VistA back-out is to repair the code with a follow-up patch. The development team recommends that sites log a ticket if it is a nationally released patch.

If it is prior to national release, the site will be already working directly with the development team and should contact that team. The development team members will have been identified in

the Initial Operating Capability (IOC) Memorandum of Understanding (MOU). As discussed in section 5.2, it is likely that development team can quickly address via a new software version. If the site is unsure whom to contact, they may log a ticket or contact Health Product Support - Management Systems Team.

Patch PSO*7.0*529 contains the build components listed below.

Patch PSO*7.0*529 installs the following routines:

Routine Name	New/Modified
PSO7E529	New
PSO7L529	New
PSO7M529	New
PSO7P529	New
PSODEAU0	New
PSODEAUT	New

Patch PSO*7.0*529 installs the following options in the OPTION file (#19):

Option Name	Menu Text	Type	Routine
PSO DEA DELETE	DEA Delete	Run Routine	START^PSO7M529
PSO DEA MIGRATION REPORT	DEA Migration Report	Run Routine	START^PSO7L529

Patch PSO*7.0*529 installs the following web service in the WEB SERVICE file (#18.02):

Web Service Name	Type	Context Root
PSO DOJ/DEA WEB SERVICE	REST	/dealnfo/

Patch PSO*7.0*529 installs the following web server:

Web Server Name	Server	Port	SSL Enabled	SSL Configuration
PSO DOJ/DEA WEB SERVICE	REST	/dealnfo/	True	encrypt_only_tlsv12

While the VistA KIDS installation procedure allows the installer to back up the modified routines using the 'Backup a Transport Global' action, the back-out procedure for global, data dictionary and other VistA components is more complex and requires issuance of a follow-up patch to ensure all components are properly removed and/or restored. All software components (routines and other items) must be restored to their previous state at the same time and in conjunction with the restoration of the data. Please contact the EPMO team for assistance since this installed patch contains components in addition to routines.

5.6 Back-out Verification Procedure

Successful back-out is confirmed by verification that the back-out patch was successfully implemented, including verification that new components were removed and modified components were returned to their pre-patch state.

6 Rollback Procedure

Rollback pertains to data. The data changes in this patch are specific to the operational software and platform settings. These data changes are covered in the Back-out procedures detailed elsewhere in this document. Rollback is not applicable to this VistA patch.

6.1 Rollback Considerations

Not applicable.

6.2 Rollback Criteria

Not applicable.

6.3 Rollback Risks

Not applicable.

6.4 Authority for Rollback

Not applicable.

6.5 Rollback Procedure

Not applicable.

6.6 Rollback Verification Procedure

Not applicable.