Medical Care Collection Fund (MCCF)

Electronic Data Interchange (EDI) Transaction Applications Suite (TAS)

ePayments Debit Electronic Funds Transfer (EFT) Patch

ePayments PRCA*4.5*375

Deployment, Installation, Back-out, and Rollback Guide

June 2021

Department of Veterans Affairs

Office of Information and Technology

Revision History

Date	Version	Description	Author
June 2021	1.0	Initial Version	MCCF EDI TAS ePayments

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Plan for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Plan is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

1. Introduction 1
1.1. Purpose 1
1.2. Dependencies 1
1.3. Constraints 1
2. Roles and Responsibilities 1
3. Deployment 2
3.1. Timeline 2
3.2. Site Readiness Assessment 2
3.2.1. Deployment Topology (Targeted Architecture) 2
3.2.2. Site Information (Locations, Deployment Recipients) 2
3.2.3. Site Preparation 3
3.3. Resources 3
3.3.1. Facility Specifics 3
3.3.2. Hardware 3
3.3.3. Software 3
3.3.4. Communications 4
3.3.4.1. 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 6
4.10. System Configuration 6
4.11. Database Tuning 6
5. Back-out Procedure 6
5.1. Back-out Strategy 6
5.2. Back-out Considerations 6
5.2.1. Load Testing 7
5.2.2. User Acceptance Testing 7
5.3. Back-out Criteria 7
5.4. Back-out Risks 7
5.5. Authority for Back-out 7
5.6. Back-out Procedure 7
5.7. Back-out Verification Procedure 8

6. Rollback Procedure 8

6.1. Rollback Considerations 8

6.2. Rollback Criteria 8

6.3. Rollback Risks 8

6.4. Authority for Rollback 8

6.5. Rollback Procedure 8

6.6. Rollback Verification Procedure 8

List of Tables

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

Table 2: Site Preparation 3

Table 3: Facility-Specific Features 3

Table 4: Hardware Specifications 3

Table 5: Software Specifications 4

Table 6: Deployment / Installation / Back-out Checklist 4

1. Introduction

This document describes how to deploy and install the PRCA*4.5*375 as well as how to back-out the product and rollback to a previous version or data set.

1.1. Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the PRCA*4.5*375 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 patches must be installed **before** PRCA*4.5*375:

- PRCA*4.5*184
- PRCA*4.5*332
- PRCA*4.5*345

1.3. Constraints

This patch is intended for a fully patched 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 OI&T, VA OI&T Health Product Support& PMO (Leidos)	Deployment	Plan and schedule deployment (including orchestration with vendors).	Planning
2	Local VAMC and CPAC processes	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 & 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	VIP Release Agent	Installation	Ensure authority to operate and that certificate authority security documentation is in place.	Deployment
7	N/A for this patch as we are using only the existing VistA system	Installation	Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes.	N/A
8	VA's eBusiness team	Installations	Coordinate training.	Deployment
9	VIP release Agent, Health Product Support & the development team	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out).	Deployment
10	No changes to current process – we are using the existing VistA system	Post Deployment	Hardware, Software and System Support.	Warranty

3. Deployment

The deployment is planned as a national rollout.

This section provides the schedule and milestones for the deployment.

3.1. Timeline

The deployment and installation are scheduled to run for 30 days.

3.2. Site Readiness Assessment

This section discusses the locations that will receive the PRCA*4.5*375 deployment.

3.2.1. Deployment Topology (Targeted Architecture)

This patch PRCA*4.5*375 is to be nationally released to all VAMCs.

3.2.2. Site Information (Locations, Deployment Recipients)

The test sites for IOC testing are:

1. Mann-Grandstaff (Spokane, WA) - Station 668.
2. Jonathan M. Wainwright Memorial (Walla Walla, WA) - Station 687.

- These sites will not be defined here until the sites have signed the Memorandum of Understanding (MOUs) and testing has completed as sometimes a site has to stop testing prior to the end of IOC.

Upon national release all VAMCs are expected to install this patch within the compliance date.

3.2.3. Site Preparation

The following table describes preparation required by the site prior to deployment:

Table 2: Site Preparation

Site / Other	Problem / Change Needed	Features to Adapt / Modify to New Product	Actions / Steps	Owner
N/A	N/A	N/A	N/A	N/A

3.3. Resources

3.3.1. Facility Specifics

The following table lists facility-specific features required for deployment.

Table 3: Facility-Specific Features

Site	Space / Room	Features Needed	Other
N/A	N/A	N/A	N/A

3.3.2. Hardware

The following table describes hardware specifications required at each site prior to deployment.

Table 4: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Existing VistA system	N/A	N/A	N/A	N/A	N/A

Please see the Roles and Responsibilities table in Section 2 for details about who is responsible for preparing the site to meet these hardware specifications.

3.3.3. Software

The following table describes software specifications required at each site prior to deployment:

Table 5: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other
Fully patched Accounts Receivable package within VistA	N/A	4.5	N/A	N/A	N/A
PRCA*4.5*184	N/A	Nationally released version	N/A	N/A	N/A
PRCA*4.5*321	N/A	Nationally released version	N/A	N/A	N/A
PRCA*4.5*326	N/A	Nationally released version	N/A	N/A	N/A
PRCA*4.5*3345	N/A	Nationally released version	N/A	N/A	N/A

Please see the Roles and Responsibilities table in Section 2 above for details about who is responsible for preparing the site to meet these software specifications.

3.3.4. Communications

The sites that are participating in field testing (IOC) will use the "Patch Tracking" message in Outlook to communicate with the ePayments eBusiness team, the developers, and product support personnel.

3.3.4.1. Deployment / Installation / Back-out Checklist

The Release Management team will deploy the patch PRCA*4.5*375, 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. 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 in the chart below.

Table 6: Deployment / Installation / Back-out Checklist

Activity	Day	Time	Individual who completed task
Deploy	N/A	N/A	N/A
Install	N/A	N/A	N/A

4. Installation

4.1. Pre-installation and System Requirements

PRCA*4.5*375, a patch to the existing VistA Accounts Receivable 4.5 package, is installable on a fully patched M(UMPS) VistA system and operates on the top of the VistA environment provided by the VistA infrastructure packages. The latter provides utilities which communicate with the underlying operating system and hardware, thereby providing Accounts Receivable independence from variations in hardware and operating system.

4.2. Platform Installation and Preparation

Refer to PRCA*4.5*375 documentation on the National Patch Module (NPM) on Forum for the detailed installation instructions. These instructions would include any pre installation steps if applicable.

4.3. Download and Extract Files

Refer to PRCA*4.5*375 documentation on the NPM to find the location of related documentation that can be downloaded. PRCA*4.5*375 will be transmitted via a PackMan message and can be pulled from the NPM. It is not a host file, and therefore does not need to be downloaded separately.

4.4. Database Creation

PRCA*4.5*375 modifies the VistA database. All changes can be found on the NPM documentation for this patch.

4.5. Installation Scripts

No installation scripts are needed for PRCA*4.5*375 installation.

4.6. Cron Scripts

No Cron scripts are needed for PRCA*4.5*375 installation.

4.7. Access Requirements and Skills Needed for the Installation

The following staff will need access to the PackMan message containing the PRCA*4.5*375 patch or to Forum's NPM for downloading the nationally released PRCA*4.5*375 patch. The software is to be installed by the site's or region's designated: VA OI&T IT OPERATIONS SERVICE, Enterprise Service Lines, VistA Applications Division[1].

4.8. Installation Procedure

Refer to PRCA*4.5*375 documentation on the NPM for the detailed installation instructions.

[1] "Enterprise service lines, VAD" for short; formerly known as the IRM (Information Resources Management) or IT support.

4.9. Installation Verification Procedure

Refer to PRCA*4.5*375 documentation on the NPM for the detailed installation instructions. These instructions would include any post installation steps if applicable.

4.10. System Configuration

No system configuration changes are required for this patch.

4.11. Database Tuning

No reconfiguration of the VistA database, memory allocations or other resources is necessary.

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

Although it is unlikely due to care in collecting, elaborating, and designing approved user stories, followed by multiple testing stages (Developer Unit Testing, Component Integration Testing, SQA Testing, and User Acceptance Testing), a back-out decision due to major issues with this patch could occur. A decision to back out could be made during site Mirror Testing, Site Production Testing or after National Release to the field (VAMCs). The best strategy decision is dependent on the stage of testing during which the decision is made.

If during Mirror testing or Site Production Testing, a new version of a defect correcting test patch is produced, retested, and successfully passes development team testing, it will be resubmitted to the site for testing. If the patch produces catastrophic problems, the patch may be backed out by installing the back-up message created via the “Back-up a Transport Global” option used during patch installation.

If the defect(s) were not discovered until after national release a decision would have to be made as to the best course of action. The patch may be backed out by installing the back-up message created via the “Back-up a Transport Global” option used during patch installation, *if there were no overlapping components with subsequent builds.* Alternatively, a new patch might be created by the development team to remedy the fault. This determination should be made in close consultation with the development team.

5.2. Back-out Considerations

It is necessary to determine if a wholesale back-out of the patch PRCA*4.5*375 is needed or if a better course of action is to correct through a new version of the patch (if prior to national release) or through a subsequent patch aimed at specific areas modified or affected by the original patch (after national release). A wholesale back-out of the patch will still require a new version (if prior to national release) or a subsequent patch (after national release). If the back-out is post-release of patch PRCA*4.5*375, this patch should be assigned status of “Entered in Error” in Forum’s NPM.

5.2.1. Load Testing

N/A. The back-out process would be executed at normal, rather than raised job priority, and is expected to have no significant effect on total system performance. Subsequent to the reversion, the performance demands on the system would be unchanged.

5.2.2. User Acceptance Testing

1. Receipt transactions for a debit type EFT will be marked with a new debit flag. These transactions will be subtracted from the calculated receipt total, which may result in a negative receipt total.
2. When an EFT is removed from the system using the menu option: Remove Duplicate EFT Deposits, [RCDPE REMOVE DUP DEPOSITS], the new field REMOVAL TYPE [.2] will be entered, after the removal reason text.

The user must enter one of two codes from the set:

- D = DUPLICATE EFT
- M = MILLENIUM EFT

The new field will show on the Duplicate EFT Deposits Audit report [RCDPE EFT AUDIT REPORT].

5.3. Back-out Criteria

The project is canceled, or the requested changes implemented by PRCA*4.5*375 are no longer desired by VA Office of Information and Technology (OIT) and the ePayments eBusiness team, or the patch produces catastrophic problems.

5.4. Back-out Risks

Since the ePayments software is tightly integrated with external systems, any attempt at a back-out should include close consultation with the external trading partners such as the Financial Services Center (FSC) the Health Care Clearing House (HCCH), the VA 3rd Party Lockbox bank, and the Financial Management System (FMS) to determine risk.

5.5. Authority for Back-out

The order would come jointly from: release coordinator (product support), portfolio director and health product support. This should be done in consultation with the development team and external trading partners such as FSC, the HCCH, VA 3rd Party Lockbox bank, and the FMS to determine the appropriate course of action. ePayments is tightly integrated with these external partners and a back-out of the patch should not be a standalone decision.

5.6. Back-out Procedure

This patch may be backed out by installing the back-up message created via the “Back-up a Transport Global” option used during patch installation, *if there were no overlapping components with subsequent builds* installed after this patch. Alternatively, a new patch might be created by the development team to remedy the fault. This determination should be made in close consultation with the development team.

The PRCA*4.5*375 patch contains the following build components:

- Routines
- Data Dictionary Changes

5.7. Back-out Verification Procedure

Successful back-out is confirmed by verification that the back-out patch was successfully installed.

6. Rollback Procedure

Rollback pertains to data. Patch PRCA*4.5*375 does impact the data in the Accounts Receivable package. Therefore, to roll back the patch one will need to install a new patch to rollback the database changes and restore the system back to its prior state. In the case where a rollback is needed, refer to the Back-out procedures detailed elsewhere within this document.

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.