Community Care (CC) Integrated Billing (IB) and Accounts Receivable (AR) Phase 2

Accounts Receivable PRCA*4.5*365

Software Version 1.0

Deployment, Installation, Back-Out, and Rollback Guide

May 2020

Department of Veterans Affairs

Office of Information and Technology (OI&T)

Revision History

Date	Version	Description	Author
05/18/2020	1.0	Initial Delivery	AbleVets

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 2
   3.3 Resources 3
      3.3.1 Hardware 3
      3.3.2 Software 3
      3.3.3 Communications 3
         3.3.3.1 Deployment/Installation/Back-Out Checklist 3
4. Installation 3
   4.1 Pre-installation and System Requirements 3
   4.2 Platform Installation and Preparation 4
   4.3 Download and Extract Files 4
   4.4 Database Creation 4
   4.5 Installation Scripts 4
   4.6 Cron Scripts 4
   4.7 Access Requirements and Skills Needed for the Installation 4
   4.8 Installation Procedure 4
   4.9 Installation Verification Procedure 5
   4.10 System Configuration 5
   4.11 Database Tuning 5
5. Back-Out Procedure 5
   5.1 Back-Out Strategy 5
   5.2 Back-Out Considerations 6
      5.2.1 Load Testing 6
      5.2.2 User Acceptance Testing 6
   5.3 Back-Out Criteria 6
   5.4 Back-Out Risks 6
   5.5 Authority for Back-Out 6

5.6 Back-Out Procedure 7
5.7 Back-out Verification Procedure 7
6. Rollback Procedure 7
6.1 Rollback Considerations 7
6.2 Rollback Criteria 7
6.3 Rollback Risks 8
6.4 Authority for Rollback 8
6.5 Rollback Procedure 8
6.6 Rollback Verification Procedure 8

1. Introduction

This document describes how to deploy and install the Community Care Accounts Receivable (AR) Enhancements patch PRCA*4.5*365 as well as how to back-out the product and rollback to a previous version or data set. This document is a companion to the project charter and management plan for this effort.

1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the Community Care Accounts Receivable Enhancements patch PRCA*4.5*365 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 prior to installing PRCA*4.5*365:

- PRCA*4.5*153
- PRCA*4.5*357

1.3 Constraints

This product is intended for 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

Team	Phase / Role	Tasks
Health Product Support (HPS)	Deployment	Plan and schedule deployment (including orchestration with vendors)
Health Product Support and existing local VA Medical Center (VAMC) and Consolidated Patient Account Center (CPAC) processes	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.
Health Product Support and Veteran-Focused Integration Process (VIP) Release Agent	Deployment	Test for operational readiness
Health Product Support	Deployment	Execute deployment
Designated VistA patch installer for this package	Installation	Plan and schedule installation

Team	Phase / Role	Tasks
Designated VistA patch installer for this package and VIP Release Agent	Installation	Ensure authority to operate and that certificate authority security documentation is in place
CPAC Revenue Analysts	Installations	Coordinate training
Designated VistA patch installer for this package, and CPAC Revenue Analysts, Health Product Support, and Development Team	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)
Product Development Team during warranty period, afterwards (software only) Tier 1, Tier 2, Tier 3 / VistA Maintenance	Post Deployment	Hardware, Software and System Support

3. Deployment

The deployment is planned as a simultaneous national rollout to all 130 VistA production instances. This section provides the schedule and milestones for the deployment.

3.1 Timeline

The deployment and installation are scheduled to run for 5 days starting with the National Release date and concluding with the National Compliance date by which time all 130 VistA production instances should have the patch installed.

3.2 Site Readiness Assessment

This section discusses the locations that will receive the Community Care Accounts Receivable Enhancements patch PRCA*4.5*365 deployment.

3.2.1 Deployment Topology (Targeted Architecture)

N/A for a VistA patch.

3.2.2 Site Information (Locations, Deployment Recipients)

All 130 VistA production instances. The Initial Operating Capabilities (IOC) test sites for this project were Edward J Hines VA Hospital (578), Hunter Holmes McGuire VA Medical Center (652), and Central Alabama Veterans Health Care System (East/West) (619).

3.2.3 Site Preparation

None required other than prerequisite patch installation as described in the patch description and in the Forum National Patch Module (NPM).

3.3 Resources

The Community Care Accounts Receivable Enhancements patch PRCA*4.5*365 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 PRCA*4.5*365, 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 in the chart below. The table is included below if manual tracking is desired and because it is part of the VIP document template.

Table 2: Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual who completed task
Deploy	TBD	TBD	TBD
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 the patch 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" to create a backup message of any routines exported with this patch. This step is important to make any routine rollback in a simple and efficient manner.

Post-installation checksums are found in the patch description and in Forum NPM.

4.3 Download and Extract Files

N/A for this VistA patch.

4.4 Database Creation

N/A for this VistA patch.

4.5 Installation Scripts

N/A for this VistA patch.

4.6 Cron Scripts

N/A 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

Installation Instructions:

1. Choose the PackMan message containing this patch.
2. Choose the **INSTALL/CHECK MESSAGE** PackMan option.
3. From the **Kernel Installation and Distribution System** menu, select the **Installation** menu.
4. From the **Installation** menu, you may elect to use the following options. When prompted for the **INSTALL NAME** enter **PRCA*4.5*365**.
    - **Backup a Transport Global** - This option will create a backup message of any routines exported with this patch. It will not backup any other changes such as DDs or templates.

- **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 components of this patch routines, DDs, templates, etc.
- **Verify Checksums in Transport Global** - This option will allow you to ensure the integrity of the routines that are in the transport global.

5. From the **Installation** menu, select the Install Package(s) option and choose the patch to install.
6. When prompted Want KIDS to INHIBIT LOGONs during the install? NO// answer **NO**.
7. When prompted 'Want to DISABLE Scheduled Options, Menu Options, and Protocols? NO // answer **NO**.
8. If prompted Delay Install (Minutes): (0 60): 0// respond **0**.

4.9 Installation Verification Procedure

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

4.10 System Configuration

N/A for this VistA patch.

4.11 Database Tuning

N/A 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

The back-out plan for VistA applications is complex and is not able to be a “one size fits all” strategy. The general strategy for VistA software 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; 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)/Pharmacy Benefits Management (PBM) review and multiple testing stages (Primary Developer, Secondary Developer, and Component Integration 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. This project, however, has prepared a set of back-out patch instructions if necessary, as in the case that the project is canceled, or the

implemented design is found to be so wrong and detrimental to the site's delivery of services to veterans that the software must be removed. 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. After 30 days, the VistA Maintenance Program would produce the new patch, either to correct the defective components or to back-out.

5.2 Back-Out Considerations

It is necessary to determine if a wholesale back-out of the patch PRCA*4.5*365 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*365, this patch should be assigned status of "Entered in Error" in Forum's NPM.

5.2.1 Load Testing

N/A for this VistA patch.

5.2.2 User Acceptance Testing

This is detailed in the User Stories in Rational Tools Management.

5.3 Back-Out Criteria

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.

5.4 Back-Out Risks

N/A for this VistA patch.

5.5 Authority for Back-Out

Back-out authorization will be determined by a consensus consisting of one of the following POCs in each area:

- Health Product Support Management –
  - Primary: John P Elliott; email - John.Elliott@va.gov
  - Primary: Falencia Marshall; email - Falencia.Marshall2@va.gov
  - Secondary: Angela Murray; email - Angela.Harris@va.gov
- Release Managers –
  - Primary: John Tas Ward; email - John.T.Ward@va.gov
- CPAC Revenue System Managers –

    - Primary: Brandon Bergeron; email - Brandon.Bergeron@va.gov
    - Secondary: Jerry Battles; email - Jerry.Battles@va.gov
- Development Team –
    - Primary: Rajeev Vadgama; email - Rajeev.Vadgama@va.gov
    - Secondary: Scott Bush; email - Scott.Bush@va.gov

5.6 Back-Out Procedure

The back-out procedure 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 not, the site should contact the Enterprise Program Management Office (EPMO) team directly for specific solutions to their unique problems.

The PRCA*4.5*365 patch contains the following build components:

- Routines
- Modification of the following files:
    - ACCOUNTS RECEIVABLE CATEGORY [#430.2] – one (1) new field

While the VistA installation procedure of the KIDS build 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.

5.7 Back-out Verification Procedure

The success of the back-out can be verified by verifying checksums for the routines removed to validate that they reflect the nationally released checksums.

6. Rollback Procedure

Rollback pertains to data associated with this 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