# Suicide High Risk Patient Enhancements (SHRPE)

# IB*2.0*614

## Deployment, Installation, Back-Out, and Rollback Guide


**Department of Veterans Affairs**

**October 2018**

**Version 4.0**

# Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 9/13/2018 | 4.0 | Monthly Review, No Updates | Shavkat Shamukhamedov |
| 8/23/2018 | 4.0 | Added information about the activation patch to the section 1. Introduction; Made other minor changes. | Shavkat Shamukhamedov |
| 7/05/2018 | 3.0 | Added information about additional functionality to the section 1. Introduction | Shavkat Shamukhamedov |
| 4/12/2018 | 2.0 | Added new information, including: addressed issues found by reviewers and added Legislation Effective Date switch functionality overview | Shavkat Shamukhamedov |
| 1/15/2018 | 1.0 | Initial Draft | Shavkat Shamukhamedov |

# Table of Contents

# 1 Introduction

This document describes how to deploy and install the Veterans Information Systems and Technology Architecture (VistA) Integrated Billing patch IB*2.0*614, 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.

To meet the objectives of the Suicide High Risk Patient Enhancements (SHRPE) of minimizing the financial burden to high risk patients, the solution will be deployed in two patches:

The first patch is the Integrated Billing patch IB*2.0*614, which will:

- Exempt patients with an active Category 1 (national) Patient Record Flag High Risk for Suicide from Outpatient visit copay,
- Prorate outpatient medication copay (and dosages) for less than 30 days' supply for patients with active National (Category I) High Risk for Suicide patient record flag
- Send MailMan bulletins to IB MEANS TEST mail group to notify IB staff about charges that might need to be adjusted or cancelled due to changes of the PRF flag of the patient that occurred later than the date of service or RX medication released date.

The functionality described above will be installed with dormant / inactive code. This is due to unavailability of the legal effective date of the legislation from which policy determines the logic used in the code. The legislation proposal is currently being formalized and could take years before it results in an approval. Therefore, this patch will have an effective date placeholder and its functionality won't be activated until the date is populated.

The second patch, referred to as the "activation" patch or IB*2.0*629, will contain the installation code that enters the activation date of legislation into the database so the IB*2.0*614 code can read the effective date, compare it with the date of Outpatient visit or outpatient medication issue date, and apply the new business logic for billing accordingly. This "activation" patch IB*2.0*629 will be created in advance during this project, entered in FORUM and await completion as an "under development" patch.

The "activation" patch IB*2.0*629 code will be tested by the development team of the patch IB*2.0*614. No changes for the "activation" patch will be needed except inserting the effective date in the MUMPS post-install routine of the patch IB*2.0*629. The copy of the patch description and code will be posted in both Jazz (as a KIDS build) and in FORUM (as NPM patch). If any discrepancies are found, then the latest copy in Jazz should be used.

When the federal government passes the legislation that affects copay in this situation and the effective date becomes known to stakeholders of the SHRPE project, either this development team will be notified and will release the activation patch IB*2.0*629 or, if this development team is not available at that time, a subsequent team should be assigned to finalize and release the patch IB*2.0*629.

## 1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the VistA Integrated Billing patch IB*2.0*614 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

This patch modifies existing VistA Integrated Billing routines to provide new functionality that addresses changes for billing system for the patient with an active National Category 1 Patient Record Flag High Risk for Suicide.

- IB*2.0*339, IB*2.0*549, IB*2.0*563 must be installed before IB*2.0*614.

## 1.3 Constraints

This patch should be installed in all VA's VistA production sites. This patch is intended for a fully patched VistA system. Its installation will not noticeably impact the production environment.

# 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 | Deployment | Plan and schedule deployment (including orchestration with vendors) | Planning |
| 2 | Local Individual Veterans Administration Medical Centers (VAMC) | 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 |
| 5 | VAMCs | Installation | Plan and schedule installation | Deployment |

| ID | Team | Phase / Role | Tasks | Project Phase (See Schedule) |
|---|---|---|---|---|
| 6 | VIP Release Agent | Installation | Obtain 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 Point of Contact (POC) to ensure that IT equipment has been accepted using asset inventory processes | Deployment |
| 8 | The VA's SHRPE team | Installations | Coordinate knowledge transfer with the team responsible for user 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 | SHRPE Team | 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 duration of deployment and installation is 30 days. A detailed schedule will be provided during the build.

## 3.2 Site Readiness Assessment

This section discusses the locations that will receive the IB*2.0*614 patch deployment.

### 3.2.1 Deployment Topology (Targeted Architecture)

The VistA Integrated Billing patch IB*2.0*614 should be installed in all VA VistA production sites.

### 3.2.2 Site Information (Locations, Deployment Recipients)

List of test sites that are used for IO testing:

- West Palm Beach
- Palo Alto

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

Not any site preparation specific steps are needed for this patch. The VA site should follow the standard procedure they are using now for installation of VistA patches (Table 2)

**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

There are no other resources required for installation of the patch other than the personnel that are normally required for the deployment and installation of VistA patches.

### 3.3.1 Facility Specifics

There are no facility-specific features (Table 3) required for deployment of this patch.

**Table 3: Facility Specific Features**

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

### 3.3.2 Hardware

There are no special requirements regarding new or existing hardware capability. Existing hardware resources (Table 4) will not be impacted by the changes in this project.

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

### 3.3.3 Software

Table 5 describes the software specifications required at each site prior to deployment.

**Table 5: Software Specifications**

| Required Software | Make | Version | Configuration | Manufacturer | Other |
|---|---|---|---|---|---|
| Fully patched Integrated Billing package within VistA | N/A | 2.0 | N/A | N/A | N/A |
| IB*2.0*339, IB*2.0*549, IB*2.0*563 | N/A | Nationally released version | N/A | N/A | N/A |

Please see the *Deployment, Installation, Back-out, and Rollback Roles and Responsibilities* Table in Section 2 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 messages in Outlook and weekly meetings to communicate with the SHRPE team, the developers, and product support personnel.

#### 3.3.4.1 Deployment/Installation/Back-Out Checklist

The Release Management team will deploy the patch IB*2.0*614, which is tracked nationally for all VAMCs in the National Patch Module (NPM) in FORUM. 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 currently installed the patch in their VistA production system. Therefore, this information does not need to be manually tracked in Table 6.

**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 |
| Back-Out | N/A | N/A | N/A |

# 4 Installation

## 4.1 Pre-installation and System Requirements

IB*2.0*614, a patch to the existing VistA Integrated Billing 2.0 package, is installable on a fully patched Massachusetts General Hospital Utility Multi-Programming System (MUMPS) VistA system and operates on 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 Integrated Billing independence from variations in hardware and operating system.

## 4.2 Platform Installation and Preparation

Refer to the IB*2.0*614 Patch Description on the NPM in FORUM for the detailed installation instructions. These instructions would include any pre-installation steps if applicable.

## 4.3 Download and Extract Files

Refer to the IB*2.0*614 documentation on the NPM to find related documentation that can be downloaded. IB*2.0*614 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

The patch is applied to an existing MUMPS VistA database.

## 4.5 Installation Scripts

Refer to the IB*2.0*614 Patch Description in the NPM for installation instructions

## 4.6 Cron Scripts

No Cron scripts are needed for the IB*2.0*614 installation.

## 4.7 Access Requirements and Skills Needed for the Installation

Access to National VA Network, as well as the local network of each site to receive IB patches is required to perform the installation, as well as authority to create and install patches.

Knowledge of, and experience with, the Kernel Installation and Distribution System (KIDS) software is required. For more information, see Section V, Kernel Installation and Distribution System, in the Kernel 8.0 & Kernel Toolkit 7.3 Systems Management Guide.

## 4.8 Installation Procedure

Refer to the IB*2.0*614 patch description documentation on the NPM in FORUM for detailed installation instructions.

## 4.9 Installation Verification Procedure

After installation, the user verifies installation results by using the "Install File Print" menu option in the "Utilities" submenu of the Kernel Installation & Distribution System.

Also refer to the IB*2.0*614 documentation on the NPM for detailed installation instructions. These instructions include any post installation steps if applicable.

## 4.10 System Configuration

No system configuration changes are required for this patch.

Refer to the IB*2.0*614 patch documentation in the NPM for information concerning new or modified security keys and assignment of user privilege.

## 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.

**NOTE:** Due to the complexity of this patch (because of the data dictionary changes), it is not recommended for back-out. However, if a site decides to back-out this patch, the site should contact the National Service Desk (NSD) to submit a ticket; the development team will assist with the process.

The Back-Out Procedure consists of restoring routines and removing manually each new Data Dictionary (DD) definition component introduced by the patch.

The back-out is to be performed by persons with programmer-level access, and in conjunction with the SHRPE Team.

## 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 such as the 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 defect's/defects' degree of severity and the stage of testing during which the decision is made.

### 5.1.1 Mirror Testing or Site Production Testing

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, a new version of the patch can be used to restore the build components to their pre-patch condition.

### 5.1.2 After National Release but During the Designated Support Period

VistA KIDs builds cannot be backed out/restored in totality – only routines are part of a backup transport global. Special care is taken during development of VistA code (routines, files, remote procedures, etc.) to make them backward compatible with newer GUI versions to alleviate the issue and avoid typical critical scenario solutions such as emergency patches.

The decision to back out a specific release needs to be made in a timely manner. Catastrophic failures are usually known early in the testing process – within the first two or three days. Sites are encouraged to perform all test scripts to ensure new code is functioning in their environment, with their data. A back-out should only be considered for critical issues or errors. The normal or an expedited, issue-focused patch process can correct other bugs.

The general strategy for SHRPE VistA functionality rollback will likely be to repair the code with another follow-on patch.

If any issues with SHRPE Vista software are discovered after it is nationally released and within the 30-day maintenance window, the SHRPE development team will research the issue and provide guidance for any immediate, possible workaround. After discussing the defect with VA and receiving their approval for the proposed resolution, the SHRPE development team will communicate guidance for the long-term solution to the field.

The long-term solution will likely be the installation of a follow-up patch to correct the defect, a follow-up patch to remove the SHRPE updates, or a detailed set of instructions on how the software can be safely backed out of the production system.

In addition, at the time of deployment, local sites can perform the following steps:

1. At the time of system deployment, create a complete backup of the current system and store it on a separate machine.
2. Continue with application-specific system deployment steps.
    a. If the system fails during deployment, perform a system rollback using the system backup created in step 1.
3. Perform thorough and comprehensive testing to ensure the integrity and functionality of the system is intact.
4. Perform a system backup once the system is deemed stable and ready for users and store it on a separate machine.
    a. Once users begin working on the system, regularly create system backups and store them on another machine.

If system failure occurs after users are on the system, perform a system rollback using the system backup created in step 4a.

### 5.1.3 After National Release and Warranty Period

After the support period, the VistA Maintenance Program would produce the new patch, either to correct the defective components or restore the build components to their original pre-patch condition.

## 5.2 Back-Out Considerations

It is necessary to determine if a wholesale back-out of the patch IB*2.0*614 is needed or if a better course of action is needed to correct through a new version of the patch (if prior to national release) or 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 IB*2.0*614, this patch should be assigned status of "Entered in Error" in Forum's NPM.

### 5.2.1 Load Testing

The installation process of the back-out patch, which would be executed at normal, rather than raised job priority, is expected to have minimal effect on total system performance. To minimize the potential impact on users, installation of the back-out patch can be queued to run during hours of reduced user activity. After the reversion, the performance demands on the system would be slightly decreased as less data would be filed per transaction.

### 5.2.2 User Acceptance Testing

The results will be provided upon the completion of the User Acceptance Testing.

## 5.3 Back-Out Criteria

The project is canceled, the requested changes implemented by IB*2.0*614 are no longer desired by VA OI&T, or the patch produces catastrophic problems.

## 5.4 Back-Out Risks

By backing out IB*2.0*614 patch, the local facility will not be able to provide SHRPE functionality implemented by the patch:

- Exempt patients with an active National Category 1 Patient Record Flag High Risk for Suicide from copay charges for outpatient visits,
- Prorate prescription copay amounts for patients with an active National Category 1 Patient Record Flag High Risk for Suicide.

The current changes made in the patch don't affect other applications and thus the backing out the software should not pose any issues.

The project is still under development so there are chances that dependencies with other applications are introduced and if this happens then this section will need to be re-evaluated to determine potential risks.

## 5.5 Authority for Back-Out

The order would come from: Release Coordinator (product support), Portfolio Director and Health Product Support. This should be done in consultation with the development team and project stakeholders.

## 5.6 Back-Out Procedure

The rollback plan for VistA applications is complex and not a "one size fits all" solution. The general strategy for a VistA rollback 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. The IB*2.0*614 patch contains the following build components:

- Routines

The pre-patch versions of routines can be restored by using backup MailMan message that should be created during installation.

Note: The routines can be modified by another patch that follows the IB*2.0*614 and released after the installation of the IB*2.0*614. In this case restoring routines from the backup MailMan message might cause issues. It is recommended that the sites contact the development team and the National VistA Support team after for specific solutions to their unique problems.

- Data dictionaries

The new SHRPE ACTIVATION DATE field (#70.02) of the IB SITE PARAMETERS file (#350.9) can be deleted by using the standard FileMan option MODIFY FILE ATTRIBUTES.

## 5.7 Back-out Verification Procedure

If restoring routines from back up emails is used, then successful back-out is confirmed by verification of BEFORE checksums listed in the patch description for these routines in NPM in FORUM.

If removing of the SHRPE ACTIVATION DATE field (#70.02) of the IB SITE PARAMETERS file (#350.9) was performed manually then the standard FileMan DATA DICTIONARY UTILITIES utility can be used to verify if the field was removed successfully.

If the special back-out patch is used, then successful back-out is confirmed by verification that the back-out patch was successfully installed.

# 6 Rollback Procedure

Rollback pertains to data. This patch doesn't change any standard data on the site. If any billing errors occurred due to the patch, then research performed by qualified IB staff will be required and corrections will need to be performed manually.

## 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.