

**Veterans Health Administration (VHA) Health Finance
Development, Security, and Operations (DevSecOps)
Medical Care Collection Fund (MCCF)**

eInsurance 31

IB*2.0*822

Deployment, Installation, Back-out, and Rollback Guide



February 2026

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
02/2026	1.1	Updated the days to install in section 3.1. Added item 5 to section 5.2.2.	VHA HF DSO MCCF eInsurance
01/2026	1.0	IOC Exit	VHA HF DSO MCCF eInsurance
08/2025	0.1	Draft version for MOU	VHA HF DSO MCCF eInsurance

Template v2.4, July 2024

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.

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	3
3.2	Site Readiness Assessment	3
3.2.1	Deployment Topology (Targeted Architecture)	3
3.2.2	Site Information (Locations, Deployment Recipients).....	3
3.2.3	Site Preparation.....	3
3.3	Resources.....	3
3.3.1	Facility Specifics.....	3
3.3.2	Hardware.....	4
3.3.3	Software	4
3.3.4	Communications.....	5
3.3.4.1	Deployment / Installation / Back-out Checklist	5
4	Installation.....	5
4.1	Pre-installation and System Requirements.....	5
4.2	Platform Installation and Preparation.....	5
4.3	Download and Extract Files.....	6
4.4	Database Creation	6
4.5	Installation Scripts	6
4.6	Cron Scripts.....	6
4.7	Access Requirements and Skills Needed for the Installation	6
4.8	Installation Procedure	6
4.9	Installation Verification Procedure.....	6
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 Criteria	9
5.4	Back-out Risks	9
5.5	Authority for Back-out	9
5.6	Back-out Procedure	10
5.7	Back-out Verification Procedure	10
6	Rollback Procedure	11
6.1	Rollback Considerations	11
6.2	Rollback Criteria	11
6.3	Rollback Risks	11
6.4	Authority for Rollback	11
6.5	Rollback Procedure	11
6.6	Rollback Verification Procedure	11

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	4
Table 5:	Software Specifications.....	4
Table 6:	Deployment / Installation / Back-out Checklist.....	5

1 Introduction

This document describes how to deploy and install the VHA DSO MCCF eInsurance 31 IB*2.0*822 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. In cases where a non-developed Commercial Off The Shelf (COTS) product is being installed, the vendor provided User and Installation Guide may be used, but the Back-out Recovery strategy still needs to be included in this document.

1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the patch IB*2.0*822 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 IB*2.0*822:

- IB*2.0*593
- IB*2.0*647
- IB*2.0*778
- IB*2.0*806

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 OIT, VHA Finance Financial Management VistA Support, and PMO	Deployment	Plan and schedule deployment (including orchestration with vendors).	Planning

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
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)), VHA Finance Financial Management VistA Support Testing, and VistA Office Approval	Deployment	Test for operational readiness.	Testing
4	VHA Finance Financial Management VistA Support and Field Operations	Deployment	Execute deployment.	Deployment
5	Individual Veterans Affairs Medical Centers (VAMCs)	Installation	Plan and schedule installation.	Deployment
6	VistA Office	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	VistA Office, VHA Finance Financial Management VistA Support and 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 concurrent rollout. This section provides the schedule and milestones for the deployment.

3.1 Timeline

The deployment and installation are scheduled to run for 10 days, starting with the day after national release.

3.2 Site Readiness Assessment

This section discusses the locations that will receive the IB*2.0*822 deployment.

3.2.1 Deployment Topology (Targeted Architecture)

This patch IB*2.0*822 is to be nationally released to all VAMCs.

3.2.2 Site Information (Locations, Deployment Recipients)

The test sites for IOC testing are:

- CW Bill Young VAMC (Bay Pines, FL) (Site #516)
- VA Heartland-East (St. Louis, MO) (Site #657)
- Central Alabama Veterans Health Care System (Montgomery, AL) (Site #619)

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

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 1](#) 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 Integrated Billing package within VistA	N/A	2.0	N/A	N/A	N/A
IB*2.0*593	N/A	Nationally released version	N/A	N/A	N/A
IB*2.0*647	N/A	Nationally released version	N/A	N/A	N/A
IB*2.0*778	N/A	Nationally released version	N/A	N/A	N/A
IB*2.0*806	N/A	Nationally released version	N/A	N/A	N/A

Please see the Roles and Responsibilities [Table 1](#) 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 eBusiness Insurance sub-team, the developers, and product support personnel.

3.3.4.1 Deployment / Installation / Back-out Checklist

The Release Management team will deploy the IB*2.0*822 patch, which is tracked in the National Patch Module (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 and by whom the patch was installed in the VistA Production at each site. A report can also be run to identify which sites have not currently installed the patch in their VistA Production systems. 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
Back-out	N/A	N/A	N/A

4 Installation

4.1 Pre-installation and System Requirements

IB*2.0*822, a patch to the existing VistA Integrated Billing 2.0 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, providing Integrated Billing independence from variations in hardware and operating system.

4.2 Platform Installation and Preparation

Refer to the IB*2.0*822 documentation on the NPM on Forum for the detailed installation instructions. These instructions will include any pre-installation steps if applicable.

4.3 Download and Extract Files

Refer to the IB*2.0*822 documentation on the NPM to find the location of related documentation that can be downloaded. IB*2.0*822 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

This patch IB*2.0*822 does NOT introduce a new database. It uses the existing VistA database.

4.5 Installation Scripts

No installation scripts are needed for IB*2.0*822 installation.

4.6 Cron Scripts

No Cron scripts are needed for IB*2.0*822 installation.

4.7 Access Requirements and Skills Needed for the Installation

The following staff need access to the PackMan message containing the IB*2.0*822 patch or Forum's NPM to download the nationally released IB*2.0*822 patch. The software is to be installed by the sites or regions designated: VA OI&T IT OPERATIONS SERVICE, Enterprise Service Lines, VistA Applications Division, or all¹.

4.8 Installation Procedure

Refer to the IB*2.0*822 documentation on the NPM for the detailed installation instructions.

4.9 Installation Verification Procedure

Refer to the IB*2.0*822 documentation on the NPM for detailed installation instructions. These instructions include any post installation steps if applicable.

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

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 valid instance of operational software and 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 during site Mirror Testing, Site Production Testing, or after National Release to the field (VAMCs). The best strategy is dependent on the stage 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 would be resubmitted to the site for testing. If the patch produced catastrophic problems, a new version of the patch can be used to restore the build components to their pre-patch condition.

If the defect(s) were not discovered until after national release but during the designated 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 a patch for a patch. It is up to VA OIT and product support whether this new patch would be defined as an emergency patch or not. This new patch could be used to address specific issues pertaining to the original patch or could be used to restore the build components to their original pre-patch condition.

After the support period, the VistA Maintenance Program would produce the new patch, either to correct the defective components or to back-out the patch.

5.2 Back-out Considerations

It is necessary to determine if a wholesale back-out of the patch IB*2.0*822 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 this patch IB*2.0*822, 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 if necessary is 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. Modified EINSURANCE NIGHT PROCESS [IBCN EINSURANCE NIGHT PROCESS] to include checking the DATE LAST VERIFIED (#2.312,1.03) on active policies associated with pre selected insurance companies from INSURANCE COMPANY (#36) file. When applicable, the DATE LAST VERIFIED is automatically updated to "Today's" date.
2. Modified PROCESS INSURANCE BUFFER [IBCN INSURANCE BUFFER PROCESS] to allow a E1 Pharmacy response buffer entry to be accepted and saved to the PATIENT (#2) file. A new action, "Pharmacy Eligibility" (PE), was added to the following options:
 - Patient Insurance Info View/Edit [IBCN PATIENT INSURANCE]
 - View Patient Insurance [IBCN VIEW PATIENT INSURANCE]
 - Third Party Joint Inquiry (TPJI) [IBJ THIRD PARTY JOINT INQUIRY]
 - Claims Tracking Edit [IBT EDIT HR TRACKING ENTRY]
 - Claims Tracking Edit [IBT EDIT BI TRACKING ENTRY]
 - Claims Tracking Edit [IBT EDIT IR TRACKING ENTRY]
 - Claims Tracking Edit [IBT EDIT TRACKING ENTRY]
3. Renamed an existing entry in the SOURCE OF INFORMATION (#355.12) file. "E-PHARMACY" was changed to "EPHARMACY".

4. The MCCR Site Parameter Display/Edit [IBJ MCCR SITE PARAMETERS], under the Insurance Verification section was modified to include the new E1 TRANSACTIONS ENABLED (#350.9, 54.05) field. This field is controlled by the users at the site. The action "Send Rx Ins Inquiry" (RX) within the VistA option INITIATE E-PHARMACY ELIGIBILITY INQUIRY (EPI) [IBCNR ELIGIBILITY INQUIRY] will only allow a user to attempt to create an E1 Pharmacy transaction if the E1 TRANSACTIONS ENABLED field is set to "YES". Upon installation, the default for this field is "YES".
5. Modified the functionality of Request Electronic Insurance Inquiry [IBCNE REQUEST INQUIRY] so that the user may enter a date of service up to six years in the past or four months in the future, when allowable by the payer.

5.3 Back-out Criteria

Back-out Criteria (any of the following):

- The project is canceled.
- The requested changes implemented by IB*2.0*822 are no longer desired by VA OIT and the eBusiness eInsurance sub-team.
- The patch produces catastrophic problems.

5.4 Back-out Risks

Since the eInsurance 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) and the Health Care Clearing House (HCCH) to determine risk.

5.5 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 the VHA Finance Financial Management VistA Support Application Coordinator, developers (both project and Tier 3 HSP), and if appropriate, external trading partners such as the VA FSC or HCCH.

eInsurance 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

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.

Back-out Procedure prior to National Release. If it is prior to national release, the site will be already working directly with the development team daily 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 the development team can quickly address via a new software version. If the site is unsure who to contact, they may log a ticket to contact VHA Finance Financial Management VistA Support.

The IB*2.0*822 patch contains the following build components:

- Routines
- Data Dictionaries
- Protocol
- Input Template
- List Template

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, due to the complexity of this patch, it is not recommended for back-out, and a restore from a backup of the Transport Global should not be attempted. In the event that a site decides to back out this patch, the site should contact the Enterprise Service Desk (ESD) to submit a help desk ticket. The development team will need to issue a follow-on patch in order to comprehensively back-out this patch, to clean up corrupted data / remove data dictionary changes, or both, if needed and restore the system to a functioning state.

Please contact the VHA Finance Financial Management VistA Support team for assistance since this installed patch contains components in addition to routines.

5.7 Back-out Verification Procedure

Successful back-out is confirmed by verification that the back-out patch was successfully implemented. This includes successful installation and testing that the back-out acted as expected, as defined together with the team the site contacted in section [5.5](#).

6 Rollback Procedure

Rollback pertains to data. The only data changes in this patch are specific to the operational software and platform settings and they are covered in the Back-out procedures detailed elsewhere in 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.