Medical Care Collection Fund (MCCF) Electronic Data Interchange (EDI) Transaction Applications Suite (TAS) eBilling

Integrated Billing IB*2.0*665

Deployment, Installation, Back-out, and Rollback Guide

March 2022

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
March 2022	1.0	National release version	TAS MCCF eBilling Development Team

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

List of Tables

1 Introduction

This document describes how to deploy and install the patch IB*2.0*665 and 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 IB*2.0*665 will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2 Dependencies

- IB*2.0*650 and IB*2.0*649 must be installed **before** IB*2.0*665.
- Deployment of Transaction Application Suite (TAS) 5.0 or greater.

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	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
5	Individual Veterans Administration Medical Centers (VAMCs)	Installation	Plan and schedule installation	Deployment

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
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	
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 is scheduled to run for 15 days starting with national release.

3.2 Site Readiness Assessment

This section discusses the locations that will receive the IB*2.0*665 deployment.

3.2.1 Deployment Topology (Targeted Architecture)

This patch IB*2.0*665 is to be nationally released to all VAMCs.

3.2.2 Site Information (Locations, Deployment Recipients)

The test sites for IOC testing are:

- Charles George VAMC (Asheville, NC)
- Connecticut HCS (West Haven, CT)
- Michael E. DeBakey VA Medical Center (Houston, TX)
- West Palm Beach VAMC (West Palm Beach, FL)

Upon national release all VAMCs are expected to install this patch prior to or on the compliance date.

3.2.3 Site Preparation

The following table describes preparation required by the "TEST" site prior to deployment.

Table 2: TEST Site Preparation

Site / Other	Problem / Change Needed	Features to Adapt / Modify to New Product	Actions / Steps	Owner
Asheville	Testers need to obtain access to the Test Environment(s)	N/A	Grant the assigned testers the necessary access to the Test Environment(s)	N/A
Connecticut HCS	Testers need to obtain access to the Test Environment(s)	N/A	Grant the assigned testers the necessary access to the Test Environment(s)	N/A
Houston	Testers need to obtain access to the Test Environments	N/A	Grant the assigned testers the necessary access to the Test Environment(s)	N/A
West Palm Beach	Testers need to obtain access to the Test Environments	N/A	Grant the assigned testers the necessary access to the Test Environment(s)	N/A

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

Table 3: 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 4: 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 5: 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 6: 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*649	N/A	Nationally released version	N/A	N/A	N/A
IB*2.0*650	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 eBilling 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 IB*2.0*665, which is tracked nationally for all VAMCs in the NPM in Forum. Forum automatically tracks the patches as they are installed in the different VAMC production systems. A report can be run 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 the chart below.

Table 7: 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

IB*2.0*665, 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, thereby providing Integrated Billing independence from variations in hardware and operating system.

4.2   Platform Installation and Preparation

Refer to the IB*2.0*665 documentation on the National Patch Module (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*665 documentation on the NPM to find related documentation that can be downloaded. IB*2.0*665 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

IB*2.0*665 does not modify the VistA database.

4.5   Installation Scripts

No installation scripts are needed for IB*2.0*665 installation.

4.6 Cron Scripts

No Cron scripts are needed for IB*2.0*665 installation.

4.7 Access Requirements and Skills Needed for the Installation

The following staff will need access to the PackMan message containing the IB*2.0*665 patch or to Forum's NPM for downloading the nationally released IB*2.0*665 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 the IB*2.0*665 documentation on the NPM for detailed installation instructions.

4.9 Installation Verification Procedure

Refer to the IB*2.0*665 documentation on the NPM for specific and 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.

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.

---

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

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 issues, installing the backup of the entire build which was created during installation may be recommended to restore the build components to their pre-patch condition.

5.1.2 After National Release but During the Designated Support Period

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 in Forum and will 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 be used to restore the build components to their original pre-patch condition. If the original patch produces catastrophic issues, installing the backup of the entire build which was created during installation may be recommended to restore the build components to their pre-patch condition.

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.

A backup of the entire build is suggested in the installation instructions. If there are no overlapping components with subsequent builds, that backup of the build can be installed which would restore the system to its original condition. Do not do this without close consultation with the development team in coordination with external trading partners such as the Financial Services Center (FSC) and the Health Care Clearing House (HCCH).

5.2 Back-out Considerations

It is necessary to determine if a wholesale back-out of the patch IB*2.0*665 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). If the back-out is post-release of patch IB*2.0*665, 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

The following features of the IB software will be affected by this patch:

- Enhancements to 277STAT Transactions through TAS

  - Enable 277STAT transactions through the Transaction Application Suite (TAS) technology platform using Fast Healthcare Interoperability Resources (FHIR) instead of legacy proprietary format for Professional, Institutional, and Dental claims.

NOTE: *The 277STAT is an incoming transaction. After installation of this patch, sites will be able to receive the 277STAT using either FHIR or MailMan. After installation of the patch, there will be a controlled implementation as sites are transitioned to FHIR by the Financial Services Center (FSC) in Austin.*

- Enhancements to X12 837 Transactions through TAS

  - Modify VistA to stop the user from sending more than 837 X12 limit of allowable codes - PC1 (Procedure Code) Segment.
  - Modify VistA to stop the user from sending more than 837 X12 limit of allowable codes - VC1 (Value Code) Segment.
  - Modify VistA to stop the user from sending more than 837 X12limit of allowable codes - DC1 (Diagnosis Code) Segment.
  - Modify VistA to stop the user from sending more than 837 X12 limit of allowable codes - CC1 (Condition Code) Segment.
  - Modify VistA to stop the user from sending more than 837 X12 limit of allowable codes - OC1 (Occurrence Code) Segment.
  - Modify VistA to stop the user from sending more than 837 X12 limit of allowable codes - OS1 (Occurrence Span Code) Segment.
  - Allow up to 999 occurrences of the X12 2400 Loop (Revenue Codes) for Institutional claims.

- Miscellaneous Billing enhancements:

  - Improvements to RCB View/Resubmit Claims - Live or Test [IBCE PREV TRANSMITTED CLAIMS] to allow easier selection of claims for resubmission.
  - Principal procedure code must be blank on the second and subsequent pages for printed inpatient UB-04 claims.
  - Modify the Re-Generate Unbilled Amounts Report [IBT RE-GEN UNBILLED REPORT] to include additional non-MCCF Rate Types.

- Defect Fixes:
  - INC20090604 MIAMI: Multiple errors - <SUBSCRIPT>GET+25^IBCE837I

    Problem:

    EDI TRANSMIT BILL (#364) file entry was missing a BILL NUMBER (#.01) field, which points to the BILL/CLAIMS (#399) file. Because of this, a <SUBSCRIPT> error occurred when looking to the 399 file entry with a null subscript. This error stops all claims from being transmitted from the site.

    Resolution:

    Since the File 364 entry doesn't contain any useful data, the entry is deleted so that claims continue to transmit from the site.

  - Back-out of IB*2.0*649 (no tickets logged)

    Problem:

    When ePharmacy entries are made to file# 433, AR TRANSACTION, the system had been using the date of service for the transaction date of each entry. The enhancement causing the defect is to use today's date as the transaction date instead of the date of service. It seems that other functions in the system assume this transaction date to be the date of service, leading to unexpected results.

    Resolution:

    The correction to this defect will be to back-out that enhancement, which is being done as part of this patch.

5.3   Back-out Criteria

The project is canceled, the requested changes implemented by IB*2.0*665 are no longer desired by VA OIT and the Integrated Billing eBusiness team, or the patch produces catastrophic problems.

5.4   Back-out Risks

Since the eBilling 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

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 external trading partners such as FSC and the HCCH to determine the appropriate course of action. eBilling 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 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 IB*2.0*665 patch contains the following build components:

- Routines
- Protocols/Protocol Menu

A backup of the entire build is suggested in the installation instructions. If there are no overlapping components with subsequent builds, that backup of the build can be installed which would restore the system to its original condition. Do not do this without close consultation with the development team in coordination with external trading partners such as the Financial Services Center (FSC) and the Health Care Clearing House (HCCH).

Please contact the EPMO team for guidance.

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. This patch deals with incoming informational status messages.

6.1   Rollback Considerations

Rollback considerations will be based on when the issue is detected and could require a new version of the patch or a subsequent patch if an issue is detected after national release.

6.2   Rollback Criteria

Rollback criteria will be based on when the issue is detected and could require a new version of the patch or a subsequent patch if an issue is detected after national release.

6.3   Rollback Risks

Since the eBilling software is tightly integrated with external systems, any attempt at a roll-back should include close consultation with the external trading partners such as the Financial Services Center (FSC) and the Transaction Application Suite (TAS) team to determine risk.

6.4   Authority for Rollback

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 external

trading partners such as FSC and TAS to determine the appropriate course of action. eBilling is tightly integrated with these external partners and a rollback of the patch should not be a standalone decision.

6.5   Rollback Procedure

The general strategy for a VistA rollback is to repair the data 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.

6.6   Rollback Verification Procedure

Not applicable.