Medical Care Collection Fund (MCCF) Electronic Data Interchange (EDI) Transaction Applications Suite (TAS) eBilling Build 5/6

Integrated Billing IB*2.0*608

Version 2.0

Deployment, Installation, Back-Out, and Rollback Guide

April 2019

Department of Veterans Affairs

Office of Information and Technology (OI&T)

Revision History

Date	Version	Description	Author
April 2019	1.0	Initial Version	REDACTED
April 2019	2.0	IOC completed updates	MCCF EDI TAS 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

Table of Tables

1 Introduction

This document describes how to deploy and install the patch IB*2.0*608 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*608 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*592 and IB*2.0*621 must be installed **before** IB*2.0*608.

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
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 duration of deployment and installation is 30 days, as depicted in the master deployment schedule[1].

3.2 Site Readiness Assessment

This section discusses the locations that will receive the IB*2.0*608 deployment.

3.2.1 Deployment Topology (Targeted Architecture)

This patch IB*2.0*608 is to be nationally released to all VAMCs.

3.2.2 Site Information (Locations, Deployment Recipients)

The test sites for IOC testing are:

- REDACTED

[1] Project schedule (right click and select open hyperlink to access) REDACTED

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
REDACTED	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
REDACTED	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
REDACTED	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
REDACTED	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*592	N/A	Nationally released version	N/A	N/A	N/A
IB*2.0*621	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*608, 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. 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 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*608, 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*608 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*608 documentation on the NPM to find related documentation that can be downloaded. IB*2.0*608 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*608 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 IB*2.0*608 installation.

4.6 Cron Scripts

No Cron scripts are needed for IB*2.0*608 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*608 patch or to Forum's NPM for downloading the nationally released IB*2.0*608 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[2].

4.8 Installation Procedure

Refer to the IB*2.0*608 documentation on the NPM for detailed installation instructions.

4.9 Installation Verification Procedure

Refer to the IB*2.0*608 documentation on the NPM for specific and detailed installation instructions. These instructions include any post installation steps if applicable. The post installation routine will accomplish the following:

- The Post-install (IBY608PO) will automatically generate the one-time Insurance Company EDI Parameter Report and send an email to the eBiz Rapid Response Group, ("REDACTED"). This report will list all of the insurance companies that have the current setting for the Transmit Electronically parameter set to ZERO which equals 'NO'.

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.

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

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.

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

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 OI&T 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.

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*608 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*608, 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

Transmitting SNF Claims with Appropriate Revenue Codes:

- The user should be able to create and transmit a Skilled Nursing Facility (SNF) Institutional claim for Medicare as a primary payer.

- The System should automatically add the new 2400 loop(s) and related segments to the flat file (This should not involve the user; there should be no change for the user).
- The flat file transmission from VistA to FSC should contain Health Insurance Prospective Payment System (HIPPS) Skilled Nursing Facility Rate Code information in the 2400 Loop segment SV202-1.
- The user should be able to see the HP information in the View/Print EDI Bill Extract Data [IBCE EDI VIEW/PRINT EXTRACT] (VPE) option under the INS record ID.
- The Claim should be able to pass the validator at the Financial Service Center (FSC).
- The Claim should be able to process at Medicare with the receipt of an electronic MRA back into the facilities VistA account.

Add T for Transmitted to RCB Screen:

- The user should be able select the option RCB (View/Resubmit Claims - Live or Test [IBCE PREV TRANSMITTED CLAIMS]) to generate a list of previously printed claims for a specified date range.
- The System should show "** T = Test Claim" in the legend at the top of the displayed screen.

Remove Ability to Define Insurance Company as non-EDI:

- The user should be able to select the option EI - "Insurance Company Entry/Edit" [IBCN INSURANCE CO EDIT] to update the Billing/EDI Parameters.
  The available answers for the EDI - Transmit?: prompt should be:
  YES-LIVE
  YES-TEST
  (the choice NO should no longer be available)
- The existing HELP Text should display: "This field determines whether an electronic claim to this insurance Company is sent as a test or a production claim."
- When the IB*2.0*608 patch is installed at a site, a report should be generated and sent to the eBiz Rapid Response group (REDACTED).
- The report should contain the Site Name, Site ID, Date of Report, the Insurance Company Name, the Insurance Company Address, the current setting for the Transmit Electronically field (#3.01) in Insurance Company file (#36) for those payers that have the Transmit Electronically field set to NO.

RCB View/Resubmit Claims - Live or Test [IBCE PREV TRANSMITTED CLAIMS] Screen – Match COB Data to Payer Sequence:

- The user should be able to select the "View/Resubmit Claims - Live or Test" [IBCE PREV TRANSMITTED CLAIMS] (RCB) option.
- The user should be able to select one or more claim entries for resubmission to the Test queue.
- If the user selects a Primary claim to resubmit and the claim has received an EOB/MRA from the primary payer, VistA should not send the COB data from the EOB/MRA and the amount billed should not be offset by previous payments from the primary payer.
- If the user selects a Secondary claim to resubmit and the claim has received an EOB/MRA from the secondary payer, VistA should not send the COB data from the EOB/MRA and the amount billed should not be offset by previous payments from the secondary payer.
- If the user selects a Tertiary claim to resubmit and the claim has received an EOB/MRA from the tertiary payer, VistA should not send the COB data from the EOB/MRA and the amount billed should not be offset by previous payments from the tertiary payer.
- If the user attempts to resubmit a claim(s) with EOB data in VistA to the Production queue, the system should filter out and display the claim number(s) and not transmit it/them.

Non-MCCF Unbilled Amounts Report:

- The user should be able to select the "Re-Generate Unbilled Amounts Report" [IBT RE-GEN UNBILLED REPORT] option.
- The Integrated Billing software should provide the ability for the user to specify the following *additional* search criteria when re-generating the Unbilled Amounts Report and not saving the results:

  CPAC Claims Only
  Non-CPAC Claims (CHAMPVA/TRICARE/INTERAGENCY/INELIGIBLE)
  Both
- CHAMPVA should include the Rate Types equal to “CHAMPVA” and “CHAMPVA REIMB. INS”.
- TRICARE should include the Rate Types equal to “TRICARE” and “TRICARE REIMB. INS”.

Non-MCCF Pay-To Address Rate Types:

- The Integrated Billing software should provide the ability for an authorized user with access to the IB Site Parameters and the TRICARE Pay-to security key, to add a Rate Type for which claims with that Rate Type will use the non-MCCF Pay-To Address data.
- The Integrated Billing software should provide the ability for an authorized user with access to the IB Site Parameters and the TRICARE Pay-to security key, to delete a Rate Type for which claims with that Rate Type will use the non-MCCF Pay-To Address data.
- The Integrated Billing software should use the non-MCCF Pay-To Address data on claims with specified Rate Types only when the non-MCCF Pay-To Address is not exactly the same as the Billing Provider Name and Address.
- The Integrated Billing software should transmit the TRICARE Pay-To Address data on claims with specified Rate Types in the 837-I, 837-P or 837-D when the non-MCCF Pay-To Address is not exactly the same as the Billing Provider Name and Address.
- The Integrated Billing software should print the non-MCCF Pay-To Address data on Institutional claims with specified Rate Types on the UB04 form (FL2) when the TRICARE Pay-To Address is not exactly the same as the Billing Provider Name and Address.
- The Integrated Billing software should print the non-MCCF Pay-To Address data on Professional claims with specified Rate Types on the CMS 1500 form (Box 33) when the non-MCCF Pay-To Address is not exactly the same as the Billing Provider Name and Address.

Remove Fatal Error – Rendering Provider CMS 1500:

- The Integrated Billing software should no longer require a Rendering Provider on Professional claims.
- The Integrated Billing software should display a non-fatal warning message to the user when a Professional claim does not contain a Rendering Provider.

CMN Oxygen and EPN Nutrition:

- The Enter/Edit Billing Information [IB EDIT BILLING INFO] option – The System should conditionally prompt the user for the need on a CMN form for a procedure, based upon those CPTs that are entered into the new “CMN CPT CODE INCLUSIONS” site parameter.
- The Enter/Edit Billing Information [IB EDIT BILLING INFO] option – The System should prompt the user for the type of CMN form when a biller indicates a need for a CMN form (Only 484.3 and 10126 will be available at this time).
- The Enter/Edit Billing Information [IB EDIT BILLING INFO] option – The System should prompt the user for the data elements required to complete the type of CMN form selected.
- Transmit 837-P Transaction – The System should include the CMN related data elements in the outbound Professional 837 transaction.

5.3 Back-Out Criteria

The project is canceled, the requested changes implemented by IB*2.0*608 are no longer desired by VA OI&T 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

Any back-out decision should be a joint decision of the Business Owner (or their representative) and the Program Manager with input from the Health Product Support (HPS) Application Coordinator, developers (both project and Tier 3 HPS), and if appropriate, external trading partners such as the VA FSC or HCCH.

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.

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 development team can quickly address via a new software version. If the site is unsure who to contact, they may log a ticket of contact Health Product Support - Management Systems Team.

The IB*2.0*608 patch contains the following build components.

- Routines
- Protocols
- Modifications to the following files:
    - Insurance File [#36]
    - IB Error File [#350.8]
    - IB Site Parameters File [#350.9]
    - IB Data Element Definition File [#364.5]
    - IB Form Skeleton Definition File [#364.6]
    - IB Form Field Content File [#364.7]
    - Bill/Claims File [#399]
- Data Dictionary Changes
- Modifications to Templates:
    - Input Templates
    - List Templates

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 National Service Desk (NSD) 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 and/or to clean up corrupted data/remove data dictionary changes, if needed and restore the system to a functioning state.

Please contact the EPMO 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 5.7.

6 Rollback Procedure

Rollback pertains to data. The only data changes in this patch are specific to the operational software and platform settings. These data changes 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.