Suicide High Risk Patient Enhancements (SHRPE)

DG*5.3*952 and IVM*2.0*184

Deployment, Installation, Back-Out, and Rollback Guide

Department of Veterans Affairs

February 2020

Version 10.0

Revision History

Date	Version	Description	Author
02/07/2020	10.0	Added missing pre-requisite patch to the 1.2. Dependencies section.	REDACTED
01/15/2020	9.0	Addressed issues reported by HPS.	REDACTED
12/03/2019	8.0	Removed references to DG*5.3*914.	REDACTED
10/03/2019	7.0	Changes for section 5.7 Back-out Verification Procedure.	REDACTED
09/05/2019	6.0	Changed the name of the OTH eligibility from EXPANDED MH CARE NON-VETERANS to EXPANDED MH CARE NON-ENROLLEE: Added new dependencies for DG*5.3*952 Updated KID build filename.	REDACTED
07/18/2019	5.0	IVM*2.0*184 information was added to the document because DG*5.3*952 and the new IVM*2.0*184 patch are bundled and will be installed together.	REDACTED
04/29/2019	4.0	Updated information and instructions regarding new components have been added to the patch.	REDACTED
10/02/2018	3.0	Updated information and instructions regarding new components have been added to the patch.	REDACTED
7/6/2018	2.0	Information and instructions regarding new components have been added to the sections 5.6 and 5.7	REDACTED
4/16/2018	1.0	Initial Draft	REDACTED

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

This document describes how to deploy and install the Veterans Information Systems and Technology Architecture (VistA) Registration patch DG*5.3*952 and Income Verification Match (IVM) patch IVM*2.0*184, 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.

Modifications are needed to VistA to ensure former service members with an Other Than Honorable (OTH) administrative discharge, and their eligibility for emergency mental health care services, are identifiable in the electronic health record, and VA staff can track the former service member's status within a 90-day episode of care.

The current process does not allow the health care team to readily identify a former service member's OTH discharge type and eligibility status in the electronic health record when they are treated under Emergent mental health (MH) care authority.

The current process does not capture and track where the former service member falls within the 90-day episode of care during provision of mental health care.

The current process does not allow the health care team to view former service members with OTH administrative discharges and their eligibility and 90-day status in CPRS for emergency mental health care services.

The challenges to the current process will be addressed with the following enhancements:

- A new EXPANDED MH CARE TYPE value "OTH-90" will be implemented in VistA. This new code identities former service members with an OTH discharge type that are treated under Emergent MH care authority to Veterans Health Administration (VHA) healthcare team members and allows them to be tracked. The new code will display in Registration and CPRS.
- Per VA policy, VHA DIRECTIVE 1601A.02, the former service member is allowed two 90-day episodes of care within a 365-day period. The Veterans Integrated Service Network (VISN) Chief Medical Officer must approve a second 90-day episode of care. The 90-Day Status will consist of a countdown clock to be displayed in CPRS. This clock will inform VHA healthcare team members the number of days remaining within a 90-day episode of care. The countdown clock is initiated at the number 90, decrements by 1 daily, and counts down to zero. A value of 90 indicates that the 90-Day Episode of Care has started, and a value of zero indicates that the 90-Day Episode of Care has expired. New Registration menu options will provide functionality to allow DG staff to manage the OTH clock start dates and enter/edit required authorization for the 2nd 90-days period.
- OTH status displayed on the CPRS screen.

To meet the objectives of these OTH Enhancements (SHRPE), the solution will be deployed in two parts.

The first part is a bundle of the Registration patch DG*5.3*952 and Income Verification Match (IVM) patch IVM*2.0*184, which will:

- Introduce the new EXPANDED MH CARE NON-ENROLLEE eligibility in the ELIGIBILITY CODE (#8) and MAS ELIGIBILITY CODE (#8.1) files.

- Add new EXPANDED MH CARE TYPE (#.5501) field to the PATIENT (#2) file to indicate EXPANDED MH CARE TYPE value "OTH-90" for the Emergent OTH authority.

- Create the new file OTH ELIGIBILITY PATIENT (#33) to track patients eligible for VA care under Emergent OTH authority.

- Add new functionality to the Registration Menu [DG REGISTRATION MENU] option to manage Emergent OTH authority patients. The following menu options and submenus have been added:

      Other Than Honorable Patients Menu [DG OTH MENU]
          OTH Management [DG OTH MANAGEMENT]
          Patient Inquiry (OTH) [DG OTH PATIENT INQUIRY]
          Other Than Honorable Reports [DG OTH REPORTS MENU]
              Tracking Report (OTH-90) [DG OTH 90-DAY PERIOD]
              Authorization Reports (OTH-90) [DG OTH OTH90 AUTH REPORTS]
              Other Than Honorable MH Status Report [DG OTH MH STATUS REPORT]
              Potential 'OTH' Patient Report [DG OTH POTENTIAL OTH]

- Modify the HL7 VistA software to include OTH data in transmissions between VistA and Enrollment System (ES).

- Modify the HL7 messaging to include OTH clock related fields in Z07 HL7 messages that are sent Enrollment System (ES).

- Modify the HL7 messaging code to process OTH clock related fields in Z11 HL7 messages that are sent by ES to VistA.

- Provide the new API to be used by CPRS to provide OTH information to display it on the CPRS screen. The API is covered by the Controlled Subscription ICR (#6873) DG OTH ELIGIBILITY PATIENT STATUSICR.

- Add the new OTH menu to Registration with options to manage the OTH clock.

- Introduce OTH reports.

The second part is delivered with the CPRS v31b patch OR*3.0*377, which will:

- Contain the new OR routine OROTHCL that will use the new DG OTHBTN^DGOTHBTN API introduced by DG*5.3*952.

- Contain a new OR OTHD CLOCK GET RPC that uses the code in OROTHCL to provide OTH clock information to CPRS GUI application.

Please refer to CPRS v31b documentation in regard to deployment, installation, back-out, and rollback instructions.

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 Registration patch DG*5.3*952 and Income Verification Match (IVM) patch IVM*2.0*184 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 Registration routines to provide new functionality that addresses changes for Emergent OTH patients.

- DG*5.3*504, DG*5.3*887, DG*5.3*903, DG*5.3*972 and DG*5.3*978 must be installed before DG*5.3*952.

- IVM*2.0*164 must be installed before IVM*2.0*184.

1.3 Constraints

This patch should be installed in all VA 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 (VAMCs)	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 DG*5.3*952 and IVM*2.0*184 patch deployment.

3.2.1 Deployment Topology (Targeted Architecture)

The VistA Registration patch DG*5.3*952 and IVM*2.0*184 should be installed in all VA VistA production sites.

3.2.2 Site Information (Locations, Deployment Recipients)

The test sites for IOC testing are:
- Atlanta VA Health Care System (508)
- N FL/S GA Health System (573)
- Palo Alto VA Health Care System (640)

Upon national release all VAMCs are expected to install this patch prior to or on the compliance date. The software will be distributed as a host file, which will be posted in ftp sites:
- Hines: fo-hines.med.va.gov
- Salt Lake City: fo-slc.med.va.gov

3.2.3 Site Preparation

No site-specific preparations 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 additional resources required for installation of these 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 will not be impacted by the changes in this project.

Table 4 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

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 Registration package within VistA	N/A	5.3	N/A	N/A	N/A
DG*5.3*504	N/A	Nationally released version	N/A	N/A	N/A
DG*5.3*972	N/A	Nationally released version	N/A	N/A	N/A
DG*5.3*903	N/A	Nationally released version	N/A	N/A	N/A
DG*5.3*978	N/A	Nationally released version	N/A	N/A	N/A

Required Software	Make	Version	Configuration	Manufacturer	Other
IVM*2.0*164	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 "Patch Tracking" message in Outlook 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 patches DG*5.3*952 and IVM*2.0*184, which are 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. 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

DG*5.3*952, a patch to the existing VistA Registration 5.3 package, and IVM*2.0*184, a patch to the existing VistA Income Verification Match 2.0 package, are installable as a bundle (a host file with the combined build) 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 that communicate with the underlying operating system and hardware, thereby providing Registration and Income Verification Match independence from variations in hardware and operating system.

4.2 Platform Installation and Preparation

Refer to the DG*5.3*952 and IVM*2.0*184 Patch Descriptions 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 DG*5.3*952 and IVM*2.0*184 documentation on the NPM to find related documentation that can be downloaded. DG*5.3*952 and IVM*2.0*184 combined build host file DG_53_P952.KID will be made available for downloading from VA sftp sites.

4.4 Database Creation

The patch is applied to an existing MUMPS VistA database.

4.5 Installation Scripts

Refer to the DG*5.3*952 and IVM*2.0*184 Patch Descriptions in the NPM for installation instructions.

4.6 Cron Scripts

No Cron scripts are needed for the DG*5.3*952 and IVM*2.0*184 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 DG 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 DG*5.3*952 and IVM*2.0*184 Patch Descriptions 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 DG*5.3*952 and IVM*2.0*184 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 DG*5.3*952 and IVM*2.0*184 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, in the event that a site decides to back-out this patch, the site should contact the Enterprise Service Desk (ESD) to submit a ticket; the development team will assist with the process.

The Back-Out Procedure consists of restoring routines and manually removing 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 severity of the defects 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 90-day warranty period, 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 DG*5.3*952 and IVM*2.0*184 patches 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 patches will still require a new version (if prior to national release) or a subsequent patch(es) (after national release). If the back-out is post-release of patch DG*5.3*952 and IVM*2.0*184, these patches should be assigned the status of "Entered in Error" in Forum's NPM.

5.2.1 Load Testing

The installation process of the back-out patches, 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 patches can be queued to run during hours of reduced user activity. Subsequent to 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 DG*5.3*952 and IVM*2.0*184 are no longer desired by VA OI&T, or the patches produce catastrophic problems.

5.4   Back-Out Risks

By backing out DG*5.3*952 and IVM*2.0*184 patches, the local facility will not be able to provide SHRPE functionality implemented by the patch:

- Process HL7 messages with OTH data that allows to keep VistA systems and ES in sync in regard to the OTH eligibility and OTH 90-day periods (OTH clocks) across all the VA sites.

- The new EXPANDED MH CARE TYPE value "OTH-90" identities former service members with an OTH discharge type to VHA healthcare team members, that are eligible to receive emergent MH care and allows them to be tracked. The new value will display in Registration and CPRS.

- Per VA policy, the former service member is allowed two 90-day episodes of care within a 365-day period. The VISN Chief Medical Officer must approve a second 90-day episode of care. The 90-Day Status will consist of a countdown clock to be displayed in CPRS. This clock will inform VHA healthcare team members the number of days remaining within a 90-day episode of care. The countdown clock is initiated at the number 90, decrements by 1 daily, and counts down to zero. A value of 90 indicates that the 90-Day Episode of Care has started, and a value of zero indicates that the 90-Day Episode of Care has expired. New Registration menu options will provide functionality to allow DG staff to manage the OTH clock start dates and enter/edit required authorization for the 2nd 90-day period.

- OTH status displayed on the CPRS screen.

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: Portfolio Director, VA Project Manager and Business Owner. Health Product Support will work to identify the problem and assisting with implementation. 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 DG*5.3*952 and IVM*2.0*184 patches contain 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 DG*5.3*952 and IVM*2.0*184 and released after the installation of the DG*5.3*952 and IVM*2.0*184. 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 Health Product Support team after for specific solutions to their unique problems.

- Data dictionaries

The following data dictionaries in the environment need to be restored to their previous state by the back-out patch that needs to be designed for this:

> PATIENT file (#2)
>
> PATIENT ENROLLMENT file (#27.11)
>
> ELIGIBILITY CODE file (#8)
>
> MAS ELIGIBILITY CODE file (#8.1)

The new OTH ELIGIBILITY PATIENT file (#33) can be deleted by the back-out patch that needs to be designed for this.

- Options

The following new entries in the OPTION file (#19) can be deleted by the back-out patch that needs to be designed for this:

```
OPTION NAME
-----------
DG OTH 90-DAY PERIOD
DG OTH MANAGEMENT
DG OTH MENU
DG OTH MH STATUS REPORT
DG OTH OTH90 AUTH REPORTS
DG OTH PATIENT INQUIRY
DG OTH POTENTIAL OTH
DG OTH REPORTS MENU
```

The following entry in the OPTION file (#19) needs to be restored to the previous version by the back-out patch that needs to be designed for this:

```
OPTION NAME
- - - - - - - - - - -
DG REGISTRATION MENU
```

- Protocols

The following new entries in the PROTOCOL file (#101) can be deleted the back-out patch that needs to be designed for this:

```
OPTION NAME

- - - - - - - - - - -

DG OTH ADD 90 DAYS
DG OTH MGMT MENU
DG OTH PATIENT INQUIRY
DG OTH SELECT PATIENT
DG OTH SHOW DETAILS
DG OTH SHOW PENDING
DG OTH VIEW APPROVED
DG OTH VIEW DENIED
```

- Security keys

The following new entries in the SECURITY KEY file (#19.1) can be deleted the back-out patch that needs to be designed for this:

```
SECURITY KEY NAME
- - - - - - - - - - - - - - - -
DG OTH ADD PERIOD
DG OTH MGR
```

- List Template

The following list template can be deleted by the back-out patch that needs to be designed for this.

```
NAME:
- - - - - - - - - - - - - - - - - -
DG OTH MANAGEMENT
```

- Input Template

The following template needs to be restored to the previous version by the back-out patch that needs to be designed for this.

```
NAME:
- - - - - - - - - - - - - - - - - -
DG LOAD EDIT SCREEN 7     FILE #2
```

- Data

The following entry in the ELIGIBILITY CODE file (#8) can be deleted by the back-out patch that needs to be designed for this:

```
NAME:
- - - - - - - - - - - - - - - - - -
```

```
EXPANDED MH CARE NON-ENROLLEE
```

The following entry in the MAS ELIGIBILITY CODE file (#8.1) can be deleted by the back-out patch that needs to be designed for this:

```
NAME:
--------------------
EXPANDED MH CARE NON-ENROLLEE
```

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

If deletion of the new OTH ELIGIBILITY PATIENT file (#33) was performed manually, then the standard FileMan DATA DICTIONARY UTILITIES utility can be used to verify if the file was deleted successfully.

If deletion of the new field EXPANDED MH CARE TYPE (#.5501) in the PATIENT file (#2) was performed manually, then the standard FileMan DATA DICTIONARY UTILITIES utility can be used to verify if the file was updated correctly.

If deletion of the new field EXPANDED MH CARE TYPE (#50.31) in the PATIENT ENROLLMENT file (#27.11) was performed manually, then the standard FileMan DATA DICTIONARY UTILITIES utility can be used to verify if the file was updated correctly.

If deletion of the new entries in the OPTION file (#19) was performed manually, then the standard FileMan INQUIRE TO FILE ENTRIES utility can be used to verify if the entries were deleted successfully.

If deletion of the new entries in the SECURITY KEY file (#19.1) was performed manually, then the standard FileMan INQUIRE TO FILE ENTRIES utility can be used to verify if the entries were deleted successfully.

If deletion of the new entry in the ELIGIBILITY CODE file (#8) was performed manually, then the standard FileMan INQUIRE TO FILE ENTRIES utility can be used to verify if the entry was deleted successfully.

If deletion of the new entry in the MAS ELIGIBILITY CODE file (#8.1) was performed manually, then the standard FileMan INQUIRE TO FILE ENTRIES utility can be used to verify if the entry was deleted successfully.

If deletion of the new entry in the LIST TEMPLATE file (#409.61) was performed manually, then the standard FileMan INQUIRE TO FILE ENTRIES utility can be used to verify if the entry was deleted successfully.

If deletion of the new entries in the PROTOCOL file (#101) was performed manually, then the standard FileMan INQUIRE TO FILE ENTRIES utility can be used to verify if the entries were deleted successfully.

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 DG 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