Existing Product Intake Program (EPIP)

Patch OR\*3.0\*431

Test Evaluation



Department of Veterans Affairs

**November 2016**

Version 1.0

Revision History

**Note**: The revision history cycle begins once changes or enhancements are requested after the Communications Plan has been baselined.

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 11/18/2016 | 1.0 | Initial document. | EPIP Project Team |

Artifact Rationale

The test evaluation document is the primary output of the test and evaluation process, an integral part of the systems engineering process, which identifies levels of performance and assists the developer in correcting deficiencies.

Table of Contents

[1. Test Evaluation Introduction 1](#_Toc467177997)

[1.1. Test Evaluation Scope 1](#_Toc467177998)

[1.2. Test Architecture 1](#_Toc467177999)

[1.3. Test Environment/Configuration 1](#_Toc467178000)

[1.4. Installation Process 2](#_Toc467178001)

[2. Test Data 2](#_Toc467178002)

[3. Issues 2](#_Toc467178003)

[4. Test Execution Log 2](#_Toc467178004)

[5. Test Defect Log 3](#_Toc467178005)

[6. Test Results Summary 3](#_Toc467178006)

[6.1. Defect Severity and Priority Levels 3](#_Toc467178007)

[6.2. Total Defects by Severity Level 3](#_Toc467178008)

[6.3. Breakdown of Test Results 4](#_Toc467178009)

[6.4. Performance Testing 4](#_Toc467178010)

[7. Test Coverage 4](#_Toc467178011)

[7.1. Requirements Covered 4](#_Toc467178012)

[7.2. Section 508 Compliance Coverage 4](#_Toc467178013)

[8. Suggested Actions 4](#_Toc467178014)

[9. Defect Severity and Priority Definitions 5](#_Toc467178015)

[9.1. Defect Severity Level 5](#_Toc467178016)

[9.1.1. Severity Level 1 – Critical 5](#_Toc467178017)

[9.1.2. Severity Level 2 - High 5](#_Toc467178018)

[9.1.3. Severity Level 3 - Medium 6](#_Toc467178019)

[9.1.4. Severity Level 4 - Low 6](#_Toc467178020)

[9.2. Priority Classifications 6](#_Toc467178021)

[9.2.1. Priority 1 - Resolve Immediately 6](#_Toc467178022)

[9.2.2. Priority 2 - Give High Attention 6](#_Toc467178023)

[9.2.3. Priority 3 - Normal Queue 7](#_Toc467178024)

[9.2.4. Priority 4 - Low Priority 7](#_Toc467178025)

[10. Optional Tables, Charts, and Graphs 7](#_Toc467178026)

[11. Document Approval Signatures 8](#_Toc467178027)

[Appendix A - Test Execution Log 9](#_Toc467178028)

[Appendix B – Defect Log 10](#_Toc467178029)

# Test Evaluation Introduction

The purpose of this Test Evaluation is to:

* Identify the testing approach used.
* Present a summary analysis of the key test results from the remediation of this intake for review and assessment by designated stakeholders.
* Provide a general statement of the quality of the system under test.
* Make recommendations for future testing efforts.

## Test Evaluation Scope

The scope of this Test Evaluation is to verify the functionality of the Patch OR\*3.0\*431 code modification, as determined by Functional, Component Integration/System, and Regression testing. Testing activities followed the specifications outlined in the following Master Test Plan**: OR\*3.0\*431 Master Test Plan** (included in Appendix A).

## Test Architecture

Following are the EPIP test accounts used by the Leidos Development and SQA teams to test OR\*3.0\*431.

|  |  |
| --- | --- |
| **Development Test Accounts**  (for Unit Testing) | **SQA Test Accounts**  (for Functional, Regression, and Component Integration and System Testing) |
| VistAS1 ( alternate name: D1S1) | VistAG1 (alternate name: D1G1) |
| VistAS2 (alternate name: D1S2) | VistAG2 (alternate name: D1G2) – for CPRS GUI testing only |

## Test Environment/Configuration

The EPIP test accounts are maintained by the EPIP System Administrator, who installs all VA-released patches as soon as they are nationally released. All EPIP test accounts are cloned from existing VA Enterprise Testing Services (ETS) test accounts. The Computerized Patient Record System (CPRS) Graphical User Interface (GUI) executable is configured for each VistA instance utilizing a unique Internet Protocol (IP) address to connect to the VistA applications. Any updates to the CPRS GUI executable are handled by the EPIP System Administrator.

All EPIP Test Engineers and Developers who have the proper credentials can access the test accounts. The VA Austin Information Technology Center (AITC) support team resets passwords and sets up new access credentials on an as-needed basis.

## Installation Process

As soon as the remediation process is complete and the patch is available for testing, a KIDS build is created in the Development account and then sent to FORUM for final packaging. The patch is then submitted to the VA SQA Lead’s Mailman account for installation.

An EPIP Developer or Test Engineer utilizes the KIDS Installation process to extract the build from the patch and install the build into a test account. The individual who installs the patch verifies the routine checksums and also checks for errors during the installation process. If the patch is successfully installed without any errors, then the EPIP Test team proceeds with Functional, Regression, and Component Integration and System testing. If defects are found, then the Development team works to find a resolution and creates new versions of the patch until all defects are resolved.

# Test Data

The EPIP Test team utilizes the test data in the designated test accounts (D1G1, D1G2).

The test data is encrypted following the standards set forth by the VA Office of Information & Technology (OI&T). All Personally Identifiable Information (PII) and Protected Health Information (PHI) is scrubbed and is not available to the Test Engineers.

All testing is executed using encrypted test patients available from any of the EPIP test accounts. Examples of encrypted test patients:

AAAHURMMX, XPHY

BADHB, HAADXS

FDHUX, YHI J

All tests were executed manually by EPIP Test Engineers.

# Issues

No issues were encountered during testing of OR\*3.0\*431.

| **Title** | **Issue Description** | **Type** | **Severity** |
| --- | --- | --- | --- |
| N/A | N/A | N/A | N/A |

# Test Execution Log

The Test Execution Log records the execution of test scripts and documents the test results for each test script. The Test Engineer is responsible for completing the Test Execution Log.

The Test Execution Records for OR\*3.0\*431 are included in the EPIP Patch OR\*3.0\*431 Master Test Plan. The Master Test Plan is available in Appendix A.

# Test Defect Log

The Test Defect Log is a tool for recording, analyzing, tracking, and documenting the closure of defects. It specifies the Defect ID, affected application, behavior or result that occurred, and the IEEE-defined Severity Level. It includes enough information for the developer to find and re-create the defect. The Defect Log is available in Appendix B.

# Test Results Summary

**NSR20080317 Default Encounter Location** – SQA testing for this NSR started in the Dev1 Gold1 test environment on September 19, 2016 and ended on November 16, 2016. Test version 1 was installed in the test environment after Unit testing was completed. Upon completion of Integration testing (Component Integration and System Testing, Functional Testing, and Regression Testing), one (1) defect was found and reported. This defect was resolved with version 2 of the patch. The new version was retested by the Test Engineer and no other defects were found for this functionality.

**NSR20150608 Accession of Site-Supported Lab Test**  – SQA testing for this NSR started in the Dev1 Gold1 test environment on September 19, 2016 and ended on November 16, 2016. Test version 1 was installed in the test environment after Unit testing was completed. Upon completion of Integration testing (Component Integration and System Testing, Functional Testing, and Regression Testing), zero (0) defects were found and reported.

**NSR20141210 CPRS Pop-Up Box** – SQA testing for this NSR started in the Dev1 Gold1 test environment on September 19, 2016 and ended on November 16, 2016. Test version 1 was installed in the test environment after Unit testing was completed. Upon completion of Integration testing (Component Integration and System Testing, Functional Testing, and Regression Testing), five (5) defects were found and reported. All five defects were resolved with new versions of the patch and retested by the Test Engineer. No other defects were found for this functionality.

## Defect Severity and Priority Levels

A defect is defined as a flaw in a component or system that can cause the component or system to fail to perform its required function, e.g., an incorrect statement or data definition. A defect, if encountered during execution, may cause a failure of the component or system.

Defects are categorized according to severity and priority levels. The test analyst assigns the severity, while the development manager assigns the priority for repair. For more information, see Defect Severity and Priority Definition in this Test Evaluation.

## Total Defects by Severity Level

The following defects were found during testing of Test version 1.

| **Defect Number** | **Severity** |
| --- | --- |
| 419696 | Medium |
| 419712 | Medium |
| 419795 | Medium |
| 419989 | High |
| 419992 | Medium |
| 419996 | Medium |

## Breakdown of Test Results

Testing was completed on November 16, 2016. All test results were recorded in the Rational Quality Manager tool. Detailed results are available in the EPIP Patch OR\*3.0\*431Master Test Plan (see Appendix A).

## Performance Testing

Performance testing was not conducted.

# Test Coverage

The EPIP Patch OR\*3.0\*431 Master Test Plan contains details on test coverage (see Appendix A).

## Requirements Covered

The following Traceability Matrix for Patch OR\*3.0\*431 reports information stored in the Rational tool, such as the total number of requirements and the percentage of requirements covered by executed tests.



## Section 508 Compliance Coverage

Section 508 testing was not required for this patch.

# Suggested Actions

None.

# Defect Severity and Priority Definitions

The classification of defects within a system examines both the severity and priority of the defect.

Severity is a measure of how great the impact is on the user’s ability to complete the documented actions within the system.

Priority determines the speed with which a given defect must be repaired.

Defect classification may be determined either because testing is delayed by a failure in the system or because a cumbersome workaround prevents a user from completing the assigned tasks. Both severity and priority measures must be recorded when scheduling defect resolution tasks.

## Defect Severity Level

The following subsections identify the defect severity levels.

### Severity Level 1 – Critical

Institute of Electrical and Electronics Engineers (IEEE) definition: The defect results in the failure of the complete software system, of a subsystem, or of a software unit (program or module) within the system.

* Any defect that compromises patient safety or system security. Examples of system security defects include breach of confidentiality requirements of the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA), or Federal Tax Information guidelines.
* Loss of system functionality critical to user operations with no suitable workaround, i.e., there is no way to achieve the expected results using the application.
* System crash or hang that prevents further testing or operation of the complete application or a section of the application.
* Any defect that causes corruption of data from a result of the system (as opposed to user error).
* Any defect in which inappropriate transmissions are consistently generated or appropriate transmissions of HL7 messages fail to be generated.
* Loss of functionality resulting in erroneous eligibility/enrollment determinations or communications not being sent.

### Severity Level 2 - High

IEEE definition: The defect results in the failure of the complete software system, of a subsystem, or of a software unit (program or module) within the system. There is no way to make the failed component(s) function. However, there are acceptable processing alternatives which will yield the desired result.

* A major defect in the functionality that does not result in corruption of data.
* A major defect in the functionality resulting in a failure of all or part of the application, where:
* The expected results can temporarily be achieved by alternate means. The customer indicates the work around is acceptable for the short term.
* Any defect that does not conform to Section 508 standards.
* Any defect that results in inaccurate or missing requirements.
* Any defect that results in invalid authentication or authentication of an invalid end user.

### Severity Level 3 - Medium

IEEE definition: The defect does not result in a failure, but causes the system to produce incorrect, incomplete, or inconsistent results, or the defect impairs the systems usability.

* Minor functionality is not working as intended and a workaround exists but is not suitable for long term use
* The inability of a valid user to access the system consistent with granted privileges
* Typographical or grammatical errors in the application, including installation guides, user guides, training manuals, and design documents
* Any defect producing cryptic, incorrect, or inappropriate error messages
* Any defect that results from the use of non-standard data terminology in the application or documentation, as defined by the Department of Veterans Affairs
* Cosmetic issues that are important to the integrity of the product, but do not result in data entry and or data quality problems.

### Severity Level 4 - Low

IEEE definition: The defect does not cause a failure, does not impair usability, and the desired processing results are easily obtained by working around the defect.

* Minor loss of, or defect in the functionality where a long term use exists
* Low-level cosmetic issues.

## Priority Classifications

The following subsections identify the appropriate actions for defects at each priority level, per definitions of IEEE.

### Priority 1 - Resolve Immediately

Further development and/or testing cannot occur until the defect has been repaired. The system cannot be used until the repair has been affected.

### Priority 2 - Give High Attention

The defect must be resolved as soon as possible because it is impairing development and/or testing activities. System use will be severely affected until the defect is fixed.

### Priority 3 - Normal Queue

The defect should be resolved in the normal course of development activities. It can wait until a new build or version is created.

### Priority 4 - Low Priority

The defect is an irritant that should be repaired, but can be repaired after more serious defects have been fixed.

# Optional Tables, Charts, and Graphs

None.

# Document Approval Signatures

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Program/Project Manager Date

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Business Sponsor Representative Date

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Test Lead Date

Appendix A - Test Execution Log

Please refer to the attached OR\*3.0\*431 Master Test Plan to view the Test Execution Records.



Appendix B – Defect Log

Six defects were found during testing of OR\*3.0\*431.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Defect ID** | **Patch Number** | **Affected Application** | **NSR Number** | **Severity** | **Description** | **Status** |
| 419696 | OR\*3.0\*431 | CPRS | 20080317 | Medium | Error occurred when user clicked on Provider Location in CPRS. | Resolved |
| 419712 | OR\*3.0\*431 | VistA | 20141210 | Medium | Missing CPRS Pop-Up Box Flags. | Resolved |
| 419795 | OR\*3.0\*431 | VistA | 20141210 | Medium | Missing “Ineligible” flag for CPRS Pop-Up Box functionality. | Resolved |
| 419989 | OR\*3.0\*431 | CPRS | 20141210 | High | Missing Pop-Up Flags. | Resolved |
| 419992 | OR\*3.0\*431 | VistA | 20141210 | Medium | Code cleanup needed for this NSR. | Resolved |
| 419996 | OR\*3.0\*431 | VistA | 20141210 | Medium | Installation instructions for OR\*3.0\*431 need to be edited. | Resolved |