

Pharmacy Product System (PPS)-N Version 3.0

PSN*4*513

Deployment, Installation, Back-Out, and Rollback Guide



January 2018

Department of Veterans Affairs

Office of Information and Technology (OI&T)

Revision History

| Date | Version | Description | Author |
|------------|---------|--|---|
| 06/12/17 | 2.5 | Incorporated review findings – updated table on page 9-10, section 3.3.1, section 4.11.2, section 6 and 7. | Linda Ellzey |
| 06/09/17 | 2.4 | Updated installation, roll back, and back out sections | Linda Ellzey |
| 05/16/2017 | 2.3 | Updated back out plans and POC | Eric Pace |
| 04/06/2017 | 2.2 | Updated footer, and additional information | Eric Pace |
| 03/17/2017 | 2.1 | Continue updating | Eric Pace |
| 03/09/2017 | 2.0 | Updated prerelease Patch information | Eric Pace |
| 03/08/2017 | 1.9 | Updated test site information | Eric Pace |
| 03/08/2017 | 1.8 | Updated date | Eric Pace |
| 02/03/2017 | 1.7 | Update deployment information | Eric Pace |
| 11/19/2016 | 1.6 | Review of Draft Deployment Plan with PM/IMs | Robert Longo, Douglas Schneider, Eric Pace, Cheryl Spiess |
| 11/3/2015 | 1.5 | Review and updated; sent to IMs for review | Cheryl Spiess |
| 10/16/2015 | 1.4 | Review and updates | Cheryl Spiess |
| 9/21/2015 | 1.3 | Review and updates | Cheryl Spiess |
| 8/14/2015 | 1.2 | Reviewed Draft Deployment Plan and updated | Cheryl Spiess |
| 7/10/2015 | 1.1 | Made changes to Deployment Plan | Cheryl Spiess |
| 6/1/2015 | 1.0 | Development of Deployment Plan PPS-N v3.0 | Eric Pace Cheryl Spiess |

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 5**
 - 1.1. Purpose 5**
 - 1.2. Dependencies 5**
 - 1.3. Constraints 5**
- 2. Roles and Responsibilities..... 6**
- 3. Deployment 7**
 - 3.1. Timeline 7**
 - 3.2. Site Readiness Assessment 7**
 - 3.2.1. Deployment Topology (Targeted Architecture)..... 7**
 - 3.2.2. Site Information (Locations, Deployment Recipients)..... 8**
 - 3.2.3. 3.2.3 Site Preparation 9**
 - 3.3. Resources 9**
 - 3.3.1. Facility Specifics..... 9**
 - 3.3.2. Hardware 10**
 - 3.3.3. Software..... 10**
 - 3.3.4. Communications..... 10**
- 4. Installation 11**
 - 4.1. Pre-installation and System Requirements 11**
 - 4.2. Platform Installation and Preparation 11**
 - 4.3. Download and Extract Files 11**
 - 4.4. Database Creation 11**
 - 4.5. Installation Script..... 11**
 - 4.6. Cron Scripts 11**
 - 4.7. Access Requirements and Skills Needed for the Installation 12**
 - 4.8. Installation Procedure 12**
 - 4.9. Installation Verification Procedure..... 12**
 - 4.10. Post install procedure 13**
 - 4.10.1. Web server and service verification..... 13**
 - 4.10.2. Post-Install Routine (No Action Required) 16**
 - 4.10.3. New PSN PPS ADMIN Security Key (Action Required)..... 17**
 - 4.10.4. New PSN PPS COORD Security Key (Action Required)..... 17**
 - 4.10.5. Open VMS Directory (May Require Action) 17**
 - 4.10.6. LINUX Directory 17**
 - 4.10.7. PPS-N Site Parameters (Enter/Edit) (Action Required)..... 18**
 - 4.10.8. Create a new SSH Key Pair (Action Required) 21**
 - 4.10.9. Mail Group 24**

| | |
|--|-----------|
| 4.10.10. Auditing | 24 |
| 4.11. System Configuration..... | 26 |
| 4.12. Database Tuning | 26 |
| 5. Back-Out Procedure | 27 |
| 5.1. Back-Out Strategy..... | 27 |
| 5.2. Back-Out Considerations | 28 |
| 5.2.1. Load Testing | 28 |
| 5.2.2. User Acceptance Testing | 28 |
| 5.3. Back-Out Criteria | 28 |
| 5.4. Back-Out Risks | 29 |
| 5.5. Authority for Back-Out | 29 |
| 5.6. Back-Out Procedure | 29 |
| 5.7. Back-out Verification Procedure | 30 |
| 6. Rollback Procedure | 33 |
| 6.1. Rollback Considerations..... | 33 |
| 6.2. Rollback Criteria | 33 |
| 6.3. Rollback Risks | 33 |
| 6.4. Authority for Rollback | 33 |
| 6.5. Rollback Procedure | 33 |

1. Introduction

This document describes the plan to deploy and install the Pharmacy Product System (PPS) PPS-N v3.0, as managed through the Pharmacy Reengineering (PRE) Program Office, 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 full Pharmacy Reengineering (PRE) Project Management Plan. The Pharmacy PPS-N v3.0 is intended to complete the development that was started in PPS-N v1.1 and builds upon the v2.0 system, developed previously, but not released to production. It will add improvements to operations, and correct anomalies, defects, and user interface issues that exist in the PPS-N v1.0 and v2.0 systems. The PPS-N v3.0 effort will focus on constructing functionality to update the local copy of the National Drug File NDF Vista files using the PPS-N3.0 data eliminating the need for National Drug File Management System NDFMS to include the patches. The new functionality will eliminate the need to update the national NDF files, increase the timeliness of the local copy of the NDF Vista files, and increase the efficiency of the NDF/local drug file (#50) matching process. In addition, this effort will correct anomalies, defects, and user interface issues, which are critical or require minimal effort to fix.

PPS-N v3.0 will prerelease three patches to prepare for national release in July 2017, these patches will replace the current National Drug File Management System (NDFMS) monthly update functionality via the FORUM patch process.

The PPS-N v3.0 project will replace the Legacy NDFMS with a system that better meets the current and expected business needs and cost effective technical architecture for the VA with faster updates for patient safety. PPS-N v3.0 will provide pharmacy managers with improved work flow, customization, and processes on a scalable platform aligned to VA target architecture. National and Local drug information will update to local sites including updated industry information that allows for better order checks to increase patient safety.

1.1. Purpose

The purpose of this plan is to provide a single common document that describes how, when, where, and to whom the PPS-N v3.0 product will be deployed and installed as well as how it is to be backed out and rolled back, if necessary. Appropriate communications planning has been completed, as well as a rollout schedule. 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

There are no dependencies for the release of the PPS-N v3.0 PSN*4*513 patch.

1.3. Constraints

There are no constraints for release of the PPS-N v3.0 PSN*4*513 patch.

2. Roles and Responsibilities

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

| ID | Team | Phase / Role | Tasks | Project Phase (See Schedule) |
|----|--|-----------------|---|------------------------------|
| | FO, EO | Deployment | Plan and schedule deployment (including orchestration with vendors) | |
| | FO, EO | Deployment | Determine and document the roles and responsibilities of those involved in the deployment. | |
| | FO, EO | Deployment | Test for operational readiness | |
| | FO, EO | Deployment | Execute deployment | |
| | FO, EO | Installation | Plan and schedule installation | |
| | Regional PM/Field Implementation Services (FIS)/Office of Policy and Planning (OPP) PM | Installation | Ensure authority to operate and that certificate authority security documentation is in place | |
| | Regional PM/FIS/OPP PM | Installation | Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes | |
| | | Installations | Coordinate training | |
| | Regional PM/FIS/OPP PM | Back-out | Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out) | |
| | Product Support | Post Deployment | Hardware, Software and System Support | |

Table 2: Roles and Descriptions

| Role | Description | Responsible Party |
|----------------------|--|-------------------|
| Program Manager | Person that has overall responsibility for the successful planning and execution of the PRE Program. | Grant Tucker |
| Project Manager - VA | Person that has overall responsibility for the Government oversight of successful planning and execution of the project. | Heidi Cross (VA) |

| | | |
|-------------------------------|---|--|
| Stakeholders | Persons that hold a stake in a situation in which they may affect or be affected by the outcome. | Lynn Sanders (VA), Don Lees (VA), Deb Coulter (VA) |
| SDE FO Implementation Manager | Develops Deployment Plan and Deployment Tracking Schedule, collaborating with SDE FO IM and contractor IM(s) with implementation and deployment issues. | Douglas Schneider |
| PD Implementation Manager | Develops Deployment Plan and Deployment Tracking Schedule, collaborating with SDE FO IM and contractor IM(s) with implementation and | James Goldsmith |

3. Deployment

PPS will release PSN*4*513 on January 2018. This patch follows the release of PSN*4*396 and PSS*1*195 released in July/August 2017.

PSN*4*513 is the latest part of the ongoing effort to replace the current National Drug File Management System (NDFMS) monthly update functionality via the FORUM patch process.

Other tasks to be done during national deployment:

1. Service Delivery and Engineering (SD&E) will send a bulletin to the field announcing the new PPS-N v3.0 update file process (approximately one (1) month prior to deployment of PPS-N v3.0)
2. NDFMS generated VistA patches will be produced, released, and archived until NDFMS is retired, which should happen after all VA sites have switched to the new automatic download/install of NDF data directly from PPS-N 3.0.

The deployment will be performed by PPS-N project team members along with representatives from peer organizations, as needed. The installation will be performed by Information Resource Management (IRM) staff responsible for VistA administration at local VA Medical Centers (VAMC) and Regional Data Processing Centers (RDPC) and Regional Operations Centers (ROC), where applicable. Facility preparation work will take place prior to national release. SDE FO will ensure site readiness.

3.1. Timeline

The deployment and installation is scheduled to run for 3 months, as depicted in the master deployment schedule.



3.2. Site Readiness Assessment

This section discusses the locations that will receive the PPS-N v3.0 deployment.

3.2.1. Deployment Topology (Targeted Architecture)

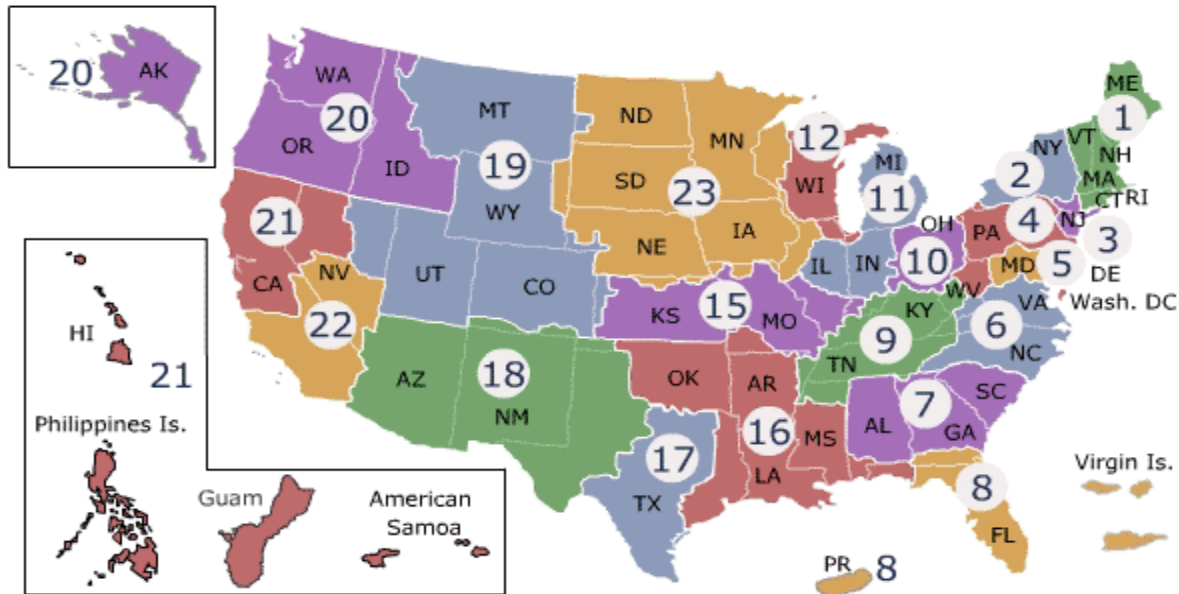
Please refer to section 3.2.2 Site Information.

3.2.2. Site Information (Locations, Deployment Recipients)

The following are the initial test sites:

| Test Site | Address | Pharmacy POC |
|---|---|------------------|
| TUCSAN, AZ (CMOP) | Tucson, AZ 85706 | Jennifer Tidrick |
| Central Plains HCS - VA Nebraska Western Iowa Healthcare System | 4101 Woolworth Ave Omaha, NE 68105 | Kevin Kratz |
| Shreveport, LA - Overton Brooks VAMC | 510 E. Stoner Avenue Shreveport, LA | Matthew Pirkey |
| Big Springs, TX - West Texas HCS | 300 Veterans Blvd Big Spring, TX | Hamp Yearwood |
| VAMC Oklahoma City | 921 NE 13 th , OKC OK, 73104 | Danny Garrett |

Deployment and installation of the PPS-N v3.0 is planned a standard release to all sites.



Veterans Integrated Service Networks (VISN):

VISN 1: VA New England Healthcare System

VISN 2: VA Health Care Upstate New York

VISN 3: VA NY/NJ Veterans Healthcare Network

VISN 4: VA Healthcare - VISN 4

VISN 5: VA Capitol Health Care Network

VISN 6: VA Mid-Atlantic Health Care Network

- VISN7: VA Southeast Network
- VISN 8: VA Sunshine Healthcare Network
- VISN 9: VA Mid-South Healthcare Network
- VISN 10: VA Healthcare System of Ohio
- VISN 11: Veterans In Partnership
- VISN 12: VA Great Lakes Health Care System
- VISN 15: VA Heartland Network
- VISN 16: South Central VA Health Care Network
- VISN 17: VA Heart of Texas Health Care Network
- VISN 18: VA Southwest Health Care Network
- VISN 19: Rocky Mountain Network
- VISN 20: Northwest Network
- VISN 21: Sierra Pacific Network
- VISN 22: Desert Pacific Healthcare Network
- VISN 23: VA Midwest Health Care Network

3.2.3. 3.2.3 Site Preparation

The PPS-N v3.0 will not require site preparation tasks for the pre-release patches. 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 | | | | |

3.3. Resources

Resources involved in the release of the VistA MUMPS patch PSN*4*513 are the assigned Release Coordinators and the project VistA development team. The team will work in coordination with the test site IRMs to install and verify patches.

3.3.1. Facility Specifics

The following table lists facility-specific features required for deployment.

All sites will be polled for site readiness, as listed above, prior to the beginning of deployment.

- Facilities: All VistA parent facilities will be required to install the PPS-N v3.0 Patch PSN*4*513.
- Documentation: Essential documentation is included in the PPS-N v3.0 patch. Additional supporting documentation will be made available via the PRE PPS-N Project SharePoint site and TSPR for informal or working documents and Frequently Asked Questions (FAQs).

The following table lists facility-specific features required for deployment.

Table 4: Facility-Specific Features

| Site | Space/Room | Features Needed | Other |
|------|------------|-----------------|-------|
| 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.

The following table describes hardware specifications required at each site prior to deployment.

Table 5: Hardware Specifications

| Required Hardware | Model | Version | Configuration | Manufacturer | Other |
|-------------------|-------|---------|---------------|--------------|-------|
| 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.

The existing National Drug File Management System (NDFMS), local sites VistA National Drug File (NDF) V. 4.0 package, and Pharmacy Data Management package must be installed and fully patched prior to deployment.

Table 6: Software Specifications

| Required Software | Make | Version | Configuration | Manufacturer | Other |
|-------------------|------|---------|---------------|--------------|-------|
| 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 installation of PPS-N v3.0 and patch installation guides will be distributed to appropriate site staff. Additionally, sites will be provided guidance, prior to implementation, to assure that required file set ups have been completed. Sites will be provided a checklist of pre-implementation activities which must be completed. No other special requirements are necessary.

3.3.4.1 Deployment/Installation/Back-Out Checklist

Table 7 captures the coordination effort and documents the day/time/individual when each activity (deploy, install, back-out) is completed for a project.

Table 7: Deployment/Installation/Back-Out Checklist

| Activity | Day | Time | Individual who completed task |
|----------|-----|------|-------------------------------|
|----------|-----|------|-------------------------------|

| | | | |
|----------|--|--|--|
| Deploy | | | |
| Install | | | |
| Back-Out | | | |

4. Installation

4.1. Pre-installation and System Requirements

The National Drug file V. 4.0 and Pharmacy Data Management (PDM) V. 1.0 relies on a minimum of external packages to be fully patched:

| Package | Minimum Version Needed |
|----------------------------|---|
| VA FileMan | 22.2 |
| Kernel | 8.0 |
| MailMan | 8.0 |
| Pharmacy Data Management | 1.0 |
| National Drug File | 4.0 |
| Web Services Client (HWSC) | 1.0 * XOBW*1*4 patch must be installed. |

The minimum required version for Pharmacy Product System – National (PPS-N) is 1.4.

4.2. Platform Installation and Preparation

Not applicable. No new hardware or other resources are required.

4.3. Download and Extract Files

Make sure that the National Drug File package is fully patched. Refer to the PPS-N v3.0 Installation guide. The PSN*4*513 patch is being released as a FORUM Patch via the Patch Module.

4.4. Database Creation

Not applicable. The patch is applied to an existing M(UMPS) VistA database.

4.5. Installation Script

Refer to the PPS-N v3.0 Installation guide and patch documentation in the NPM for installation instructions.

4.6. Cron Scripts

Not applicable.

Note: within the VistA environment, the installation is at the user's discretion and can either be run immediately in foreground or be scheduled using VA Kernel's Task Manager to execute in background at a selected date and time.

4.7. Access Requirements and Skills Needed for the Installation

Access to National VA Network, as well as the local network of each site, is required to receive PPS-N patches PSN*4*513 and to perform the installation, as well as to have the 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 PSN*4.0*513 patch description documentation on the National Patch Module for the detailed installation steps.

4.9. Installation Verification Procedure

Refer to the PPS-N v3.0 documentation changes and validate the data dictionary changes:

- A site can verify the installation components by validating the additional data dictionary fields defined by utilizing the FileMan List File Attributes [DILIST] option.

Example 1: A high level listing for the PPS-N UPDATE CONTROL file (#57.23):

```
Select OPTION: 8 DATA DICTIONARY UTILITIES
Select DATA DICTIONARY UTILITY OPTION: 1 LIST FILE ATTRIBUTES
START WITH WHAT FILE: VA PRODUCT// 57.23 PPS-N UPDATE CONTROL
                                (1 entry)
GO TO WHAT FILE: PPS-N UPDATE CONTROL//
Select SUB-FILE:
Select LISTING FORMAT: STANDARD// GLOBAL MAP
DEVICE: ;;1000 SSH VIRTUAL TERMINAL Right Margin: 80//
GLOBAL MAP DATA DICTIONARY #57.23 -- PPS-N UPDATE CONTROL FILE
                                OCT 25,2017@14:07:46 PAGE 1
STORED IN ^PS(57.23, (1 ENTRY) SITE: TROY ISC SUPPORT ACCOUNT UCI: FLD,DDV
(VERSION 4.0)
-----
This file contains configuration and installation information for the Pharmacy
Product System - National (PPS-N) file retrieval and installation process.

CROSS
REFERENCED BY: NAME(B)

^PS(57.23,D0,0)= (#.01) NAME [1F] ^ (#1) OPEN VMS LOCAL DIRECTORY [2F] ^ (#2)
==>INSTALL VERSION [3N] ^ (#3) UNIX/LINUX LOCAL DIRECTORY [4F]
==>^ ^ (#5) PRIMARY PPS-N MAIL GROUP [6F] ^ (#8) DOWNLOAD
==>VERSION [7N] ^ (#9) DOWNLOAD STATUS [8S] ^ (#10) INSTALL
==>STATUS [9S] ^ (#45) LEGACY UPDATE PROCESSING [10S] ^
^PS(57.23,D0,1)= (#6) SECONDARY MAIL GROUP [1F] ^
^PS(57.23,D0,2)= (#20) REMOTE SERVER ADDRESS [1F] ^ (#21) REMOTE DIRECTORY
```

```

==>ACCESS [2F] ^ (#22) REMOTE SFTP USER ID [3F] ^
^PS(57.23,D0,3,0)=^57.24P^^ (#30) SCHEDULED OPTION
^PS(57.23,D0,3,D1,0)= (#.01) SCHEDULE OPTIONS [1P:19.2] ^
^PS(57.23,D0,3.1,0)=^57.2331P^^ (#31) MENU OPTIONS
^PS(57.23,D0,3.1,D1,0)= (#.01) MENU OPTIONS [1P:19] ^
^PS(57.23,D0,3.2,0)=^57.2332P^^ (#32) PROTOCOLS
^PS(57.23,D0,3.2,D1,0)= (#.01) PROTOCOLS [1P:101] ^
^PS(57.23,D0,4,0)=^57.234^^ (#50) DOWNLOAD HISTORY
^PS(57.23,D0,4,D1,0)= (#.01) DOWNLOAD FILE NAME [1F] ^ (#1) DOWNLOAD BEGIN
==>DATE/TIME [2D] ^ (#2) DOWNLOAD COMPLETE DATE/TIME [3D]
==>^ (#3) FILE SIZE [4F] ^ (#4) DOWNLOAD ERROR MESSAGE
==>[5F] ^
^PS(57.23,D0,5,0)=^57.231^^ (#100) INSTALL HISTORY
^PS(57.23,D0,5,D1,0)= (#.01) UPDATE FILE NAME [1F] ^ (#1) INSTALL BEGIN
==>DATE/TIME [2D] ^ (#2) INSTALL COMPLETION DATE/TIME [3D]
==>^ (#3) LAST VISTA FILE PROCESSED [4F] ^ (#4) LAST FILE
==>IEN PROCESSED [5F] ^ (#5) LAST TMP FILE SUBSCRIPT [6F]
==>^ (#6) LAST UPDATE FILE SECTION [7F] ^ (#7) DISPLAYED
==>LAST [8F] ^
^PS(57.23,D0,5,D1,2,0)=^57.233D^^ (#30) INSTALL ERRORS
^PS(57.23,D0,5,D1,2,D2,0)= (#.01) ERROR DATE/TIME [1D] ^ (#1) FILE [2F] ^
==>(#2) INTERNAL ENTRY NUMBER [3F] ^ (#3) TMP FILE
==>SUBSCRIPT [4F] ^ (#4) ERROR MESSAGE [5F] ^
^PS(57.23,D0,6,0)=^57.236^^ (#70) REJECT HISTORY
^PS(57.23,D0,6,D1,0)= (#.01) REJECT FILE NAME [1F] ^ (#1) REJECT BEGIN
==>DATE/TIME [2D] ^ (#2) REJECTED BY [3P:200] ^
^PS(57.23,D0,FILE1)= (#39) SFTP SSH KEY FORMAT [1S] ^ (#41) SFTP SSH KEY
==>ENCRYPTION [2S] ^
^PS(57.23,D0,PRVKEY,0)=^57.2333^^ (#33) SFTP PRIVATE KEY TEXT
^PS(57.23,D0,PRVKEY,D1,0)= (#.01) SFTP PRIVATE KEY TEXT [1W] ^
^PS(57.23,D0,PUBKEY,0)=^57.2334^^ (#34) SFTP PUBLIC KEY TEXT
^PS(57.23,D0,PUBKEY,D1,0)= (#.01) SFTP PUBLIC KEY TEXT [1W] ^

INPUT TEMPLATE(S) :

PRINT TEMPLATE(S) :

SORT TEMPLATE(S) :

FORM(S) /BLOCK(S) :

```

4.10. Post install procedure

4.10.1. Web server and service verification

During patch install of PSN*4*513, the PPS-N Web Server and the UPDATE_STATUS web service is defined. These are used to update the installation compliance report on the PPS-N system once sites have installed the PPS-N Update files.

Depending on user access level, the ADPAC or IRM need to make sure the Web Server and Web Service are updated correctly as shown below. You will need to define the correct SERVER during this verification process. When entering data, please make sure that no extra spaces are entered as this will cause communication problems.

Select the Web Server Manager [XOBW WEB SERVER MANAGER] option, and verify the parameters. If a PPSN web server and/or the UPDATE_STATUS web service are not defined, please define them as shown below.

Web Server validation:

```
Select OPTION NAME: XOBW WEB SERVER MANAGER          Web Server Manager
Web Server Manager

Web Server Manager          Jul 20, 2017@16:48:36          Page: 1 of 1
          HWSC Web Server Manager
          Version: 1.0          Build: 9

ID      Web Server Name          IP Address or Domain Name:Port
1      *PPSN          vaausppsapp21.aac.va.gov:443 (SSL)

Legend: *Enabled
AS Add Server          TS (Test Server)
ES Edit Server          WS Web Service Manager
DS Delete Server          CK Check Web Service Availability
EP Expand Entry          LK Lookup Key Manager

Select Action:Quit// ES Edit Server
Select Web Server: 1
NAME: PPSN//
SERVER: vaausppsapp21.aac.va.gov Replace >>> Make sure you have the correct server address.
PORT: 443//          >>> Make sure port number is 443.
DEFAULT HTTP TIMEOUT: 30//
STATUS: ENABLED//

Security Credentials
=====
LOGIN REQUIRED:

SSL Setup
=====
SSL ENABLED: TRUE//          >>> SSL Setup will not be available unless you have the
          XOBW*1*4 patch installed.
SSL CONFIGURATION: encrypt_only// >>> The SSL CONFIGURATION must be set to "encrypt_only".
SSL PORT: 443//          >>> The SSL PORT must be 443.

Authorize Web Services
=====
Select WEB SERVICE: UPDATE_STATUS//
WEB SERVICE: UPDATE_STATUS//
STATUS: ENABLED//
```

Web Service validation:

```
Web Server Manager          Jul 20, 2017@16:54:15          Page: 1 of 1
          HWSC Web Server Manager
          Version: 1.0          Build: 9

ID      Web Server Name          IP Address or Domain Name:Port
1      *PPSN          vaausppsapp21.aac.va.gov:443 (SSL)
```

```

Legend: *Enabled
AS Add Server                TS (Test Server)
ES Edit Server              WS Web Service Manager
DS Delete Server           CK Check Web Service Availability
EP Expand Entry            LK Lookup Key Manager
Select Action:Quit// WS   Web Service Manager

```

```

Web Service Manager          Jul 20, 2017@16:54:18          Page: 1 of 1

```

```

HWSC Web Service Manager
Version: 1.0      Build: 9

```

| ID | Web Service Name | Type | URL Context Root |
|----|------------------|------|------------------|
| 1 | UPDATE_STATUS | REST | /PRE/ndf/update/ |

```

Enter ?? for more actions
AS Add Service
ES Edit Service
DS Delete Service
EP Expand Entry
Select Action:Quit// ES Edit Service
Select Web Service: 1

```

```

=====
5      UPDATE_STATUS          REST    /PRE/ndf/update/
-----

```

```

Name: UPDATE_STATUS
Type: REST
Registered Date/Time:
Context Root: /PRE/ndf/update/
Availability Resource: status

```

```

----- Web servers 'UPDATE_STATUS' is authorized to: -----

```

```

- PPSN

```

```

-----
NAME: UPDATE_STATUS//
DATE REGISTERED:
TYPE: REST//
CONTEXT ROOT: /PRE/ndf/update///

```

AVAILABILITY RESOURCE: status//

Exit back to the main screen and select the CK Check Web Service Availability option and the sequence number for the PPSN web server. The HTTP Response Status Code should be 201. If something other than this is displayed, either the PPSN remoter server is down or the parameters are entered incorrectly. Enter a CA Service desk ticket for “NTL.APP.VistA.Pharmacy National Drug File 4_0“ group, if after checking the information and re-running the CK option results in anything other than HTTP Response Status Code 201.

```
Select OPTION NAME: XOBW WEB SERVER MANAGER           Web Server Manager
Web Server Manager

Web Server Manager           Jul 20, 2017@16:48:36           Page: 1 of 1
                               HWSC Web Server Manager
                               Version: 1.0           Build: 9

ID      Web Server Name           IP Address or Domain Name:Port
-----
1       *PPSN                       vaausppsapp21.aac.va.gov:443 (SSL)

Legend: *Enabled
AS  Add Server                     TS  (Test Server)
ES  Edit Server                     WS  Web Service Manager
DS  Delete Server                   CK  Check Web Service Availability
EP  Expand Entry                    LK  Lookup Key Manager

Select Action:Quit// CK  Check Web Service Availability
Select Web Server: (1-1): 1

Web Service Availability           Oct 25, 2017@13:37:53           Page: 1 of 1
Web Server:
2       *PPSN                       vaausppsapp82.aac.va.gov:443 (SSL)
-----
1 Unable to retrieve 'status' for UPDATE_STATUS
  o HTTP Response Status Code: 201


-----Enter ?? for more actions----->>>

Select Action:Quit//
```

4.10.2. Post-Install Routine (No Action Required)


4.10.3. New PSN PPS ADMIN Security Key (Action Required)

This new Security Key was created to restrict access to the following PPS-N functionalities:

| | |
|---|---|
|  | Action: The new security key PSN PPS ADMIN should be assigned to the National Drug File user responsible for managing the PPS-N functionalities. |
|---|---|

4.10.4. New PSN PPS COORD Security Key (Action Required)

This new Security Key was created to restrict access to the following PPS-N functionalities:

| | |
|---|---|
|  | Action: The new security key PSN PPS COORD should be assigned to the National Drug File coordinator at your site responsible for managing the SSH key and some other critical parameters that affect the download process. |
|---|---|

4.10.5. Open VMS Directory (May Require Action)

| | |
|---|--|
|  | If your site has fully migrated to Linux skip this step. |
|---|--|

If your site has not fully migrated to Linux you will need a new OpenVMS directory (e.g. USER\$:[SFTP.PPSN]) to be used by the data download process. The proposed naming convention is only a recommendation. A more knowledgeable and experienced System Manager may choose to setup the extract directory using existing drives and definitions. The directory name chosen must have the appropriate READ, WRITE, EXECUTE, and DELETE privileges. You must have administrator privileges when you perform this task in order to assure the directory is set up/created with the necessary permissions.


Below is an example that can be followed to create the file transmission directory.

```
$ CREATE/DIRECTORY USER$:[SFTP.PPSN] /own=CACHEMGR  
/PROTECTION=(S:RWED,O:RWED,G:RWED,W:RWED)/LOG
```

NOTE:

- The owner of the directory should be CACHEMGR.
- Where USER\$=the disk of your choice (e.g. USER\$, PQ\$, etc. - SYSS is not recommended).
- Confirm that the extract directory has similar protections and permissions.

```
$DIR/PROT/OWNER PPSN.DIR  
Directory USER$:[000000]  
  
PPSN.DIR;1 [CACHEMGR] (RWED,RWED,RWED,RWED)
```

| | |
|---|--|
|  | Action: Once the directory has been created, please pass this directory name (e.g., “USER\$:[SFTP.PPSN]”) to the ADPAC/Pharmacy Chief/Pharmacy Informatics. This will be used in the PPS-N Site parameters (Enter/Edit) “Outlined Below”. |
|---|--|

4.10.6. LINUX Directory



If your site runs on VMS skip this step.

If you have a LINUX operating system, the PPS-N download process will automatically create a directory to be used by the data download process. However, a more knowledgeable and experienced System Manager may choose to setup the extract directory using existing drives and definitions. The directory name chosen must have the appropriate READ, WRITE, EXECUTE, and DELETE privileges. You must have administrator privileges when you perform this task in order to assure the directory is set up/created with the necessary permissions.

Below is an example that can be followed to create the file transmission directory. Where “directoryPath/Name” is you would enter the path to the directory and the new directory name (i.e. /srv/vista/bham/user/sftp/PPSN/ where bham is the site specific folder).

```
$mkdir /srv/vista/bham/user/sftp/PPSN/
$chmod 777 /srv/vista/bham/user/sftp/PPSN/
$ls -l
  1 drwxrwxrwx.  5 cheyl200 cacheusr          4096 Aug  4 11:13 PPSN
```

NOTE:

- The owner of the directory should be CACHMGR.
- Confirm that the extract directory has similar protections and permissions.



Action: Once the directory has been created, please pass this directory name (e.g., “USER\$:[SFTP.PPSN]”) to the ADPAC/Pharmacy Chief/Pharmacy Informaticist. This will be used in the PPS-N Site parameters (Enter/Edit) “Outlined Below”.

4.10.7. PPS-N Site Parameters (Enter/Edit) (Action Required)

Next, you will need to work with the pharmacy ADPAC to correctly enter the PPS-N Site parameters through the PPS-N Site Parameters (Enter/Edit) [PSN PPS PARAM] option, located under the PPS-N Menu [PSN PPS MENU] which are explained below individually. Sites will be provided with the correct Remote Server information as they are brought on-line with PPS-N processing.



The PPS-N Site Parameters (Enter/Edit) [PSN PPS PARAM] option requires the PSN PPS ADMIN Security Key for editing the parameters (see step 4.2).

```
Select PPS-N Menu <FLD DDEV> Option: SP  PPS-N Site Parameters (Enter/Edit)
```

```
Pharmacy Product System-National(PPS-N) Site Parameters
```

- ```

1. PPS-N Install Version : 29
2. PPS-N Download Version : 29
3. *Open VMS Local Directory : USER$:[ABC]
4. *Unix/Linux Local Directory : /xxx/xxxxxx/xxx/xxxx/xxxx/xxx/PPSN/
5. *Remote Server Address : xxxxxxxxxxxxxxxxxxxx.aac.va.gov
6. *Remote Server Directory : /xxxxxx/xxxxxx/xxxxxx/xxxxxx/approved
7. *Remote SFTP Username : xxxxxxxx
8. Primary PPS-N Mail Group : local_outlook_mail_GROUP@va.gov
```

```
9. Secondary PPS-N Mail group : FIRST.LAST@VA.GOV
10. *PPS-N Account Type : P - Production
11. *Legacy Update Processing : NO
12. *Download Status : NOT IN PROGRESS
13. *Install Status : NOT IN PROGRESS
14. Disable Menus, Options, etc :
```

-----  
Select field number to Edit:



An '\*' (asterisk) before the field name indicates that PSN PPS COORD security key is required for editing these fields/parameters.

### **Install Version Number**

This field contains the current version number of the last successful Pharmacy Product System - National (PPS-N) Update file that was installed. For example if the last PPS-N Update file installed was PPS\_25PRV\_26NEW.DAT, this field would contain 26. When sites are brought on line with PPS-N, this parameter should equate to the last update file created by PPS-N at the time of configuration.

### **Download Version Number**

This field contains the version number for the last Pharmacy Product System - National (PPS-N) Update file downloaded. For example if the last PPS-N Update file downloaded was PPS\_25PRV\_26NEW.DAT, this field would contain 26. When sites are brought on line with PPS-N, this parameter should equate to the last update file created by PPS-N at the time of configuration.

### **OpenVMS Local Directory**

This field should only be defined for sites that run on OpenVMS operating system. The example display above shows both OpenVMS and Linux define only as an example. This field contains the full path directory structure where the PPS-N update file will be stored on the local system after download from the PPS-N server (e.g., USER\$:[SFTP.PPSN]).

### **Unix/Linux Local Directory**

This field should only be defined for sites that run on a Linux operating system. The example display above shows both OpenVMS and Linux define only as an example. This field contains the name of the local Unix/Linux directory where the Pharmacy Product System - National (PPS-N) Update file will be stored on the local system after download from the PPS-N server (e.g. /user/sftp/PPSN/). The option may prompt you for the following after you enter the data and press <Enter> through it:

```
The directory above could not be found.
```

```
Would you like to create it now? N//
```

Answer YES.

### **Remote Server Address**

This is the secure FTP IP address of the Pharmacy Product System-National (PPS-N) server where the PPS-N NDF Update file will be retrieved.

### **Remote Server Directory**

This is the directory name at the Pharmacy Product System-National (PPS-N) server where the PPS-N NDF Update file will be retrieved.

### **Remote SFTP User ID**

This field contains the secure FTP username at the Pharmacy Product System – National (PPS-N) server where the PPS-N NDF Update file will be retrieved.

### **Primary PPS-N Mail Group**

This field is used to store the MS Outlook email group or individual Outlook email address that will receive a copy of the PPS-N update messages. These messages include download and install information, Data Update for NDF report message, Updated Interactions and FDA Med Guide, Drugs Unmatched from National Drug file, Local Drugs Re-matched to NDF, and error messages. The Interactions and Allergies Updated email report will not be sent to Outlook email as it contains patient information. All users of the PSNMGR key will continue to receive the report emails in MailMan.

### **Secondary PPS-N Mail group**

This field is used to store the secondary MS Outlook email group that will receive a copy of the PPS-N update messages. These messages include download and install information, Data Update for NDF report message, Updated Interactions and FDA Med Guide, Drugs Unmatched from National Drug file, Local Drugs Re-matched to NDF, and error messages. The Interactions and Allergies Updated email report will not be sent to Outlook email as it contains patient information. All users of the PSNMGR key will continue to receive the report emails in MailMan.

### **PPS-N Account Type**

This field defines the type of Pharmacy Product System - National (PPS-N) account. The account type can be one of the following: "Q" for National Test SQA system, "T" for Test/Mirror account, "S" for Product Support, "N" for QA NDFMS account, or "P" for Production account. Local VA sites will use "P" for their production accounts and "T" for their test/mirror accounts.

### **Legacy Update**

This field denotes YES or NO if the National Drug File will be updated by the legacy FORUM patch release process or the PPS-N 3.0 Update process. When NO is entered, sites will not be allowed to install patches from legacy FORUM patch process. Only PPS-N update files will be allowed.

### **Download Status**

This field is used to track the status of a PPS-N/NDF Update file download from the PPS-N sftp server. The possible values for this field are:

IN PROGRESS – PPS-N/NDF file is currently being downloaded  
NOT IN PROGRESS - PPS-N/NDF file is not being downloaded

### Install Status

This field is used to track the status of a PPS-N/NDF Update file install into the National Drug file package. The possible values for this field are:

IN PROGRESS – PPS-N/NDF file is currently being installed  
NOT IN PROGRESS - PPS-N/NDF file is not being installed  
DISABLE Scheduled Options, Menu Options and Protocols

Under this field, the site will select scheduled options, menu options, and protocols that needs be marked out of order during the data file installation process.

#### 4.10.8. Create a new SSH Key Pair (Action Required)

Once the PPS-N parameters have been entered the next step is to create a pair of SSH encryption keys that will be used for authenticating the sFTP connection to the PPS-N server automatically bypassing the need for the user to type in a sFTP password. This will enable the data file download from the server. Use the Manage Secure Shell (SSH) Keys [PSN PPS SSH KEY MANAGEMENT] option and follow the steps below:



The Manage Secure Shell (SSH) Keys [PSN PPS SSH KEY MANAGEMENT] option requires the PSN PPS COORD Security Key for creating or deleting SSH Key pairs.

- Verify that you don't have an SSH Key pair in place already. You can use the Action 'V' (View Public SSH Key) for this purpose, as seen in the example below:

```
Select one of the following:

 V View Public SSH Key
 C Create New SSH Key Pair
 D Delete SSH Key Pair
 H Help with SSH Keys

Action: V// v View Public SSH Key

[No SSH Key Pair found]

Press Return to continue:
```

The message [No SSH Key Pair found] displayed above indicates that there are no SSH keys meaning that it is okay to proceed with the creation of a new SSH Key Pair.

- If you are not sure how to create and share the Public SSH Key invoke the Action 'H' for detailed information to help you successfully create and share the key with the PPS-N server. It is recommended that you use RSA.

```
Action: V// h Help with SSH Keys

Secure Shell (SSH) Encryption Keys are used to allow data file download.
Follow the steps below to successfully setup data file download from Austin
```

server to Vista sites:

Step 1: Select the 'C' (Create New SSH Key Pair) Action and follow the prompts to create a new pair of SSH keys. If you already have an existing SSH Key Pair you can skip this step.  
You can check whether you already have an existing SSH Key Pair through the 'V' (View Public SSH Key) Action.

Encryption Type: RSA or DSA?  
-----

Rivest, Shamir & Adleman (RSA) and Digital Signature Algorithm (DSA) are two of the most common encryption algorithms used in IT industry for securely sharing data. The majority of servers can handle either type; however there are some servers that accept only one specific type.

Press Return to continue:

Step 2: Share the Public SSH Key content with the PPS-N SFTP server (Austin). In order to successfully establish the data download files, the SFTP server at Austin needs to install/configure the new SSH Key created in step 1 for the user id they assigned to your site. Use the 'V' (View Public SSH Key) Action to retrieve the content of the Public SSH key. The Public SSH Key should not contain line-feed characters, therefore after you copy & paste it from the terminal emulator into an email or text editor make sure it contains only one line of text (no wrapping).

- Once you have read the Help text above proceed to creating the SSH Key Pair by selecting the Action 'C' (Create New SSH Key Pair)

Action: V// **C** Create New SSH Key Pair

Enter your Current Signature Code: SIGNATURE VERIFIED

Select one of the following:

|     |                                   |
|-----|-----------------------------------|
| RSA | Rivest, Shamir & Adleman (RSA)    |
| DSA | Digital Signature Algorithm (DSA) |

SSH Key Encryption Type: RSA// ?

Rivest, Shamir & Adleman (RSA) and Digital Signature Algorithm (DSA) are two of the most common encryption algorithms used by the IT industry for securely sharing data. The majority of servers can handle either type.

You will need to contact the Austin SFTP server support to determine which type to select.

Select one of the following:

|     |                                   |
|-----|-----------------------------------|
| RSA | Rivest, Shamir & Adleman (RSA)    |
| DSA | Digital Signature Algorithm (DSA) |

SSH Key Encryption Type: RSA// Rivest, Shamir & Adleman (RSA)

Confirm Creation of SSH Keys? NO// YES

```
Creating New SSH Keys, please wait...Done.
```

- Once you have created the new SSH Key Pair use the Action ‘V’ (View Public SSH Key) one more time to retrieve the content of the Public SSH Key so that you can share with the sftp server.

```
Public SSH Key (RSA) content (does not include dash lines):
```

```

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDfdQ3vqmqVKT2V6gn34Q42fGJz7hYgEGaP48Hpxk7u
ZKid0DkUnk4NKI4bf5uwng2TeT5/fPDazUuTRJCWwJ2hmpBaUXJ+y9b+E5jXsjk8cWRz4frjGz38PTE1
J0205eYTwRoAeK9qYxVyBiYd7GJjzZkaNL32P3tFMQfBb09bhdeMwtarkPSo6gh65rXGS+3R4DgU5xFd
QeUU7SGXaVxTEXAsKQagaPIC1Xrk4wFZ8Q3JvDviWHrKXGb3gmg5RWXC7pHTuZf7LRzhBaDYUbqXN+6k
x06CycvB6GanQAflcf1+AO209pdJlJ4DN21A/HDV3BsjNLI926zgMa7ci8kL

```

- Send the key to AITC to be added.



**Action:** You will need to share the text content above (between the dash lines) with Austin SFTP server so they can install it on their server. The Public SSH Key sent to the server should not contain line-feed characters. After you copy & paste it from the terminal emulator into an email or text editor, make sure it contains only one line of text (no wrapping).

The site needs to enter CA Service ticket to the “**EO Linux Sys Admin VHA Team**” group. The SFTP server, **vaausmocftprd01**, should be entered as the Configuration Item.

The description should be something like this:

Add this key to the authorized\_keys file for the presftp user on SFTP server, vaausmocftprd01:

```
ssh-rsa AAAAB3Nza AQDgPrxWImr81RLnAZ0AsuGMok4FinQDgPrx... (rest of key)
```

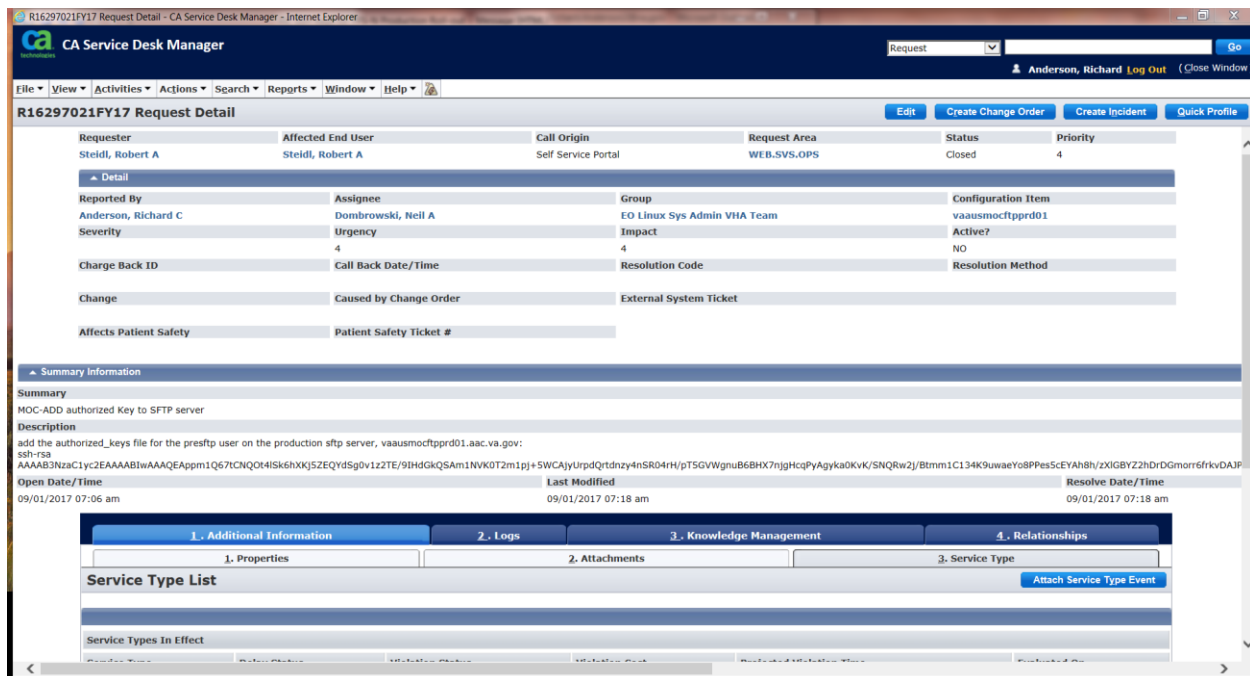


Figure 1: Example screen shot of a request

#### 4.10.9. Mail Group

Sites can set up an Outlook mail group consisting of individuals who need to receive notifications generated during PPS-N Update file processing. Holders of the PSNMGR key will continue to receive email notifications but the Outlook mail group gives flexibility. The Outlook mail group will need to be defined in the PPS-N Site Parameters (Enter/Edit) [PSN PPS PARAM] option.

#### 4.10.10. Auditing

With this patch, the Vista Comparison Report [PSN PPS VISTA COMPARISON RPT] option allows the user to view or print a report of the NDF changes for a date range. This report is meant for National SQA use but if a site wants to utilize this report they will need to turn auditing on for the NDF files. This was not done programmatically and the decision is up to the site if they want to turn on auditing for all fields, since doing so would increase disk space usage. The following example shows how to turn auditing on for fields within a file. For multiple fields, you must list each out to see if the fields are audited. Note that word processing fields cannot be audited. The files utilized for NDF are:

- 50.416 DRUG INGREDIENTS
- 50.6 VA GENERIC
- 50.605 VA DRUG CLASS
- 50.606 DOSAGE FORM
- 50.607 DRUG UNITS
- 50.608 PACKAGE TYPE



- 50.609 PACKAGE SIZE
- 50.64 VA DISPENSE UNIT
- 50.67 NDC/UPN
- 50.68 VA PRODUCT
- 55.95 DRUG MANUFACTURER
- 56 DRUG INTERACTION

Auditing is probably turned on for some of the files but for full utilization of the new option, you would need to turn auditing on for all fields.

```

VA FileMan 22.0

Select OPTION: OTHER OPTIONS
Select OTHER OPTION: ??

 Choose from:
 1 FILEGRAMS
 2 ARCHIVING
 3 AUDITING
 4 SCREENMAN
 5 STATISTICS
 6 EXTRACT DATA TO FILEMAN FILE
 7 DATA EXPORT TO FOREIGN FORMAT
 8 IMPORT DATA
 9 BROWSER

Select OTHER OPTION: AUDITING
Select AUDIT OPTION: ??

 Choose from:
 1 FIELDS BEING AUDITED
 2 DATA DICTIONARIES BEING AUDITED
 3 PURGE DATA AUDITS
 4 PURGE DD AUDITS
 5 TURN DATA AUDIT ON/OFF

Select AUDIT OPTION: 5 TURN DATA AUDIT ON/OFF
AUDIT FROM WHAT FILE: VA PRODUCT// 50.68 VA PRODUCT (27674 entries)
Select FIELD: ??

 Choose from:
 .01 NAME y
 .05 VA GENERIC NAME y
 1 DOSAGE FORM y
 2 STRENGTH y
 3 UNITS y
 4 NATIONAL FORMULARY NAME y
 5 VA PRINT NAME y
 6 VA PRODUCT IDENTIFIER y
 7 TRANSMIT TO CMOP y
 8 VA DISPENSE UNIT y
 11 GCNSEQNO n
 12 PREVIOUS GCNSEQNO n
 13 NDC LINK TO GCNSEQNO y
 14 ACTIVE INGREDIENTS (multiple)
 15 PRIMARY VA DRUG CLASS y
 16 SECONDARY VA DRUG CLASS (multiple)
 17 NATIONAL FORMULARY INDICATOR y

```

```

19 CS FEDERAL SCHEDULE y
20 SINGLE/MULTI SOURCE PRODUCT y
21 INACTIVATION DATE y
23 EXCLUDE DRG-DRG INTERACTION CK y
25 MAX SINGLE DOSE y
26 MIN SINGLE DOSE y
27 MAX DAILY DOSE y
28 MIN DAILY DOSE y
29 MAX CUMULATIVE DOSE y
30 DSS NUMBER y
31 OVERRIDE DF DOSE CHK EXCLUSION y
32 MAXIMUM DAYS SUPPLY y
40 CREATE DEFAULT POSSIBLE DOSAGE y
41 POSSIBLE DOSAGES TO CREATE y
42 PACKAGE y
43 CODING SYSTEM (multiple)
45 COPAY TIER (multiple)
99.98 MASTER ENTRY FOR VUID y
99.99 VUID y
99.991 EFFECTIVE DATE/TIME (multiple)
100 FDA MED GUIDE y
101 HAZARDOUS TO HANDLE y
102 HAZARDOUS TO DISPOSE y
103 PRIMARY EPA CODE y
104 WASTE SORT CODE y
108 CLINICAL EFFECTS OF DRUG (multiple)
109 FORMULARY DESIGNATOR y
2000 SERVICE CODE y

```

```

Select FIELD: 11 GCNSEQNO n
AUDIT: n// YES, ALWAYS

```

```

Select FIELD: 12 PREVIOUS GCNSEQNO n
AUDIT: n// YES, ALWAYS

```

```

Select FIELD: 45 COPAY TIER (multiple)
Select COPAY TIER SUB-FIELD: ??

```

Choose from:

```

.01 COPAY TIER LEVEL y
1 COPAY EFFECTIVE DATE y
2 COPAY END DATE y

```

```

Select COPAY TIER SUB-FIELD:

```

```

Select AUDIT OPTION:

```

```

Select OTHER OPTION:

```

## 4.11. System Configuration

No system configuration is required before or after deployment of PSN\*4\*513.

## 4.12. Database Tuning

Not applicable. No reconfiguration of the VistA database, memory allocation or other resources is necessary.

## 5. Back-Out Procedure

**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 National Service Desk (NSD) to submit a CA SDM ticket; the development team will assist with the process.

The Back-Out Procedure consists of restoring routines, deleting new menu options and security keys and individually removing each new Data Definitions (DD) introduced by patch PSN\*4\*513.

The back-out is to be performed by persons with programmer-level access, and in conjunction with the PPS-N Team.

### 5.1. Back-Out Strategy

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 PPS-N v3.0 VistA functionality rollback will likely be to repair the code with another follow-on patch.

If any issues with PPS-N v3.0 Vista software are discovered after it is nationally released and within the 30 day maintenance window, the PPS-N 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 PPS-N 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 PPS-N v3.0 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.

If the site cannot install the PPS-N NDF Update files, the site can revert back to the legacy FORUM deployed KIDS patches after rollback.

## 5.2. Back-Out Considerations

The back out should only be done in the event that the local facility management determines that the patch PSN\*4.0\*513 is not appropriate for that facility, and should only be done as a last resort.

### 5.2.1. Load Testing

This is not applicable for VistA PPS-N v3.0, the new PPS-N Update Process will replace the legacy FORUM deployed NDF Update KIDS patches.

### 5.2.2. User Acceptance Testing

The development team will work with all of the User Acceptance Testing test sites, answering any questions and resolving any issues until final signoff of all of the participating sites is received. When the results of the User Acceptance Testing are complete, it is documented in the Testing Analysis Report (TAR); the report is located in the Project Notebook for PPS-N v3.0.

**Table 8: User Acceptance Test Site List and Points of Contact**

| <b>Table 3: IOC Test Site Name</b>                 | <b>IT Points of Contact - Installer and Subject Matter Expert (SME) (Tester)</b> |
|----------------------------------------------------|----------------------------------------------------------------------------------|
| TUCSAN, AZ (CMOP)                                  | Amanda Emmendorfer (SME), Jennifer Tidrick (Installer)                           |
| Central Plains HCS                                 | Kevin Kratz (SME), Charles Ivey (installer)                                      |
| Big Springs, TX - West Texas VA Health Care Center | Hamp Yearwood (SME), Brian Moore, Denise Deweese (installer)                     |
| Shreveport, LA                                     | Mathew Pirkey (SME), Chris Ponder (SME), James Erdelt (Installer)                |
| Oklahoma                                           | Danny Garrett (SME), Charles Ivey installer)                                     |

## 5.3. Back-Out Criteria

Facility Systems Management would need to determine if patch PSN\*4\*513 is not appropriate for their facility. The HPS Clinical 1 team may be consulted if needed.

## 5.4. Back-Out Risks

By backing out the PSN\*4\*513 patch, the local facility will not be able to transition to the PPS-N NDF Update procedure when it is subsequently released. This patch provides infrastructure for PPS-N v3.0 which will replace the FORUM NDF patch release process.

## 5.5. Authority for Back-Out

The order would come from the local facility management, IPT Co-Chairs: Robert Longo and PBM.

## 5.6. Back-Out Procedure

The back-out is to be performed by persons with programmer-level access, and in conjunction with the PPS-N Team.

**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 National Service Desk (NSD) to submit a ticket; the development team will assist with the process.

To back out the patch PSN\*4\*513 complete the following steps:

1. Install the backup that you created during installation of the patches.
2. To remove the data dictionary fields complete the following:
  - To delete the PPS-N UPDATE CONTROL file (#57.23), cut and paste the following at the programmers prompt:

```
S DIU="^DIZ (57.23, ",DIU(0)="DES" D EN^DIU2
```

The following is an example of what the screen will look like when running this command:

```
>S DIU="^PS (57.23, ",DIU(0)="DES" D EN^DIU2
 Deleting the DATA DICTIONARY...
>
```

- For PHARMACY SYSTEM file (#59.7), remove the PPS-N NATIONAL SQA ACCOUNT field (#17) by cutting and pasting the following at the programmers prompt:

```
S DIK="^DD (59.7, ",DA=17,DA(1)=59.7 D ^DIK
```

The following is an example of what the screen will look like when running this command:

```
>S DIK="^DD (59.7, ",DA=17,DA(1)=59.7 D ^DIK
>
```

3. Delete all menu options related to PPS-N patch as follows:

```
>D DELETE^XPDMENU ("PSN PPS MENU", "PSN PPS SCHEDULE DOWNLOAD")
>D DELETE^XPDMENU ("PSN PPS MENU", "PSN PPS MANUAL DOWNLOAD")
>D DELETE^XPDMENU ("PSN PPS MENU", "PSN PPS REJECT FILE")
>D DELETE^XPDMENU ("PSN PPS MENU", "PSN PPS PARAM")
>D DELETE^XPDMENU ("PSN PPS MENU", "PSN PPS SCHEDULE INSTALL")
>D DELETE^XPDMENU ("PSN PPS MENU", "PSN PPS MANUAL INSTALL")
>D DELETE^XPDMENU ("PSN PPS MENU", "PSN PPS VISTA COMPARISON RPT")
>D DELETE^XPDMENU ("PSN PPS MENU", "PSN PPS DNLD/INST STATUS REP")
>D DELETE^XPDMENU ("PSN PPS MENU", "PSN PPS SSH KEY MANAGEMENT")
>D DELETE^XPDMENU ("PSNMGR", "PSN PPS MENU")
```

## 5.7. Back-out Verification Procedure

After backing out PSN\*4\*513 , the back-out can be verified by running a global listing from the VistA server command line after installation. Global listings should be performed for the following global nodes, after which nothing should be listed if back-out was successful:

Global ^PS(57.23

Global ^DD(57.23

Example:

```
D ^%G
Device:
Right Margin:
Screen size for paging (0=nopaging)? =>
Global ^ PS(57.23 -- NOTE: translation in effect
<nothing should print>
Global ^ DD(59.7,17 -- NOTE: translation in effect
<nothing should print>
```

The following routines are unique to PPS-N processes and can be removed from the system. If the user has access to Cache Cube, bring each routine up in a Workspace window, highlight the routine and select Edit > Delete. The routine and any generated files are deleted. To delete the routines from programmer's mode, select menu options EVE then Programmer Options then Routine Tools and then Delete Routines. Below is a list of routines unique to PPS-N processing. Once you navigate to the "Routine:" prompt, you can cut and pasted that list at this prompt so that you don't have to enter them individually.

Example of deleting routines:

```
Core Applications ...
Device Management ...
FM VA FileMan ...
Menu Management ...
Programmer Options ...
Operations Management ...
Spool Management ...
Information Security Officer Menu ...
Taskman Management ...
```

```

 User Management ...
 Application Utilities ...
 Capacity Planning ...
 Manage Mailman ...

You have PENDING ALERTS
 Enter "VA to jump to VIEW ALERTS option

You've got PRIORITY mail!

Select Systems Manager Menu <FLD DDEV> Option: Programmer Options

 KIDS Kernel Installation & Distribution System ...
 NTEG Build an 'NTEG' routine for a package
 PG Programmer mode
 Calculate and Show Checksum Values
 Delete Unreferenced Options
 Error Processing ...
 Global Block Count
 List Global
 Map Pointer Relations
 Number base changer
 Routine Tools ...
 Test an option not in your menu
 Verifier Tools Menu ...

You have PENDING ALERTS
 Enter "VA to jump to VIEW ALERTS option

You've got PRIORITY mail!

Select Programmer Options <FLD DDEV> Option: Routine Tools

 %Index of Routines
 Check Routines on Other CPUs
 Compare local/national checksums report
 Compare routines on tape to disk
 Compare two routines
 Delete Routines
 First Line Routine Print
 Flow Chart Entire Routine
 Flow Chart from Entry Point
 Group Routine Edit
 Input routines
 List Routines
 Load/refresh checksum values into ROUTINE file
 Output routines
 Routine Edit
 Routines by Patch Number
 Variable changer
 Version Number Update

You have PENDING ALERTS
 Enter "VA to jump to VIEW ALERTS option

You've got PRIORITY mail!

Select Routine Tools <FLD DDEV> Option: Delete Routines

ROUTINE DELETE

All Routines? No => No

```

```

Routine: PSN513PO
Routine: PSNCFINQ
Routine: PSNCLEAN
Routine: PSNFTP
Routine: PSNFTP2
Routine: PSNFTP3
Routine: PSNOSKEY
Routine: PSNPARM
Routine: PSNPPSCL
Routine: PSNPPSDL
Routine: PSNPPSI1
Routine: PSNPPSI2
Routine: PSNPPSI3
Routine: PSNPPSMG
Routine: PSNPPSMS
Routine: PSNPPSNC
Routine: PSNPPSNF
Routine: PSNPPSNK
Routine: PSNPPSNP
Routine: PSNPPSNR
Routine: PSNPPSNU
Routine: PSNPPSNV
Routine: PSNPPSNW
Routine: PSNVCR
Routine: PSNVCR1
Routine: PSNVCR2
Routine:
26 routines

```

26 routines to DELETE, OK: NO// Y

```

PSN513PO PSNCFINQ PSNCLEAN PSNFTP PSNFTP2 PSNFTP3
PSNOSKEY PSNPARM PSNPPSCL PSNPPSDL PSNPPSI1 PSNPPSI2 PSNPPSI3 PSNPPSMG
PSNPPSMS PSNPPSNC PSNPPSNF PSNPPSNK PSNPPSNP PSNPPSNR PSNPPSNU PSNPPSNV
PSNPPSNW PSNPPSME PSNVCR1 PSNVCR2
Done.

```

### List of routines unique to PPS-N processing:

```

PSN513PO PSNCFINQ PSNCLEAN PSNFTP PSNFTP2 PSNFTP3
PSNOSKEY PSNPARM PSNPPSCL PSNPPSDL PSNPPSI1 PSNPPSI2
PSNPPSI3 PSNPPSMG PSNPPSMS PSNPPSNC PSNPPSNF PSNPPSNK
PSNPPSNP PSNPPSNR PSNPPSNU PSNPPSNV PSNPPSNW
PSNVCR PSNVCR1 PSNVCR2

```

To validate that the routines have been deleted run the routine first line listing which will show no routines:

```
DDEVISC1A1:FLD>D ^%RFIRST
```

Print first line of selected routines or include files.

```

Routine(s): PSNPPS*
Routine(s): PSNOS*
Routine(s): PSNVC*
Routine(s): PSNKIDS*
Routine(s): PSN513*
Routine(s): PSNCFIN*
Routine(s): PSNFTP*
Routine(s): PSNPARM
Routine(s):

```

```
DDEVISC1A1:FLD>
```



## **6. Rollback Procedure**

N/A

### **6.1. Rollback Considerations**

N/A

### **6.2. Rollback Criteria**

N/A

### **6.3. Rollback Risks**

N/A

### **6.4. Authority for Rollback**

N/A

### **6.5. Rollback Procedure**

N/A

## Template Revision History

| Date          | Version | Description                                                                                                                                                                                                                                   | Author                                 |
|---------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| March 2016    | 2.2     | Changed the title from Installation, Back-Out, and Rollback Guide to Deployment and Installation Guide, with the understanding that Back-Out and Rollback belong with Installation.                                                           | VIP Team                               |
| February 2016 | 2.1     | Changed title from Installation, Back-Out, and Rollback Plan to Installation, Back-Out, and Rollback Guide as recommended by OI&T Documentation Standards Committee                                                                           | OI&T Documentation Standards Committee |
| December 2015 | 2.0     | The OI&T Documentation Standards Committee merged the existing <i>“Installation, Back-Out, Rollback Plan”</i> template with the content requirements in the OI&T End-user Documentation Standards for a more comprehensive Installation Plan. | OI&T Documentation Standards Committee |
| February 2015 | 1.0     | Initial Draft                                                                                                                                                                                                                                 | Lifecycle and Release Management       |