RESOURCE AND PATIENT MANAGEMENT SYSTEM

IHS Kernel Toolkit Extensions

(BXT)

User Manual

Version 1.0
September 2014

Office of Information Technology
Division of Information Technology
Albuquerque, New Mexico

Table of Contents

Preface

The purpose of this manual is to provide user information about the IHS Kernel Toolkit Extensions (BXT) package version 1.0. Included in this manual is the information providing instructional guidance to a site managers and other designated staff in the use of the BXT software and its component modules, such as the Parameter Audit System (BXPA) module.

1.0 Introduction

The IHS Kernel Toolkit Extensions application (namespace BXT) is an IHS-developed collection of software designed to enhance and expand the operations and functionality of the software contained in the VA Kernel Toolkit application (namespace XT).

Like its predecessor VA Kernel Toolkit application, the IHS Kernel Toolkit Extensions application contains and manages more than one namespace. In addition to the core BXT namespace, the IHS Kernel Toolkit Extensions application contains the following namespace(s):

BXPA – Parameter Audit System

The Parameter Audit System tracks modifications to individual parameter entries in the Parameter support module of the VA Kernel Toolkit. Individual parameters are not identified for audit; rather, specific classes of parameters are selected to be monitored. RPMS refers to these classes as ***parameter definitions***.

2.0 BXPA - System Navigation

Navigation of the BXT applications's BXPA Parameter Audit System module is based on traditional VA Kernel "roll-and-scroll" interaction, accessed via Telnet or SSH virtual terminal connection.

3.0 BXPA Package Management

Configuration of the BXPA Parameter Audit System consists of identifying specific parameter definitions for monitoring. When a specific parameter definition is selected, all parameters associated with that definition will be audited. Parameter definitions are specified in one of two ways:

A "starter set" of parameter definitions are loaded during the post-install portion of the application's install process into the PARAMETER AUDIT LIST file (#9002026.02). These automatically loaded parameter definitions are:

- ORB PROCESSING FLAG
- ORB SYSTEM ENABLE/DISABLE
- ORK PROCESSING FLAG
- ORK SYSTEM ENABLE/DISABLE
- ORQQPX COVER SHEET REMINDERS

The application manager can specify additional parameter definitions with the **Add a parameter to the audit list (ADPA)** option of the **Parameter Audit System Management (MGPA)** menu:

```
   MGPA   Parameter Audit System Management ...
   RPPA   Parameter Audit Reports ...

Select Parameter Audit System Menu Option: MGPA  Parameter Audit System
Management


   ADPA   Add a parameter to the audit list
   CHPA   Change the audit status of a parameter
   BAPA   Establish a baseline for all parameters

Select Parameter Audit System Management Option: ADPA  Add a parameter to
the audit list
Select the parameter to be audited:
```

4.0 BXPA - Package Operation

Additional user interaction is not required once the desired parameter definitions are selected. Any access to parameters associated with the selected parameter definitions will be recorded in the PARAMETER AUDIT LOG file (#9002026.01).

Once a parameter definition has been specified for auditing, it can never be deleted from the audit list; however, its audit status can be disabled or re-enabled via the **Change the audit status of a parameter (CHPA)** option of the **Parameter Audit System Management (MGPA)** menu:

```
   MGPA   Parameter Audit System Management ...
   RPPA   Parameter Audit Reports ...

Select Parameter Audit System Menu Option: MGPA  Parameter Audit System
Management

   ADPA   Add a parameter to the audit list
   CHPA   Change the audit status of a parameter
   BAPA   Establish a baseline for all parameters

Select Parameter Audit System Management Option: CHPA  Change the audit
status of a parameter
Select the parameter to be changed: ORB PROCESSING FLAG

Current audit status of ORB PROCESSING FLAG is ENABLE.
Do you wish to change this status to DISABLE (Y/N)? Y// YES
```

A time stamped record of a parameter definition’s audit enable/disable status is maintained in the PARAMETER AUDIT LIST file (#9002026.02):

```
Select OPTION: INQUIRE TO FILE ENTRIES



OUTPUT FROM WHAT FILE: PARAMETER AUDIT LIST//
Select PARAMETER AUDIT LIST: ORB PROCESSING FLAG
ANOTHER ONE:
STANDARD CAPTIONED OUTPUT? Yes//   (Yes)
Include COMPUTED fields:  (N/Y/R/B): NO//  - No record number (IEN), no
Computed
 Fields

PARAMETER: ORB PROCESSING FLAG          DATE_TIME ADDED: AUG 28,
2013@20:03:24
  ADDED BY: DENNIS,FLOYD B              ORIG REF ENTRY: ORB PROCESSING FLAG
  CURRENT AUDIT STATUS: DISABLED
TIMESTAMP: SEP 20, 2013@16:24:20        AUDIT STATUS: ENABLED
  STATUS SET BY: DENNIS,FLOYD B
TIMESTAMP: SEP 20, 2013@16:28:38        AUDIT STATUS: DISABLED
  STATUS SET BY: DENNIS,FLOYD B
```

5.0 BXPA - Reporting

Package reporting is accessible via the Parameter Audit Reports (RPPA) option:

- User Parameter Value Report by Date – generates a report of parameter values in effect for a specified user/provider on a given date (default is current date).

```
   MGPA   Parameter Audit System Management ...
   RPPA   Parameter Audit Reports ...

Select Parameter Audit System Menu Option: RPPA  Parameter Audit Reports
```

```
   RUPA   User Parameter Value Report by Date

Select Parameter Audit Reports Option: RUPA  User Parameter Value Report by Date
Select NEW PERSON NAME: fbd  DENNIS,FLOYD B     FBD     DIRM     COMPUTER SPECIA
LIST
Enter effective date/time of report: :  (8/1/2013 - 9/20/2013): NOW//   (SEP 20,
2013@17:34)
DEVICE: HOME// ;P-OTHER80;80;60  VT

PARAMETER SETTINGS FOR  DENNIS,FLOYD B                               09/20/2013
      IN EFFECT ON DATE 09/20/2013                                     PAGE 1
     PARAMETER                           VALUE
-------------------------------------------------------------------------------
1                                        0
ABNORMAL IMAGING RESULTS                 E
ABNORMAL LAB RESULT (INFO)               D
ABNORMAL LAB RESULTS (ACTION)            E
ADMISSION                                D
ALLERGIES UNASSESSIBLE                   E
ALLERGY-CONTRAST MEDIA INTERACTION       E
ALLERGY-DRUG INTERACTION                 E
AMINOGLYCOSIDE ORDERED                   E
BIOCHEM ABNORMALITY FOR CONTRAST MEDIA   E
CLOZAPINE APPROPRIATENESS                D
CONSULT/PROC INTERPRETATION              D
CONSULT/REQUEST CANCEL/HOLD              D
CONSULT/REQUEST RESOLUTION               E
CONSULT/REQUEST UPDATED                  D
CRITICAL DRUG INTERACTION                E
CRITICAL LAB RESULT (INFO)               D
CRITICAL LAB RESULTS (ACTION)            D
CT & MRI PHYSICAL LIMITATIONS            E
CptHistory-cboType                       0
DC ORDER                                 D
DECEASED PATIENT                         D
DISCHARGE                                D
DISPENSE DRUG NOT SELECTED               E
DNR EXPIRING                             D
DUPLICATE DRUG CLASS ORDER               E
DUPLICATE DRUG ORDER                     E
DUPLICATE OPIOID MEDICATIONS             D
DUPLICATE ORDER                          E
ERROR MESSAGE                            E
ESTIMATED CREATININE CLEARANCE           E
FLAG ORDER FOR CLARIFICATION             D
FLAGGED OI EXPIRING - INPT               D
FLAGGED OI EXPIRING - OUTPT              D
FLAGGED OI ORDER - INPT                  D
FLAGGED OI ORDER - OUTPT                 D
```

Appendix A: Rules of Behavior

The Resource and Patient Management (RPMS) system is a United States Department of Health and Human Services (HHS), Indian Health Service (IHS) information system that is ***FOR OFFICIAL USE ONLY***. The RPMS system is subject to monitoring; therefore, no expectation of privacy shall be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

All users (Contractors and IHS Employees) of RPMS will be provided a copy of the Rules of Behavior (RoB) and must acknowledge that they have received and read them prior to being granted access to a RPMS system, in accordance IHS policy.

- For a listing of general ROB for all users, see the most recent edition of *IHS General User Security Handbook* (SOP 06-11a).
- For a listing of system administrators/managers rules, see the most recent edition of the *IHS Technical and Managerial Handbook* (SOP 06-11b).

Both documents are available at this IHS Web site: http://security.ihs.gov/.

The ROB listed in the following sections are specific to RPMS.

A.1 All RPMS Users

In addition to these rules, each application may include additional RoBs that may be defined within the documentation of that application (e.g., Dental, Pharmacy).

A.1.1 Access

RPMS users shall

- Only use data for which you have been granted authorization.
- Only give information to personnel who have access authority and have a need to know.
- Always verify a caller’s identification and job purpose with your supervisor or the entity provided as employer before providing any type of information system access, sensitive information, or nonpublic agency information.
- Be aware that personal use of information resources is authorized on a limited basis within the provisions *Indian Health Manual* Part 8, “Information Resources Management,” Chapter 6, “Limited Personal Use of Information Technology Resources.”

RPMS users shall not

- Retrieve information for someone who does not have authority to access the information.
- Access, research, or change any user account, file, directory, table, or record not required to perform their *official* duties.
- Store sensitive files on a PC hard drive, or portable devices or media, if access to the PC or files cannot be physically or technically limited.
- Exceed their authorized access limits in RPMS by changing information or searching databases beyond the responsibilities of their jobs or by divulging information to anyone not authorized to know that information.

A.1.2 Information Accessibility

RPMS shall restrict access to information based on the type and identity of the user. However, regardless of the type of user, access shall be restricted to the minimum level necessary to perform the job.

RPMS users shall

- Access only those documents they created and those other documents to which they have a valid need-to-know and to which they have specifically granted access through an RPMS application based on their menus (job roles), keys, and FileMan access codes. Some users may be afforded additional privileges based on the functions they perform, such as system administrator or application administrator.
- Acquire a written preauthorization in accordance with IHS policies and procedures prior to interconnection to or transferring data from RPMS.

A.1.3 Accountability

RPMS users shall

- Behave in an ethical, technically proficient, informed, and trustworthy manner.
- Log out of the system whenever they leave the vicinity of their personal computers (PCs).
- Be alert to threats and vulnerabilities in the security of the system.
- Report all security incidents to their local Information System Security Officer (ISSO)
- Differentiate tasks and functions to ensure that no one person has sole access to or control over important resources.
- Protect all sensitive data entrusted to them as part of their government employment.

- Abide by all Department and Agency policies and procedures and guidelines related to ethics, conduct, behavior, and information technology (IT) information processes.

A.1.4 Confidentiality

RPMS users shall

- Be aware of the sensitivity of electronic and hard copy information, and protect it accordingly.
- Store hard copy reports/storage media containing confidential information in a locked room or cabinet.
- Erase sensitive data on storage media prior to reusing or disposing of the media.
- Protect all RPMS terminals from public viewing at all times.
- Abide by all Health Insurance Portability and Accountability Act (HIPAA) regulations to ensure patient confidentiality.

RPMS users shall not

- Allow confidential information to remain on the PC screen when someone who is not authorized to that data is in the vicinity.
- Store sensitive files on a portable device or media without encrypting.

A.1.5 Integrity

RPMS users shall

- Protect their systems against viruses and similar malicious programs.
- Observe all software license agreements.
- Follow industry standard procedures for maintaining and managing RPMS hardware, operating system software, application software, and/or database software and database tables.
- Comply with all copyright regulations and license agreements associated with RPMS software.

RPMS users shall not

- Violate federal copyright laws.
- Install or use unauthorized software within the system libraries or folders.
- Use freeware, shareware, or public domain software on/with the system without their manager’s written permission and without scanning it for viruses first.

A.1.6 System Logon

RPMS users shall

- Have a unique User Identification/Account name and password.
- Be granted access based on authenticating the account name and password entered.
- Be locked out of an account after five successive failed login attempts within a specified time period (e.g., one hour).

A.1.7 Passwords

RPMS users shall

- Change passwords a minimum of every 90 days.
- Create passwords with a minimum of eight characters.
- If the system allows, use a combination of alpha-numeric characters for passwords, with at least one uppercase letter, one lower case letter, and one number. It is recommended, if possible, that a special character also be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or store them in a safe place (do not store passwords in login scripts or batch files).
- Change passwords immediately if password has been seen, guessed, or otherwise compromised, and report the compromise or suspected compromise to their ISSO.
- Keep user identifications (IDs) and passwords confidential.

RPMS users shall not

- Use common words found in any dictionary as a password.
- Use obvious readable passwords or passwords that incorporate personal data elements (e.g., user’s name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Share passwords/IDs with anyone or accept the use of another’s password/ID, even if offered.
- Reuse passwords. A new password must contain no more than five characters per eight characters from the previous password.
- Post passwords.
- Keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.

- Give a password out over the phone.

A.1.8 Backups

RPMS users shall

- Plan for contingencies such as physical disasters, loss of processing, and disclosure of information by preparing alternate work strategies and system recovery mechanisms.
- Make backups of systems and files on a regular, defined basis.
- If possible, store backups away from the system in a secure environment.

A.1.9 Reporting

RPMS users shall

- Contact and inform their ISSO that they have identified an IT security incident and begin the reporting process by providing an IT Incident Reporting Form regarding this incident.
- Report security incidents as detailed in the *IHS Incident Handling Guide* (SOP 05-03).

RPMS users shall not

- Assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident gets reported more than once.

A.1.10 Session Timeouts

RPMS system implements system-based timeouts that back users out of a prompt after no more than 5 minutes of inactivity.

RPMS users shall

- Utilize a screen saver with password protection set to suspend operations at no greater than 10 minutes of inactivity. This will prevent inappropriate access and viewing of any material displayed on the screen after some period of inactivity.

A.1.11 Hardware

RPMS users shall

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).
- Keep an inventory of all system equipment.

- Keep records of maintenance/repairs performed on system equipment.

RPMS users shall not

- Eat or drink near system equipment.

A.1.12 Awareness

RPMS users shall

- Participate in organization-wide security training as required.
- Read and adhere to security information pertaining to system hardware and software.
- Take the annual information security awareness.
- Read all applicable RPMS manuals for the applications used in their jobs.

A.1.13 Remote Access

Each subscriber organization establishes its own policies for determining which employees may work at home or in other remote workplace locations. Any remote work arrangement should include policies that

- Are in writing.
- Provide authentication of the remote user through the use of ID and password or other acceptable technical means.
- Outline the work requirements and the security safeguards and procedures the employee is expected to follow.
- Ensure adequate storage of files, removal, and nonrecovery of temporary files created in processing sensitive data, virus protection, and intrusion detection, and provide physical security for government equipment and sensitive data.
- Establish mechanisms to back up data created and/or stored at alternate work locations.

Remote RPMS users shall

- Remotely access RPMS through a virtual private network (VPN) whenever possible. Use of direct dial in access must be justified and approved in writing and its use secured in accordance with industry best practices or government procedures.

Remote RPMS users shall not

- Disable any encryption established for network, internet, and Web browser communications.

A.2 RPMS Developers

RPMS developers shall

- Always be mindful of protecting the confidentiality, availability, and integrity of RPMS when writing or revising code.
- Always follow the IHS RPMS Programming Standards and Conventions (SAC) when developing for RPMS.
- Only access information or code within the namespaces for which they have been assigned as part of their duties.
- Remember that all RPMS code is the property of the U.S. Government, not the developer.
- Not access live production systems without obtaining appropriate written access, and shall only retain that access for the shortest period possible to accomplish the task that requires the access.
- Observe separation of duties policies and procedures to the fullest extent possible.
- Document or comment all changes to any RPMS software at the time the change or update is made. Documentation shall include the programmer’s initials, date of change, and reason for the change.
- Use checksums or other integrity mechanism when releasing their certified applications to assure the integrity of the routines within their RPMS applications.
- Follow industry best standards for systems they are assigned to develop or maintain, and abide by all Department and Agency policies and procedures.
- Document and implement security processes whenever available.

RPMS developers shall not

- Write any code that adversely impacts RPMS, such as backdoor access, “Easter eggs,” time bombs, or any other malicious code or make inappropriate comments within the code, manuals, or help frames.
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

A.3 Privileged Users

Personnel who have significant access to processes and data in RPMS, such as, system security administrators, systems administrators, and database administrators, have added responsibilities to ensure the secure operation of RPMS.

Privileged RPMS users shall

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government personnel and contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance.
- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to RPMS that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to RPMS.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the ISSO, Chief Information Security Officer (CISO), and systems owner.
- Protect the supervisor, superuser, or system administrator passwords.
- Avoid instances where the same individual has responsibility for several functions (i.e., transaction entry and transaction approval).
- Watch for unscheduled, unusual, and unauthorized programs.
- Help train system users on the appropriate use and security of the system.
- Establish protective controls to ensure the accountability, integrity, confidentiality, and availability of the system.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible from the time that the user is no longer authorized system. Passwords forgotten by their owner should be replaced, not reissued.
- Terminate user accounts when a user transfers or has been terminated. If the user has authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel logon IDs and passwords, and delete or reassign related active and backup files.

- Use a suspend program to prevent an unauthorized user from logging on with the current user's ID if the system is left on and unattended.
- Verify the identity of the user when resetting passwords. This can be done either in person or having the user answer a question that can be compared to one in the administrator’s database.
- Shall follow industry best standards for systems they are assigned to, and abide by all Department and Agency policies and procedures.

Privileged RPMS users shall not

- Access any files, records, systems, etc., that are not explicitly needed to perform their duties
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

Glossary

BXPA

The Parameter Audit System module of the IHS Kernel Toolkit Extensions application.

Parameter

A user-definable data object which can be used to customize the operational characteristics of a software application. A single parameter may have multiple values depending upon the entity with which the parameter is being associated for a specific operation.

Parameter Entity

A particular person/group/class for which a specific parameter value setting may be identified.

Parameter Instance

The internal database identification of a specific parameter value in relation to a particular parameter entity.

Parameter Value

The content defined for a specific parameter when used in conjunction with a particular parameter entity.

Acronym List

CAC	Clinical Applications Coordinator
CMS	Centers for Medicare and Medicaid Services
EHR	Electronic Health Record
IHS	Indian Health Service
ISSO	Information Systems Security Officer
PHI	Protected Health Information
PII	Personally Identifiable Information
RPMS	Resource and Patient Management System
VA	Department of Veterans Affairs (formerly known as the Veterans Administration)

Contact Information

If you have any questions or comments regarding this distribution, please contact the OIT Help Desk (IHS).

Phone: (888) 830-7280 (toll free)

Web: http://www.ihs.gov/helpdesk/

Email: support@ihs.gov