RESOURCE AND PATIENT MANAGEMENT SYSTEM

# IHS Pharmacy Modifications

# (APSP)

## Supplemental User Guide

Version 7.0 Patch 1033
July 2023

Office of Information Technology
Division of Information Technology

# Table of Contents

# Preface

The purpose of this guide is to provide the user with information needed to utilize new functionality introduced by IHS Pharmacy Modifications (APSP) Version 7.0 Patch 1033.

This guide contains reference information about new processes and step-by-step instructions to show users how to configure systems to utilize Clinic BarCode Medication Administration (BCMA) and functionality introduced by APSP v7.0 p1033.

# 1.0 Introduction

APSP v7.0 p1033 expands the functionality of Bar Code Medication Administration (BCMA) from its previous hardcoded limitation of patients with admitted or observation status (i.e., inpatients) to include ambulatory status (i.e., outpatients).

This patch adds Clinic BCMA report functionality, use of fractional BCMA Units Per Dose in Local Possible Dosages, prohibits leading and trailing zeros in syringe size in RPMS Inpatient Pharmacy, adds a warning in Inpatient Pharmacy package when processing Clinic medication orders for an admitted patient, drops the @NUMBER display for bolus and titration IV orders, adds support for the display of Patient Preferred Name in BCMA, and allows for the use and display of commas in day of the week schedules.

- Bar Code Medication Administration (BCMA):
  - Bar Code Medication Administration (BCMA) is a point-of-care application for validation of medication administration that supports "real-time" recording of medications administered to patients.
  - Use of an electronic medication administration record with bar code scanning verifies patient identity as well as ensuring that the patient receives the right medication, in the right dose, via the right route at the right time (commonly known as "The Five Rights").
  - BCMA was designed to augment patient safety in the administration of medication by providing checks and safeguards, but was not intended to be a replacement for the clinical judgment of the medication administrator.
  - BCMA provides a familiar graphical interface that works with the Resource and Patient Management System (RPMS) database and the Electronic Health Record (EHR) to both record medication administration and then make that information easily accessible to users of RPMS and EHR. BCMA is fully integrated with RPMS and EHR and medication changes made by providers in EHR are reflected in BCMA as soon as the order is processed. Similarly, when a medication is administered using BCMA the information is viewable in RPMS and EHR immediately.
  - BCMA supports functions such as:
    - Identification of the patient by scanning a barcoded wristband
    - Recording administration of scheduled medications including topical, unit dose, IV push, and IV piggyback medications
    - Recording administration and effectiveness of PRN Medications
    - Recording administration and management of continuous IV Fluids

- Prevention of incorrect administrations by positively identifying medications with bar codes
- Generation of lists of due medications
- Generation of lists of "missed" medications (i.e., those not recorded as administered when due)
- Generation of medication variance reports for quality improvement

- This application uses the “AUPN DISPLAY PPN” parameter functionality and is defaulted to OFF until Patient Preferred Name (PPN) is available across the enterprise.

> **Note**: While this parameter is turned off, the Patient Preferred Name will not display in this application. This allows the Patient Preferred Name display to be turned on at once without requiring a coordinated release of all applications. Once all applications support the display of the PPN, instructions will be sent out on how to enable this parameter system-wide.

# 2.0 System Navigation

Clinic BCMA and Clinic BCMA Report functionality are dependent on the existing installation of BCMA.

The current BCMA software version is PSB*3.0*42.

The GUI workstation software is a controlled release and will be installed as it is deployed at individual hospitals. These applications include PSB3_0P42.EXE and XWB1_1P29PG.EXE.

To utilize Clinic BCMA and Clinic BCMA Reports sites will have to enable Administer Inpatient Meds in the Hospital Location file and Send to BCMA in the Clinic Definition file.

## 2.1 Clinic BCMA: Enable Administer Inpatient Meds

Clinic BCMA is dependent on the use of Inpatient Medications for Outpatient (IMO) functionality which was introduced in EHR Version 1.1 Patch 12.

In RPMS:

```
Select VA FileMan <TEST ACCOUNT> Option: Enter or Edit File Entries
INPUT TO WHAT FILE: HOSPITAL LOCATION
EDIT WHICH FIELD: ALL// ADMINISTER INPATIENT MEDS
THEN EDIT FIELD: {ENTER}
Select HOSPITAL LOCATION NAME: YOUR AMBULATORY LOCATION NAME
ADMINISTER INPATIENT MEDS?: YES
```

Figure 2-1: Clinic BCMA: Enable Administer Inpatient Meds

## 2.2 Clinic BCMA: Set Send to BCMA to YES

Send to BCMA has to be set to YES in the Clinic Definition for the ambulatory location where Clinic BCMA will be utilized.

In RPMS:

```
Select VA FileMan <TEST ACCOUNT> Option: Enter or Edit File Entries
INPUT TO WHAT FILE: CLINIC DEFINITION//
EDIT WHICH FIELD: SEND TO BCMA
Select CLINIC DEFINITION: YOUR AMBULATORY LOCATION NAME
CLINIC: YOUR AMBULATORY LOCATION NAME
SEND TO BCMA?: YES
```

Figure 2-2: Clinic BCMA: Set Send to BCMA to YES

## 2.3 Clinic BCMA Reports

BCMA Reports have been updated to support reporting of most Clinic BCMA data. Certain BCMA reports and report options rely specifically on patient ward location and to return results. Since Clinic BCMA is utilized for patients who are in an ambulatory status certain BCMA reports and report options will not function for Clinic BCMA patients.

BCMA Reports that will NOT return data for Clinic BCMA and patients with ambulatory status include:

- IV Bag Status Report generated using Print by Ward: Sort by Patient
- Medication Variance Report generated by Ward
- Unable to Scan Report – Detailed and Summary – for Wristband data

## 2.4 Update Day-of-Week Schedules to Support Use and Display of Commas in Inpatient Orders

Day of Week Schedules have been updated to support the use and display of commas in inpatient orders and in BCMA.

Use of commas instead of dashes in Day of Week schedules is optional. The functionality is intended to prevent confusion with interpreting a dash as “through” instead of “and” by users when reading Day of Week medication orders.

Sites that elect to utilize commas in Day of Week schedules will need to build new Day of Week schedules. Sites should not edit existing Day of Week schedules that use a dash as this will have negative consequences on existing Day of Week medication orders utilizing those schedules.

Example in RPMS:

```
Select Standard Schedule Management <TEST ACCOUNT> Option: Standard Schedule Edit

Select ADMINISTRATION SCHEDULE: MO,SA
  Are you adding 'MO,SA' as a new ADMINISTRATION SCHEDULE (the 39TH)? No// Y
  (Yes)
NAME: MO,SA//
OUTPATIENT EXPANSION: ON MONDAYS AND SATURDAYS
OTHER LANGUAGE EXPANSION:
TYPE OF SCHEDULE: CONTINUOUS// DAY OF THE WEEK
STANDARD ADMINISTRATION TIMES: 0900
```

Figure 2-3: Update Day of Week Schedules to Support Use and Display of Commas in Inpatient Orders

# 3.0 Package Management

See https://www.ihs.gov/rpms/applications/clinical/ for patch installation notes.

# 4.0 Package Operation

APSP v7.0 p1033 expands the functionality of existing Bar Code Medication Administration (BCMA) from its previous hardcoded limitation of patients with admitted or observation status (i.e., inpatients) to include ambulatory status (i.e., outpatients).

Users should refer to https://www.ihs.gov/bcma/resources/ for BCMA specific user and technical manuals.

# 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 website:
https://home.ihs.gov/security/index.cfm.

> **Note**: Users must be logged on to the IHS D1 Intranet to access these documents.

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

### APSP

The namespace of the IHS modifications to the Outpatient Pharmacy Suite.

### Backdoor Entry

The process of entering a Backdoor Order in the RPMS Pharmacy options.

### Backdoor Order

A pharmacy order that is not entered using RPMS EHR but is entered by the pharmacist using the RPMS Pharmacy options.

### BCMA

Point of care application for validation of medication administration.

### Caret

A circumflex, also known as “up caret,” “hat,” or “up-hat,” resembling an inverted V or chevron. On most standard English language keyboards, created using the key combination Shift-6: ^.

### Day of Week Schedule

Medication schedule for medications that are intended to be administered only on specific days of the week.

### Dose Unit

The unit of measure used for a specific dose of medication. Examples include but are not limited to tablet, capsule, teaspoonful, gram, and milliliter.

### eRx

Electronic prescribing or an electronic prescription.

### Inpatient Medications for Outpatient

Functionality that enables the ordering of unit dose medications for patients in an ambulatory setting

### Intravenous Medications

Medications that are administered into a vein. For RPMS, the Pharmacy package that manages these types of medications for patients.

### Leading Zeros

For the purposes of EHR and RPMS validation, one or more zeros to the left of a decimal point in a positive number that is less than 1. Example: 0.5

### Local Possible Dose

A dose created in a local instance of the RPMS Pharmacy Data Management package that is free text.

### Outpatient Medications

Medications primarily meant to be dispensed or administered to patients who are not admitted to a hospital unit or ward. For RPMS, the Pharmacy package that manages these types of medications for patients.

### Pending Order

A medication order that has been input into the system and signed by the provider, but which has not yet been processed by Pharmacy.

### Possible Dose

A dose created in a local instance of the RPMS Pharmacy Data Management package that is a function of the numerical dose and the strength of the drug recorded in the system. Possible doses may be limited to inpatient use for some medications.

### PRN

As needed.

### Rx or Rxs

A prescription or prescriptions.

### Trailing Zeros

For the purposes of this validation, one or more zeros in a decimal number after which no other numbers follow. Example: 5.0.

### Unit Dose Medications

Medications that are specifically packaged in premeasured doses for single use. For RPMS, the Pharmacy package that manages non-IV versions of these types of medications for patients.

### Units Per Dose

The number of units of a medication that are required for administration to achieve the ordered dose.

# Acronym List

| Acronym | Term Meaning |
|---|---|
| BCMA | BarCode Medication Administration |
| CISO | Chief Information Security Officer |
| EHR | Electronic Health Record |
| FM | FileMan |
| GUI | Graphical User Interface |
| HHS | Health and Human Services |
| IHS | Indian Health Service |
| IMO | Inpatient Medications for Outpatient |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| IV | Intravenous |
| PC | Personal Computer |
| PPN | Patient Preferred Name |
| ROB | Rules of Behavior |
| RPMS | Resource and Patient Management System |
| SAC | Standards and Conventions |
| VA | Veteran's Administration |
| VPN | Virtual Private Network |

# Contact Information

If you have any questions or comments regarding this distribution, please contact the IHS IT Service Desk.

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

**Web:** https://www.ihs.gov/itsupport/

**Email:** itsupport@ihs.gov