RESOURCE AND PATIENT MANAGEMENT SYSTEM

Electronic Health Record

(EHR)

Patch Guide

Version 1.1 Patch 34
October 2022

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

The purpose of this manual is to provide the user with guidance on changes and needed configuration updates for functionality included in **EHR v1.1p34**.

Recommended Users

This document addresses the needs of Clinical Application Coordinators (CACs), as well as end-users of the Indian Health Service (IHS) Resource Patient Management System (RPMS) Electronic Health Record (EHR).

Required Configuration

Configuration is required before utilization of the new functionality and updated components. Refer to the *Electronic Health Record (EHR) Setup Guide*, **EHR v1.1p34** for configuration instructions before using this User Guide.

Important:	Read each **Notes** file (**.n**) associated with the patches coinciding the national re lease of **EHR v1.1 p34**.

1.0 Introduction

This guide provides the **Clinical Applications Site Coordinator (CAC)** instructions on implementing new functionality available in the **EHR v1.1 P34**.

1.1 Overview of Changes

1.2 Enhancements

EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. **EHRs** not only contain the medical and treatment histories of patients, but the **EHR** system is built to scale, go beyond standard clinical data collected aiding in providers ability to manage care and patient volumes in a better capacity, which is also inclusive of a broader view of a patient's care/service needs. IHS strives to add changes to the **RPMS EHR** with every national release as patients and care are in the forefront of leadership decisions.

- ***BMAG Incorporation into EHR***

  Incorporation in the RPMS EHR for BMAG changes that provide an ability to view associated administrative image files and other 'CLIN' image files not attached to a TIU note. It will further reduce the need to access the external VI Clinical Display by keeping image file viewing within the EHR.

- ***Added new accordion stylesheet to Consolidated Clinical Document Architecture (CCDA)***

  CCDA allows for expand and collapse for progress note display (+,-) due to the lengthiness of a note and added scrolling to the user.

- ***Added Medication Updates to On-Line Help Files including Surescripts Mailbox and Refill Queue***

  Users can access new online Help for the **Surescripts Queue** and **Surescripts Mailbox** Help files.

- ***Created a new RPMS report: Implantable Device List (IDL) Recall Report.***

  A new RPMS menu option, **BEHOIMP**, was created to allow users to generate an on demand Implantable device recall list based on categories and patients.

- ***Updated the Clinical Information Reconciliation (CIR) Tool for Internet browser EDGE***

  Internet Explorer will no longer be supported in June of 2022. To prepare for the deprecation of **IE**, the document viewer in **CIR** and **CCDA** must be switched to use a different HTML renderer. **Edge** is already in use in the new browser component for **EHR** and appears to render embedded PDFs correctly.

- ***Updated the Clinical Information Reconciliation (CIR) Tool for RxNorm code mappings***

  CIR was not finding a link between **RPMS** and the **CCDA** medications by **RxNorm**, only by name. Now when selected, the **CIR** displays matches (green highlighting) to the user.

1.3 Bug Fixes/Corrections

EHR has been updated with multiple changes that were identified to be corrections. These issues/changes were implemented to assist the end user of **IHS RPMS EHR** and were found internally during testing or submitted by sites to be updated thru the IHS Feedback page. The IHS leadership approval process authorized the changes to be placed into this **EHRv1.1 p34** release.

- ***Immunizations – Age@Visit Display Error***

  Age@ visit was displaying in error a value of '**1**' instead of relative calculated age at visit immunization given date.

- ***Evaluation and Management (E&M) Patient Type Coding Error***

  The **CPT** code for **Brief New Patient (99201)** was inactivated in January 2021; however the change was not reflected in the **EHR Evaluation & Management (E&M)** component due to the codes being hard coded. Coding was updated to ignore inactive codes and continue to utilize the patient type to evaluate appropriate EM code.

- ***Telerik Dynamic Link Library (DLL) Upgrade***

  Within certain **EHR** components the **Telerik** controls were different versions, this made an incompatibility issue. All components were update to v4.

- ***Order Entry: COPY ORDER TRANSFER Error***

  The **NonVA** med display group internal number overlapped the lab display group, so the system now looks at different interval values for the copy function for order display groups being transferred.

- ***Electronic Prescribing Controlled Substances (EPCS) Two Factor Authentication (2FA) Service Error Message with ActiveClient***

  ECS controlled substances and verification of credentials, the user receives the error message *CryptographicException – Key does not exist*. This only occurs if **ActivClient 7.x** is not installed.

- ***Updated Integrated Problem List (IPL) to make the IPL Component Load Faster***

  IPL loaded all patient problem related data upon patient selection, this could be a large set of data based on patient history. Now **IPL** loads only the tab core,

episodic etc. that is active and calls the remaining data on demand by user clicking other tabs.

- ***SNOMED Search on IPL displays twice***

  Resolved issue when searching for a Problem in the IPL component, users were having to select the SNOMED/Problem twice.

- ***Mitigation of Thread 6/EHR Freezing in Provider Notes***

  Mitigation efforts to resolve the issue that Windows reports a Thread 6 error while the TIU Template Dialog is being used. This error can occur while the user is interacting with the dialog or after clicking the Close button to save the note content.

2.0 EHR Enhancements

2.1 BMAG Changes Incorporation

Incorporation of **Vista Imaging (BMAG p193)** changes are delivered in **EHR v1.1 p34**. Refer to the updated *Electronic Health Record for IHS Imaging Viewer and IHS All Images Viewer User Guide* for changes.

Important:	To configure the IHS All Images Viewer Plugin, refer to the ***IHS Imaging Viewer and the IHS all Image Viewer (bmag0300.193u)*** documentation.

2.2 CCDA Incorporate New Accordion Stylesheet

Issue/Change: Clinicians prefer the availability of the full impression, the full report, or the complete progress notes, which might often be extensive. This would make the entire **CCDA** document very long and the user would have to scroll continuously through the document. This coincided with the 21 **CURES USCDI v1** requirement to add the Clinical Notes, which due to the number and the potential size of each note, can also make the **CCDA** quite lengthy.

Resolution: Progress notes display in **CCDA** initially appear to users collapsed with viewing the **CCDA for a Patient/Visit**.

1. The user can expand to view the entire note by clicking the **plus sign (+)** (Figure 2-1) on the far right of the note title.

Figure 2-1: CCDA Visit Progress Note Collapsed

2. The user can collapse the progress note when needed by clicking the **dash (-)** (Figure 2-2).

Figure 2-2: CCDA Visit Progress Note Expanded window

Set up:

Note:	Full description and list of all changes that were made to the **CCDA** product will be released within the **Consolidated Clinical Document Architecture (BCCD)** namespace, including an updated user manual.

2.3 Medication Update On-line Help Files

On-Line Help files are accessible within the **EHR** (Figure 2-3) and provides component-oriented assistance, which contains information relating to general use and functions of each component.

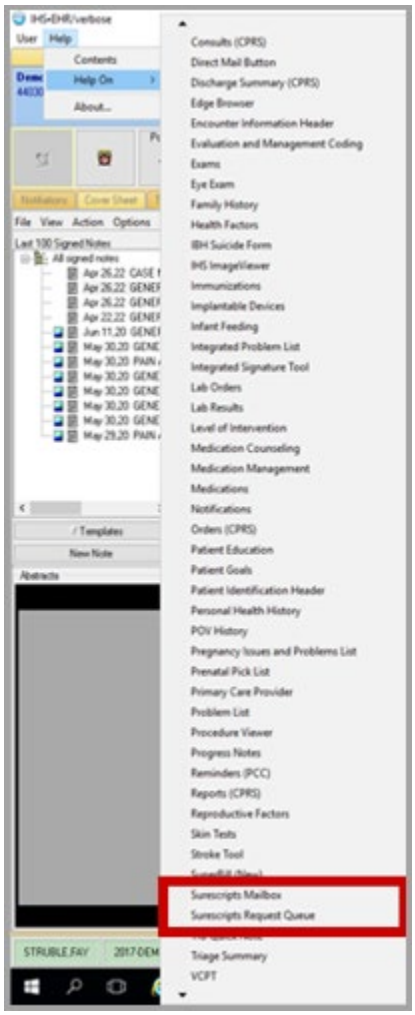


Figure 2-3: Access to Online Help in EHR for the updated help files

2.3.1 Surescripts Request Queue

Issue/Change: A new On-Line Help file was added to **EHR** for the **Surescripts Request Queue** (Figure 2-4). Requests coming from a Surescripts pharmacy to the **RPMS** system may require attention from one or more users at the site. This is to ensure that requests are being responded to within the 72-hour window and to ensure that requests that cannot be automatically matched to an order in the **RPMS** database are either manually mapped or denied if unable to be mapped. To facilitate the monitoring of the requests, a **Surescripts Request Queue** component was created.

Resolution: **Surescripts Request-Queue** On-Line Help is accessible through **EHR**.

1. Click **Help** positioned below **IHS-EHR** in the upper-left corner.
2. Place the cursor on **Help On >** and the system opens a set of menu options in alphabetical order.

3. Scroll down and click **Surescripts Mailbox**.

4. The online Help is indexed into component function content. Click a **section of functionality** and additional options appear.

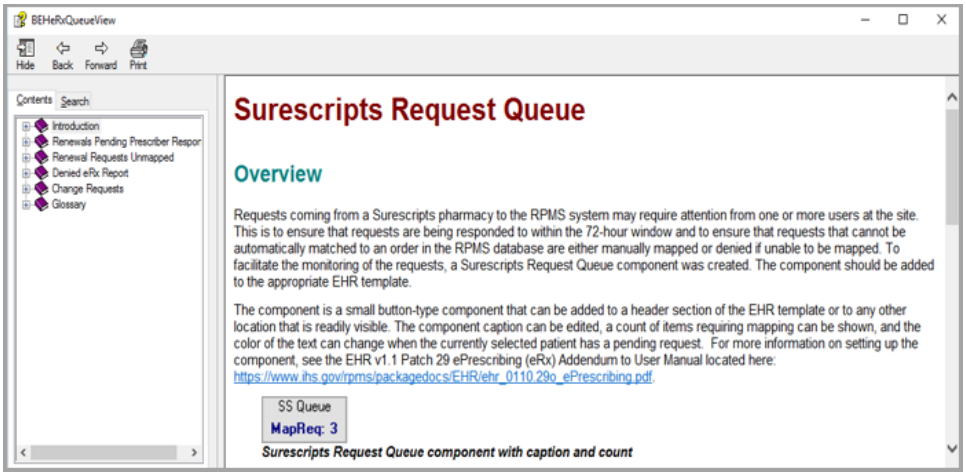


Figure 2-4: Online Help Surescripts Request Queue window

2.3.2 Surescripts Mailbox

Issue/Change: A new online Help file was added to EHR for the **Surescripts Mailbox** (Figure 2-5). The **Surescripts Mailbox** (also called **SS Mailbox** or **Mailbox**) is a component that allows prescribers to manage their incoming requests from **Surescripts**.

Resolution: The **Surescripts Mailbox** online Help is accessible through **EHR**.

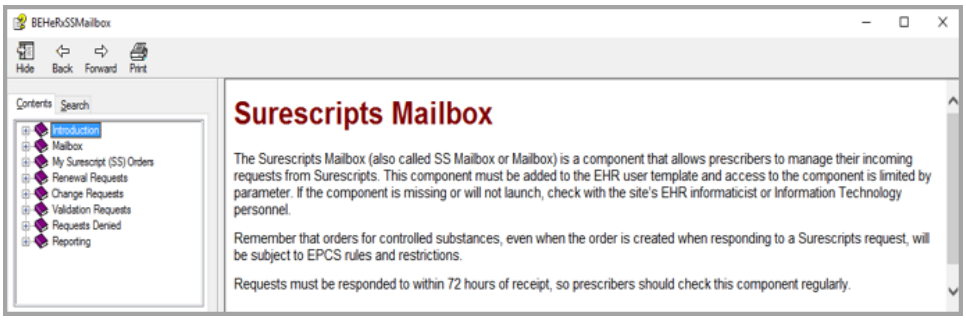


Figure 2-5: Online Help Surescripts Mailbox window

2.4 Clinical Information Reconciliation (CIR) Tool Updates for EDGE and RxNorm

2.4.1 Clinical Information Reconciliation (CIR) Update for Edge

Issue/Change: The viewing of embedded PDF functionality is not supported in the **Internet Explorer** browser. The **CIR** browser must be updated to Microsoft Edge.

Resolution: The **CIR** browser is updated to Microsoft Edge to allow for viewing of received CCDA PDFs from outside healthcare entities.

2.4.2 Clinical Information Reconciliation (CIR) Update for RxNorm

Issue/Change: The **CIR** would only highlight exact medication matches in both **RPMS** and the **CCDA Document Medication** section (Figure 2-6) when medications have the same **RxNorm** code and the document specifies that the medication code belongs to the **RxNorm** code set, or if the medication name matches.

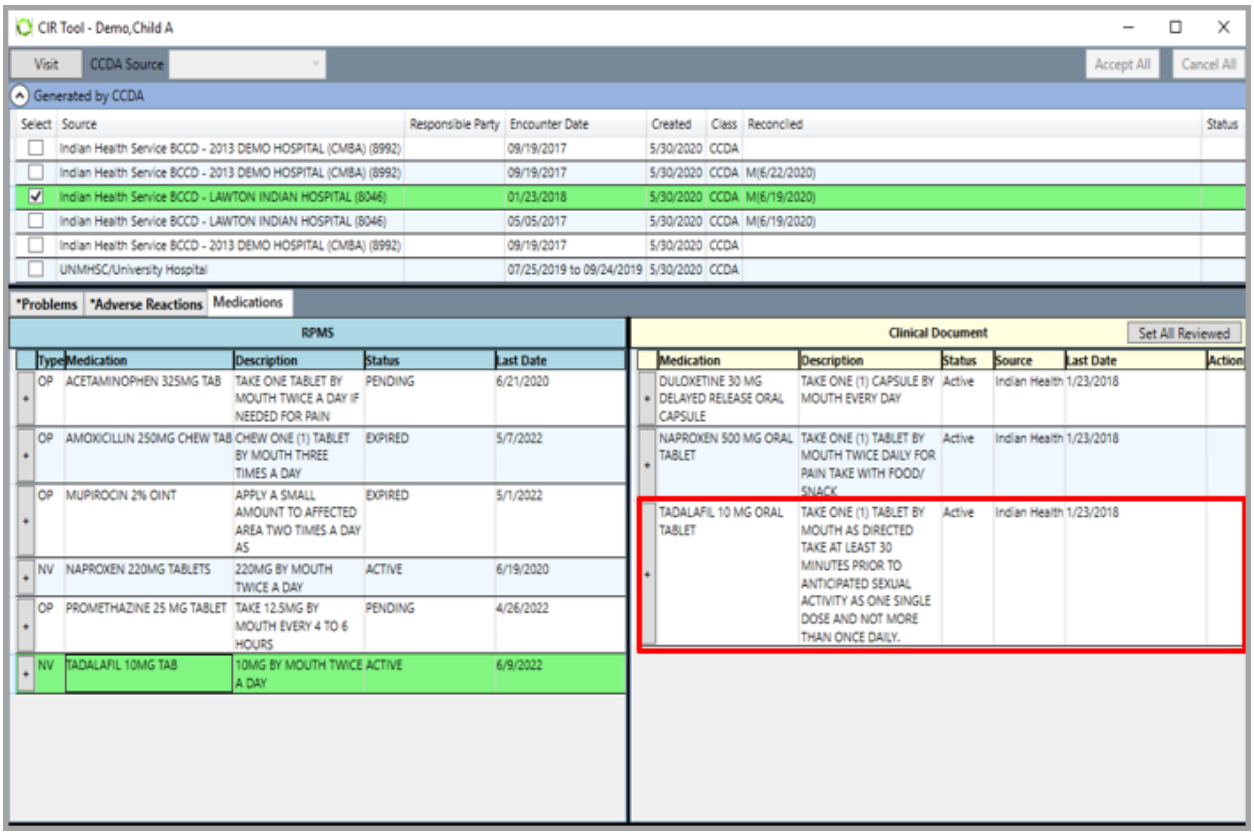


Figure 2-6: CIR RPMS and CCDA Drug Not Displaying Matched window

Resolution: Update **CIR** to check if the document specifies that a medication code belongs to the **RxNorm** code set by either the code set name or its **OID** identifier. Currently only the name is checked.

1. User selects a **patient** with a received **CCDA** from an outside source and visit in **EHR**.
2. Click the **CIR** icon.
3. Select the imported **CCDA** and select the **Medication** tab (Figure 2-7).
4. Select a **medication row** from CCDA or from **RPMS** that matches. The system highlights both entries in green.

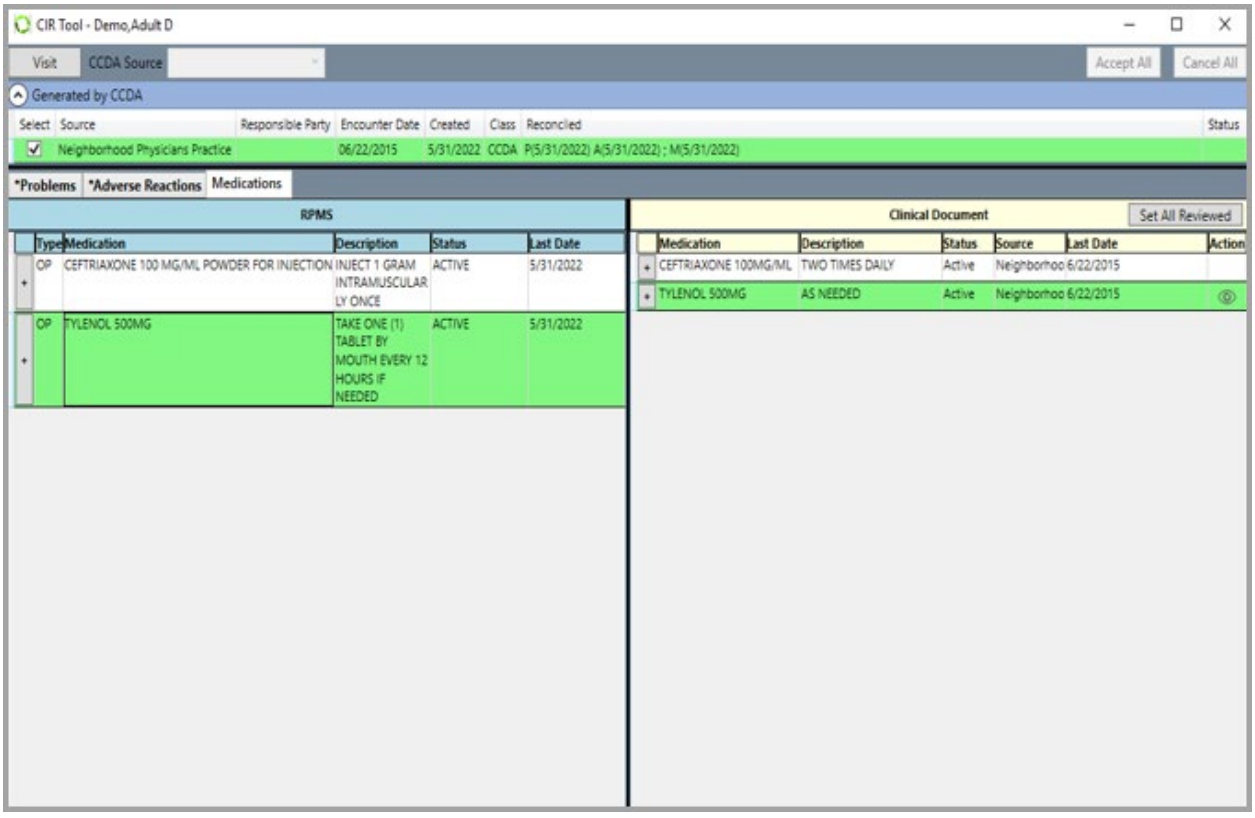


Figure 2-7: CIR RPMS and CCDA Drug Displaying Matched window

2.5 Implantable Device List (IDL) Recall Report

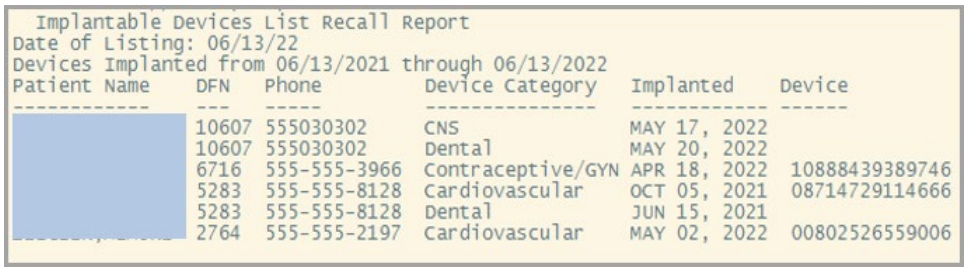
IHS feedback submission from site users of new **IDL** components have requested an implantable device **Recall List** report, as from time-to-time recalls do happen with manufactured devices. The site must find the patients with those devices and reach out to them to discuss the next steps.

Issue/Change: Create a new **Implantable Device List Recall** report in **RPMS**.

Resolution: A new **IDL** report is accessible in **RPMS**.

- The **Recalls List** report contains search capabilities on **lot number**, **device name**, and/or **device manufacturer**.

- The **Recalls List** report requires a **start** and **end date** to evaluate the data to pull forward and display to the user.
- The new **Recalls List** report (Figure 2-8) displays the following fields:
  - Patient name
  - Chart number
  - Phone numbers listed in the system
  - Device category
  - Implantation date
  - Device



```
  Implantable Devices List Recall Report
Date of Listing: 06/13/22
Devices Implanted from 06/13/2021 through 06/13/2022
Patient Name    DFN   Phone         Device Category   Implanted    Device
------------    ---   -----         ---------------   ------------ ------
[redacted]      10607 555030302     CNS               MAY 17, 2022
                10607 555030302     Dental            MAY 20, 2022
                6716  555-555-3966  Contraceptive/GYN APR 18, 2022 10888439389746
                5283  555-555-8128  Cardiovascular    OCT 05, 2021 08714729114666
                5283  555-555-8128  Dental            JUN 15, 2021
                2764  555-555-2197  Cardiovascular    MAY 02, 2022 00802526559006
```

Figure 2-8: New IDL Recalls List Report displays in RPMS

3.0 EHR Corrections

3.1 Immunizations – Age@Visit Column Display Error

Issue/Change: In the **Immunizations** component when selecting the **RPMS + State** button, the **Age@Visit** column (Figure 3-1) reverts to a **1** instead of the value.

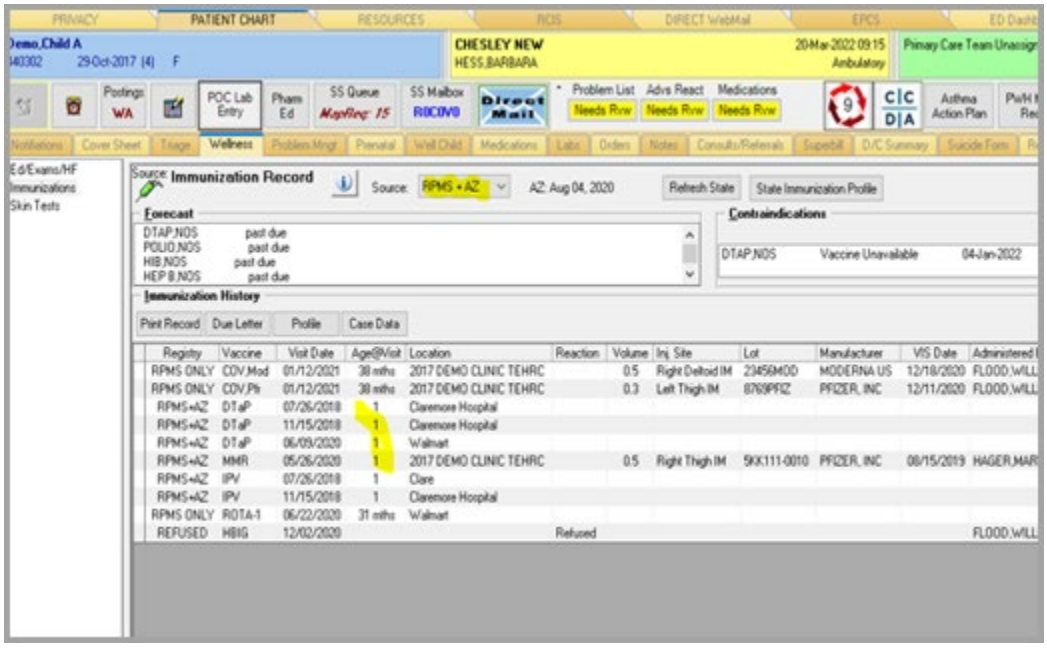


Figure 3-1: Error Displaying Correct Patient Age window

Resolution: Users have the ability to see the correct patient age (Figure 3-2) at the time the immunization was given.

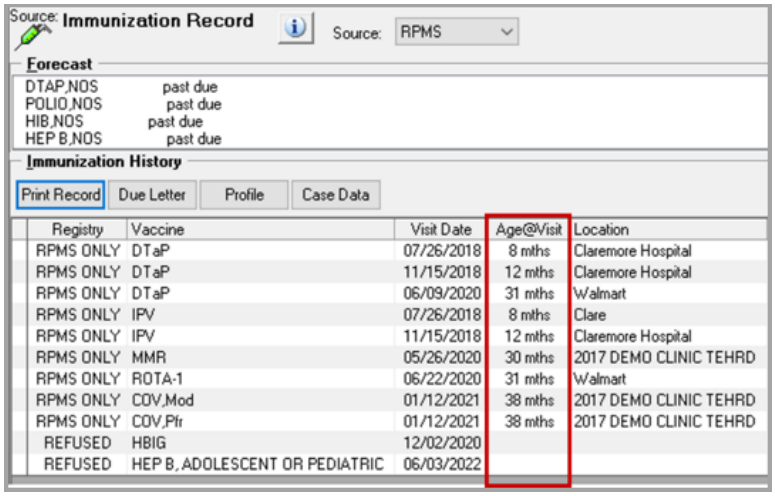


Figure 3-2: Age@Visit displays correct value

3.2 Evaluation and Management (E&M) Patient Type Coding Error

Issue/Change: Site reported that the **Brief New Patient Current Procedural Terminology (CPT)** code was saving the **Brief Established Patient CPT Code**. The **CPT** code for **Brief New Patient (99201)** was inactivated in January 2021 however the change was not reflected in the **EHR Evaluation & Management (E&M)** component due to the codes being hard coded.

Resolution:

- **E&M** component dynamically looks up the appropriate **CPT** codes and no longer is a hard-coded list that displays to users.

  Figure 3-3 displays an active, new patient **CPT Code** list.

99202	OFFICE O/P NEW SF 15-29 MIN	New
99203	OFFICE O/P NEW LOW 30-44 MIN	New
99204	OFFICE O/P NEW MOD 45-59 MIN	New
99205	OFFICE O/P NEW HI 60-74 MIN	New

Figure 3-3: Active New Patient CPT Code List

  Figure 3-4 displays an active, established **Patient CPT Code** List.

99211	OFFICE O/P EST MINIMAL PROB	Estab
99212	OFFICE O/P EST SF 10-19 MIN	Estab
99213	OFFICE O/P EST LOW 20-29 MIN	Estab
99214	OFFICE O/P EST MOD 30-39 MIN	Estab
99215	OFFICE O/P EST HI 40-54 MIN	Estab

Figure 3-4: Active Established Patient CPT Code List

- When the user selects a patient, the system evaluates if the visit exists for the patient and determines which option button to default.
  - No visits will enable the **New Patient CPT Code** set.

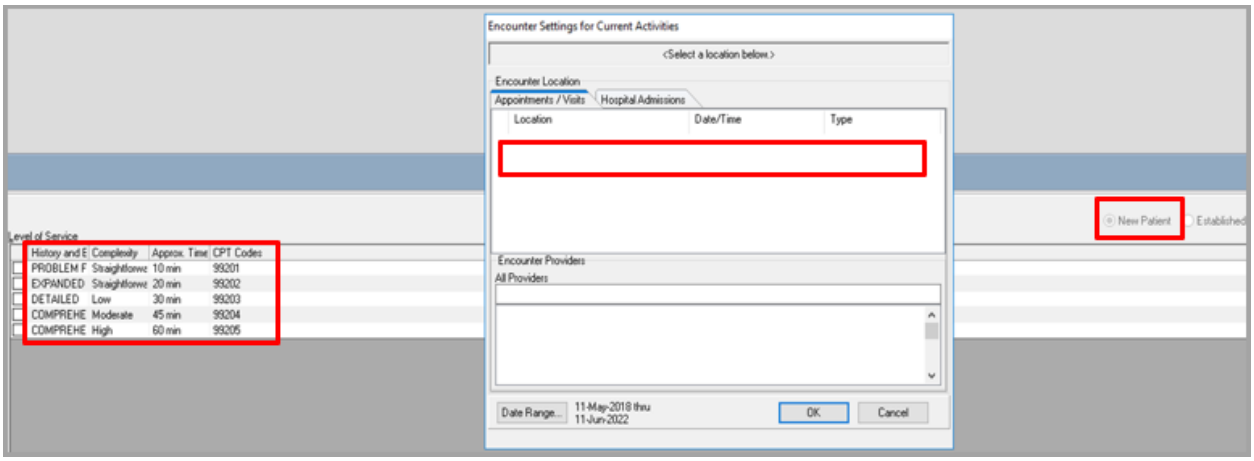


Figure 3-5: New Patient CPT Code Set not enabled due to no visits

– Visits will enable the **Established CPT Code** set.

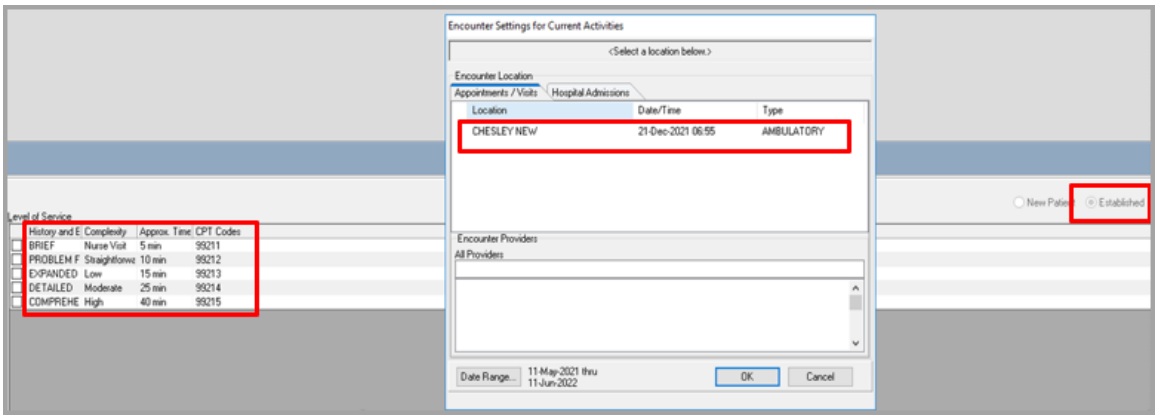


Figure 3-6: CPT Code Set enabled with visits established

3.3 Telerik DLL Upgrade

Issue/Change: Multiple **EHR** components use **Telerik** controls and were built for different versions of the **Telerik dlls**. Currently, each component that uses **Telerik** controls has to use whichever version is in the EHR run directory, even if the component has an embedded copy of the version of the **Telerik dlls** it wants.

Resolution: Upgrade **Telerik.dll** of components using other .dlls.

- All **EHR** components using the imbedded **Telrik DLL** were upgraded to the same version.
  - Affected components list:
    - Patient Goals
    - Laboratory Accession GUI (Namespace: BLGU)

3.4 Order Entry: COPY ORDER TRANSFER

Issue/Change: When copying a **Lab order** during the orders transfer process for an admitted patient, the system evaluated the display group and subset of display groups that matched and attempted to complete **Lab orders** as **Non-VA Medication orders**.

Resolution: The system now looks for a **series of display groups** instead of a **set of display groups** or **statements**.

1. Log into **EHR** and select an **Inpatient patient** with **Lab orders**.
2. Chose the menu option **Delayed Orders**.

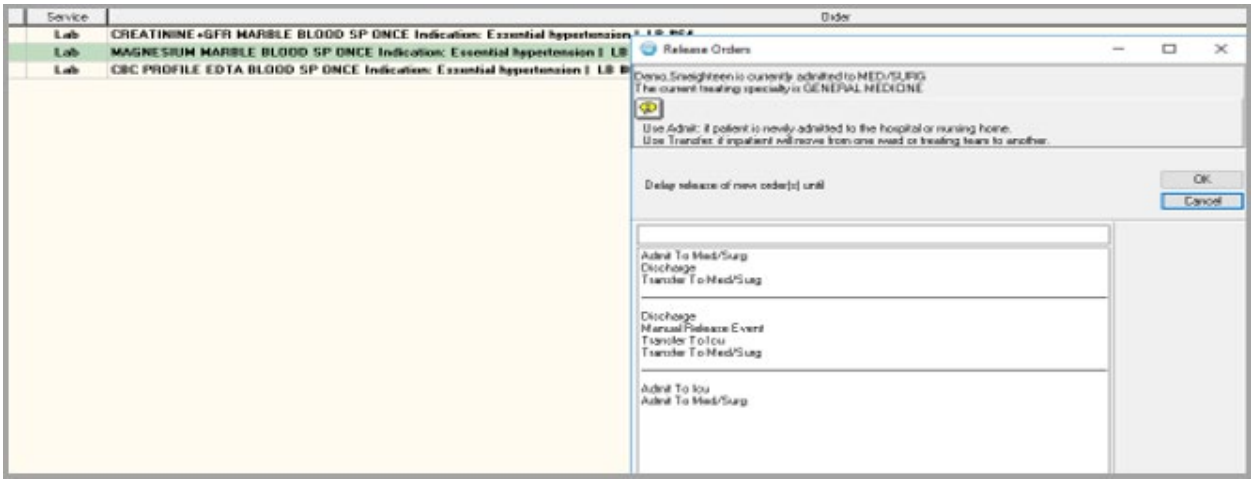


Figure 3-7: Create New Release Event for Orders window

3. Select the **option** to transfer to **another unit**.
4. Click the **Accept Order** button.

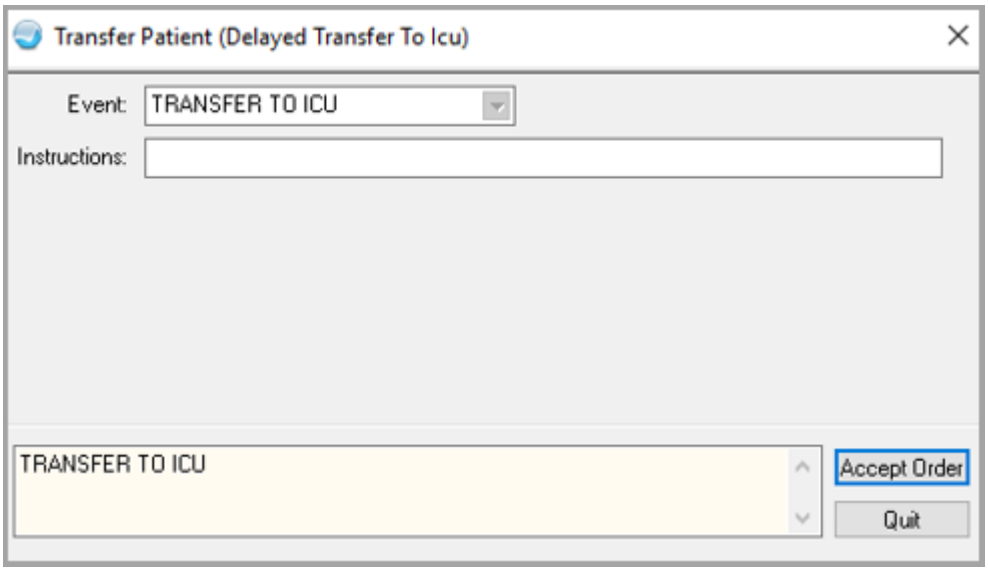


Figure 3-8: Set Up ADT Transfer of Patient window

5. Select the **Lab orders** to transfer (Figure 3-9) and click **OK**.

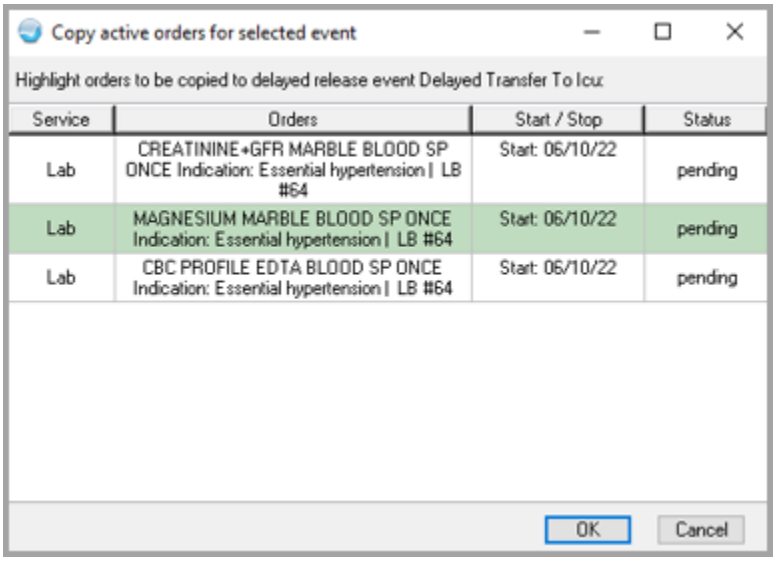


Figure 3-9: Copy Active Orders for Transfer window

Delayed **Lab orders** are placed correctly on the **Orders** pane in **Unreleased Status Without Error**.

3.5 Electronic Prescribing for Controlled Substances (EPCS) 2FA Service Error Message with ActiveClient

Issue/Change: When using the **Two-Factor Authentication (2FA)** service to sign a controlled substance order or verify **EPCS credentials** the user receives the error

message *Cryptographic Exception – Key does not exist*. This only occurs if **ActivClient 7.x** is not installed.

Resolution: RPMS handles the error when **ActivClient** is not installed by trying again with a manually specified key number.

3.6 Integrated Problem List (IPL) Changes to Mitigate Slowness

Issue/Change: Implement changes to make **IPL** load its data faster, lowering server resource usage at the same time. Many sites have ongoing slowness and resource usage issues and they highlighted **IPL** as a common point of slowness. Similar comments about **IPL** being slow on support tickets from other sites, previous changes to **IPL** in past patches has not resolved this issue.

Resolution: The system loads **Core** and **Personal History** data immediately to the **IPL** component. All other data is loaded when the user clicks additional tabs.

- Problems with the status of **Core Settings** tab (Figure 3-10) fully loaded and displayed immediately.

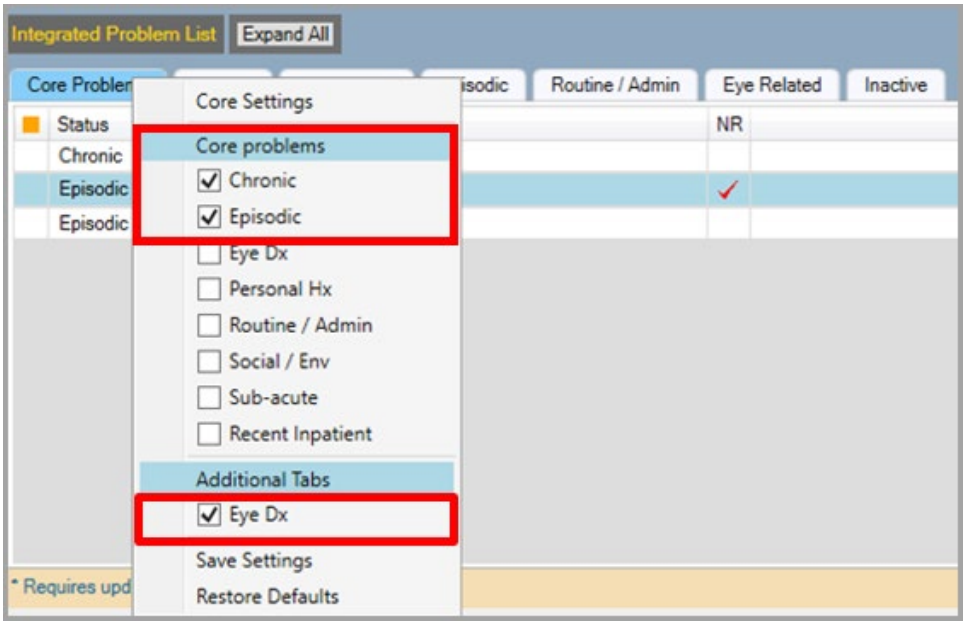


Figure 3-10: Problems Configured to Display on Core Tab Display Immediately example

- Confirm that **eye-related problems** configured to show on the **Core Problems** tab (Figure 3-11), actually appear.

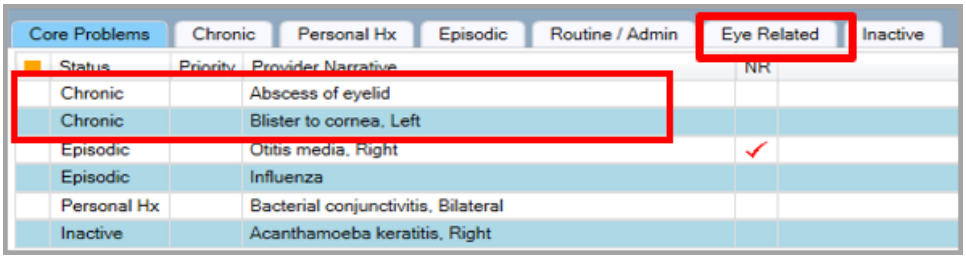


Figure 3-11: Eye-Related Problems Display on Core Tab example

- All **Personal Hx** problems (Figure 3-12) are loaded immediately.

Figure 3-12: All Personal History Problems Load Immediately example

3.7 IPL SNOMED Search displaying twice

3.8 Mitigation of Thread 6/EHR Freezing when using Notes

Issue/Change: Windows reports a Thread 6 error while the TIU Template Dialog is being used in the Notes Component. This error can occur while the user is interacting with the dialog or after clicking the Close button to save the note content.

Resolution: The TIU Template dialog was modified so that a RPC call would be made on a regular basis while the dialog was open. This change appears to alter the behavior of the error resulting is a dramatically reduced number of errors. The system inadvertently disconnects the user from that note editing session. The exact cause is unknown, with the appearance that it is a communication issue between EHR and the broker server connection an updated bpl was created to try and minimize the disconnects and lose of notes

Appendix A Resources

A.1 IHS Application FTP Site

FTP Files | Applications (ihs.gov)

A.2 RPMS Application Documentation

https://www.ihs.gov/rpms/applications/clinical/

Appendix B Parameters

B.1 New Parameters

- None

B.2 Changed Parameters

- Change in **Parameter name** to **EPCS Max DC/Cancel/Deleted Event %**.

Appendix C Menu Option

C.1 New

- BEHOIMP – Implantable Device List Recall Report

Appendix D 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.

D.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).

D.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.

D.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.

D.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.

D.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.

D.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.

D.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).

D.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.

D.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.

D.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.

D.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.

D.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.

D.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.

D.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.

D.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.

D.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.

Acronym List

Acronym	Meaning
CAC	Clinical Application Coordinator
CCDA	Consolidated Clinical Document Architecture
EHR	Electronic Health Record
IHS	Indian Health Service
IPL	Integrated Problem List
RPMS	Resource and Patient Management System
CIR	Clinical Information Reconciliation
IDL	Implantable Device List
EPCS	Electronic Prescribing of Controlled Substances
E&M	Evaluation and Management
BMAG	IHS Imaging Viewer
CPT	Current Procedural Terminology
DLL	Dynamic Link Library
2FA	Two Factor Authentication

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