RESOURCE AND PATIENT MANAGEMENT SYSTEM

Clinical Reminders

(PXRM)

Set Up Guide for Reminder Dialog for Monkeypox Vaccine Documentation

PXRM v2.0 p2006
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 setting up and documenting the Clinical Reminder Monkeypox Dialog.

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 dialog.

Important: Read each **Notes** file (**.n**) associated with the patches with the national release of **PXRM v2.0 p2006, TIU v1.0 Patch1026 and ACPT v2022 p9**.

1.0 Introduction

This guide provides the site Informatics Team (IT) teams instructions on...

The **PXRM v2.0 p2006** patch is dependent on **TIU** v1.0 Patch1026 and **ACPT 2022 patch 9** that was nationally released in September 2022.

1.1 Clinical Reminders Resource

This guide is intended to be used by individuals who have previous experience with the Clinical Reminders.

Clinical Reminders Office Hours:

Office hours are announced periodically on the EHR and Reminders Listservs.

Clinical Reminders Listserv:

Send a question to the EHR Reminders Listserv. To subscribe go to:

https://www.ihs.gov/listserv/topics/signup/?list_id=159

Clinical Reminders Documentation:

Review documentation on the RPMS Clinical Applications Website under VA Clinical Reminders (PXRM) section.

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

2.0 Monkeypox Reminder and Dialog Configuration

This patch contains a reminder dialog designed to document the administration of the Smallpox Monkeypox vaccination.

The dialog is listed below.

IHS-Monkeypox IMM 202209

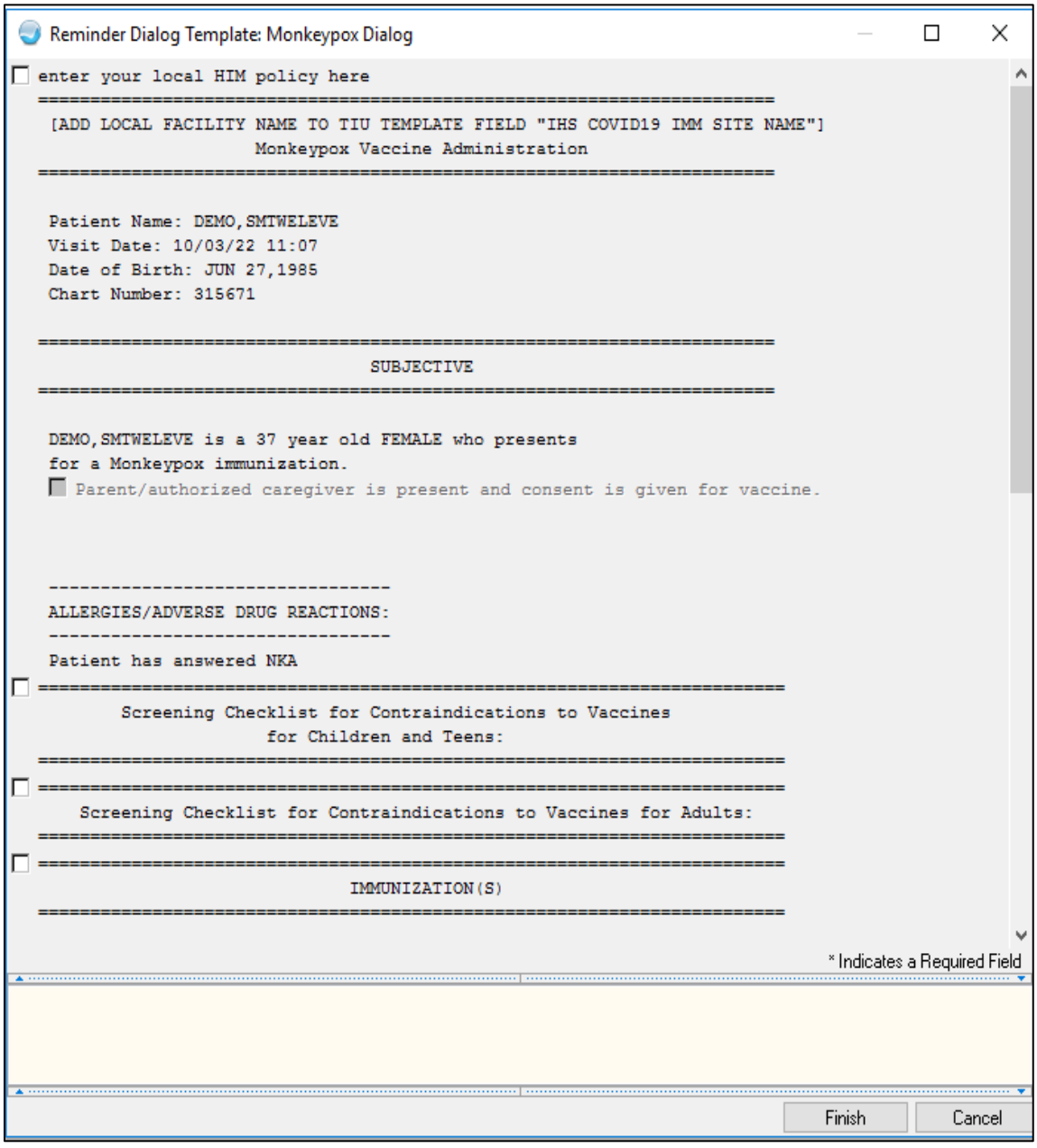

Figure 2-1: Clinical Reminders IHS-Monkeypox IMM 202209 dialog

Important: Read all instructions, notes, and documentation before installing this patch.

This reminder dialog contains the following:

- Patient Ed topics to the Patient Ed Component
- Immunizations to the Immunization Component
- Visit Services

Sites can change the dialog to reflect the facility name, policy, form, ID, and date. These instructions can be found in the Section 5.0 in this document.

2.1 PXRM Prerequisites

- ACPT*2.22*9
- PXRM*2.0*2005
- BI*8.5*1008
- TIU*1.0*1026

2.2 TIU v1.0 Patch1026

This patch contains a TIU data object called LAST # MONKEYPOX IMMS to support PXRM Monkeypox reminder dialog.

PXRM Monkeypox Dialog.

Important: Read all instructions, notes, and documentation before installing this patch.

2.2.1 Prerequisites for TIU v1.0 p1026

The following are prerequisites for TIU v1.0 p1026:

TIU*1.0*1025

Kernel (XU) v8.0 patch 1018 or later

FileMan (DI) v22.0 patch 1018 or later

3.0 Install the KIDS Build

Installation of **PXRM 2006** should be done by the appropriate IRM personnel using the instructions in the patch notes. Users may be on the system.

Installation of Patch 2006 will put the reminder dialog into the **REMINDER EXCHANGE** file.

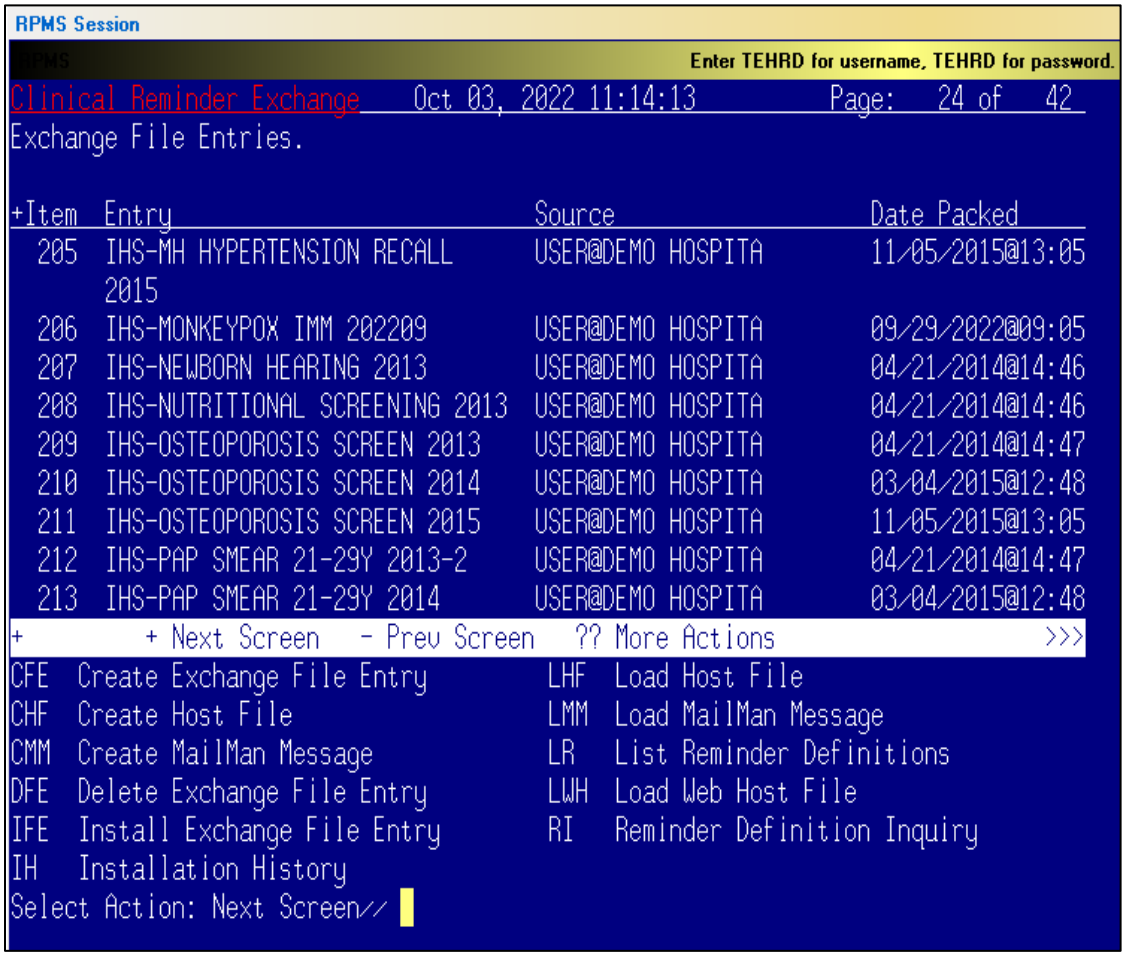

Figure 3-1: Clinical Reminders Kids Build IHS-Monkeypox IMM 202209

> **Note**: It does ***not*** install them.

The new reminders/dialogs will not work until they are installed and activate.

4.0 Installing the Reminders/Dialog

Follow these instructions to install the one (1) item in this patch. The CAC or another designated person should install it using **REMINDER EXCHANGE**.

4.1 Installing the Item from Exchange

1. Select Reminder Exchange from the Reminder Configuration menu (Figure 4-1). You will be presented with a list of packed reminders that reside in the RPMS file system.

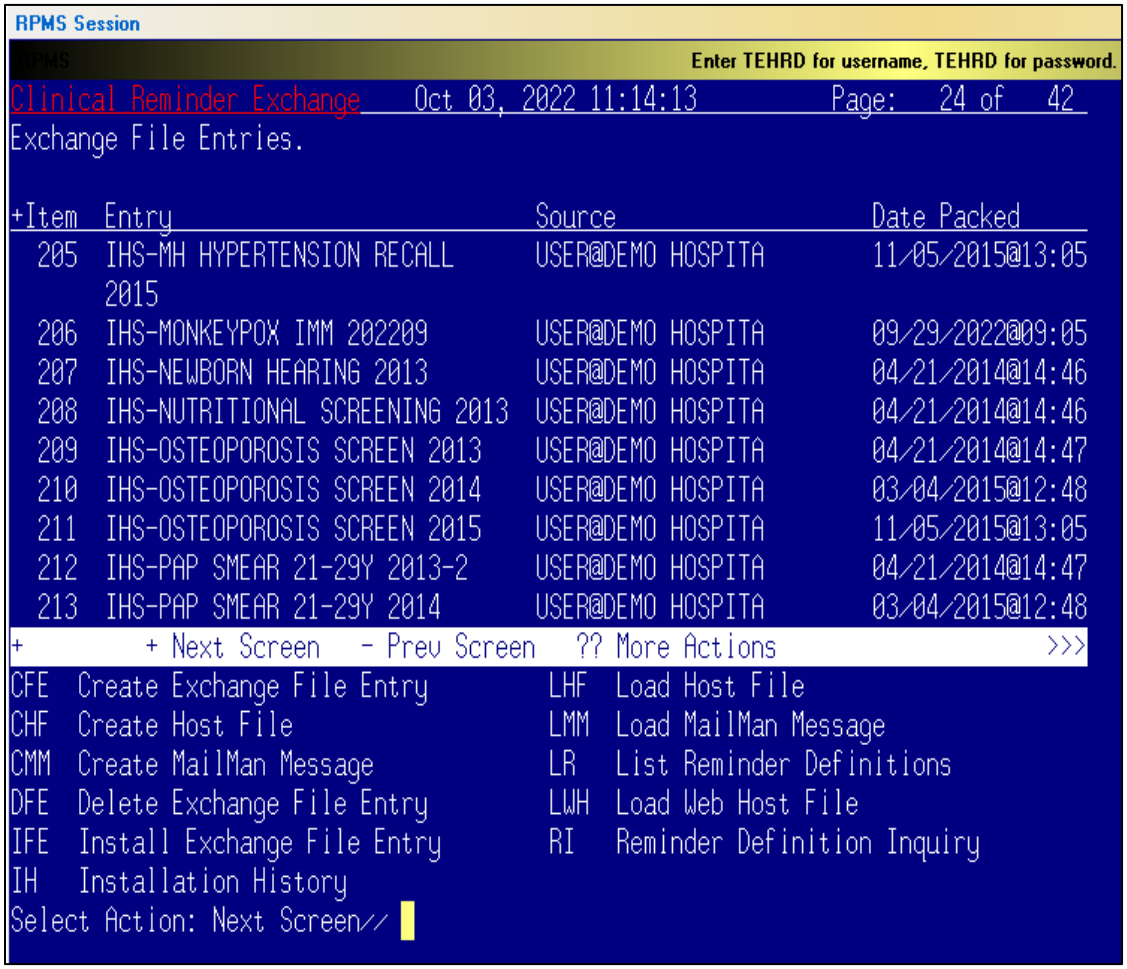

Figure 4-1: Exchange List of Reminders

> **Note**: Use the **Up** and **Down** arrows to scroll through the list.

2. If you are searching for a specific dialog, use the command **SL** to search for the dialog name. For patch **2006** there is one (1):

DIALOG NAME IHS-MONKEYPOX IMM 202209

```
Select Action: Next Screen// SL
Search for: //MONKEYPOX?
```

Figure 4-2: SL Command

3. Select **IFE – Install Exchange File Entry** to install the reminder.

4. Enter the number of the reminder (4-3) to install.

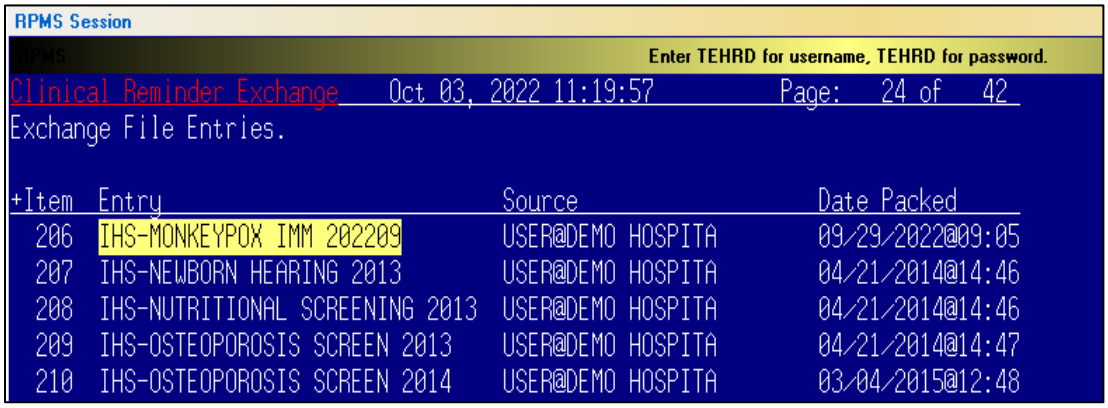

Figure 4-3: Reminder List with number selected

4.2 Installing Dialog – Part 1

Before starting an installation, you should examine the list of components in the packed reminder to determine which ones already exist on your system. You should decide what to do with each component and have a plan of action before proceeding with the installation.

The following is a sample of part 1 of the **Exchange File Components** screen (Figure 4-4). You can use either the up and down arrows on the keyboard or just select return to view all the items.

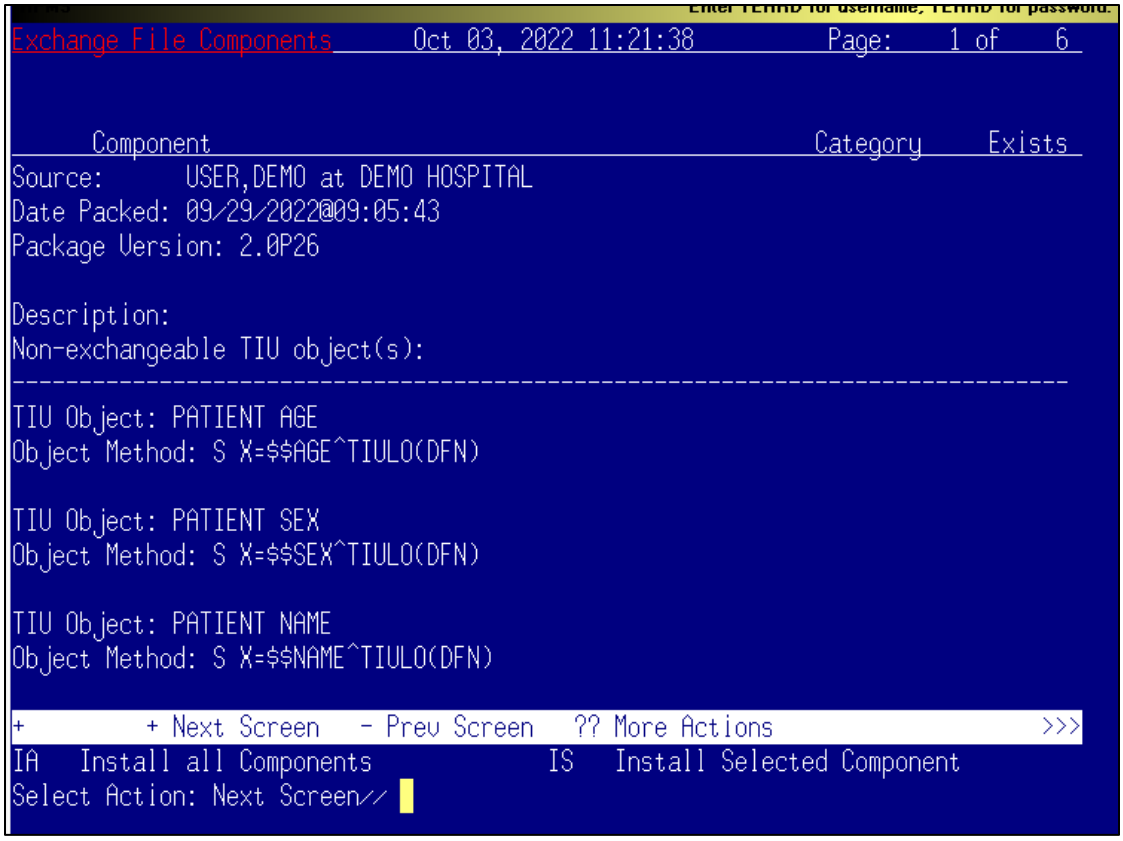

Figure 4-4: Exchange Entry

- Notice that for each item in the reminder, an **X** (X) now displays to indicate if the item in exchange matches an item in the file. Users are not asked about the elements if there is a match. This will make the installation much faster.
- There are two (2) choices: **IA** (Install All) and **IS** (Install Selected). Select IA to install all components. The installation will start.
- Each item is examined. If the item exists on your system, the default will be to skip installing it again. If it is new, the default is to install it. See below.

1. There are many new TIU template fields (Figure 4-5) in this dialog. Install all of them. Take the default and install them.

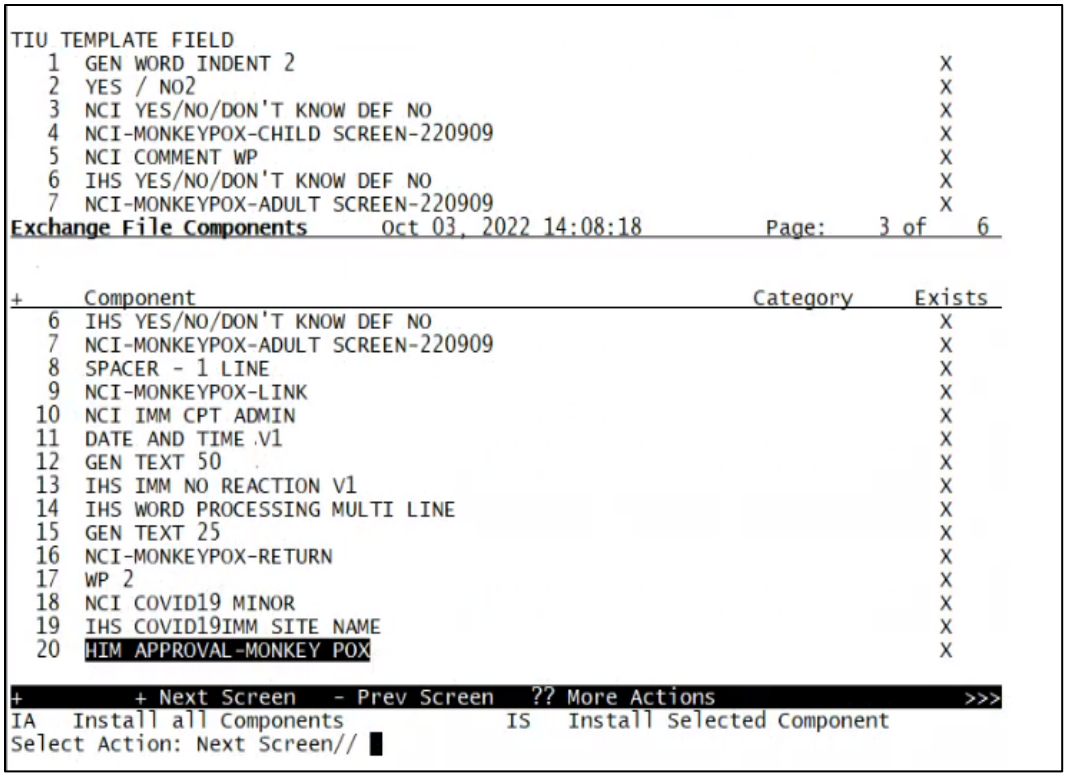

Figure 4-5: Exchange Entry

```
TIU Template Field TIU TEMPLATE FIELD entry HIM APPROVAL MONKEY POX is NEW,
what do you want to do?

     Select one of the following:

          C         Create a new entry by copying to a new name
          I         Install
          Q         Quit the install
          S         Skip, do not install this entry

Enter response: I// install
```

Figure 4-6: TIU Template Field, Entry HIM APPROVAL MONKEY POX is NEW, what do you want to do?

4.3 Install Dialog – Part 2

You will see a second screen with a list of the items to install.

When installing the dialog, there are multiple choices:

```
DD   Dialog Details       DT   Dialog Text          IS   Install Selected
DF   Dialog Findings      DU   Dialog Usage         QU   Quit
```

```
DS   Dialog Summary        IA   Install All
```

Figure 4-7: Installation Items

1. Choose **IA** to install all components.

   During installation, a routine will compare the checksum of the item on your system to the one in exchange (Figure 4-8). If they are identical, it will not update the item on your database.

```
Dialog Components          Oct 03, 2022 11:23:35        Page:    1 of    9
Packed reminder dialog: IHS-MONKEYPOX IMM 202209

 Item  Seq. Dialog Findings                                    Type     Exists
   1    IHS-MONKEYPOX IMM 202209                              dialog      X

   2   5 GRP-IHS HD-IMM MONKEYPOX 202209                      group       X
         Finding: *NONE*

   3   8 GRP-IHS MONKEYPOX SCREENING CHECKLIST PEDS 202209    group       X
         Finding: *NONE*
   4   8.5 IM-IHS SCREENING CHECKLIST PEDS 2020-202209      element       X
         Finding: *NONE*

   5   10 GRP-IHS MONKEYPOX SCREENING CHECKLIST ADULT         group       X
       202209
         Finding: *NONE*
   6   10.5 IM-IHS SCREENING CHECKLIST ADULTS 202209        element       X
         Finding: *NONE*
+        + Next Screen   - Prev Screen   ?? More Actions
DD   Dialog Details      DT   Dialog Text         IS   Install Selected
DF   Dialog Findings     DU   Dialog Usage        QU   Quit
DS   Dialog Summary      IA   Install All
Select Action: Next Screen// IA
```

Figure 4-8: Dialog Section

2. Install the reminder dialog and all components with no further changes: **Y// YES:**

   - REMINDER DIALOG entry named **ED IMMUNIZATION SCHEDULE 2020** already exists and the packed component is identical, skipping.
   - REMINDER DIALOG entry named **PXRM COMMENT** already exists and the packed component is identical, skipping.

- REMINDER DIALOG entry named **PXRM PED READY TO LEARN** already exists and the packed component is identical, skipping.
- REMINDER DIALOG entry named **PR ED LENGTH 1MIN** already exists and the packed component is identical, skipping.
- If it is not identical, the application will ask what you want to do about all the elements in this reminder. If it is new, the default is to install it.

Take all the defaults as you load the reminder unless you have loaded a previous version of this reminder. If you have loaded a previous version of the reminders, always re-install the reminder definition itself and overwrite any elements.

4.4 Activate the Dialog

All dialogs are inactive if they are loaded from Reminder Exchange (Figure 4-9). This section describes how to activate the dialog so that they are visible within the EHR.

```
                              Reminder Configuration

   CFM    Reminder Computed Finding Management ...
   DEF    Reminder Definition Management ...
   DLG    Reminder Dialog Management ...
   EXC    Reminder Exchange
   INF    Reminder Information Only Menu ...
   PAR    Reminder Parameters ...
   RPT    Reminder Reports ...
   SPO    Reminder Sponsor Management ...
   TAX    Reminder Taxonomy Management ...
   TRM    Reminder Term Management ...
   TST    Reminder Test
```

Figure 4-9: Reminder Menu

Use the DLG option to access the options on the Reminder Dialog Management menu.

4.4.1 Reminder Dialog Management (DLG)

1. Select **Reminder Dialog Management** (Figure 4-10) from the **Reminder Configuration** menu.

```
Reminder Dialog Management
   DLG    Reminder Dialogs
   PAR    Dialog Parameters ...
```

Figure 4-10: Reminder Dialog Management

2. Use the **DLG** option to access the options on the **Reminder Dialog Management** menu (Figure 4-11).

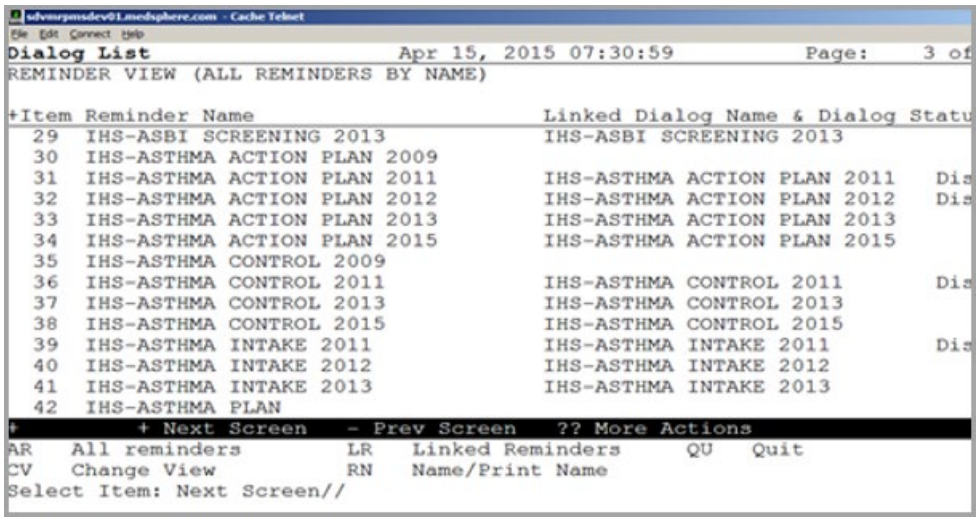

Figure 4-11: Sample Reminder View

3. Choose **CV**, and then choose **D** for dialogs (Figure 4-12).

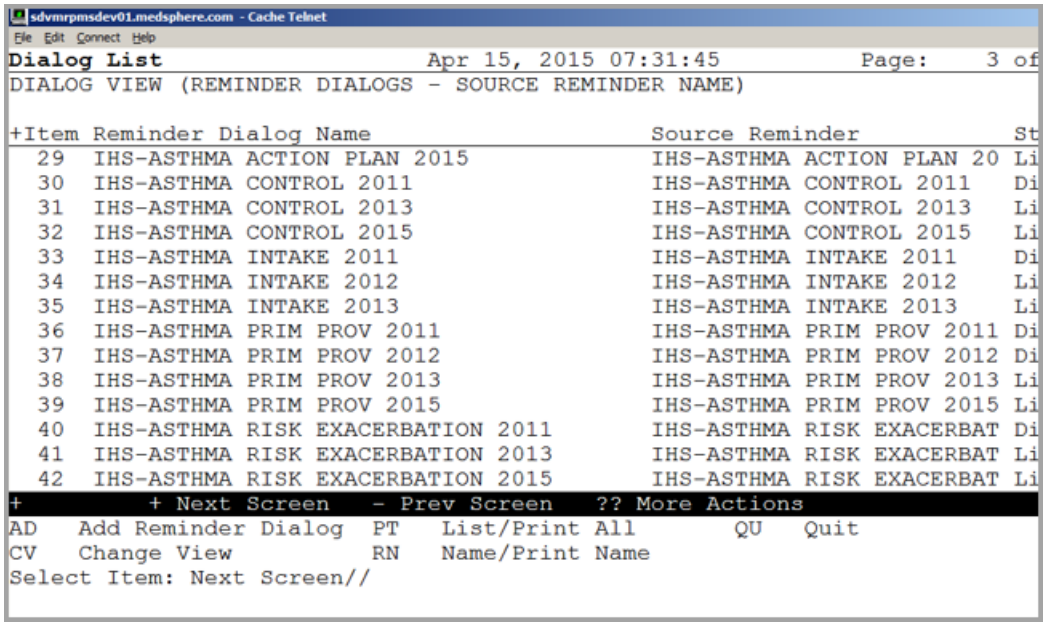

Figure 4-12: Sample Dialog View

4. Select the number of the item you want to edit (Figure 4 12).

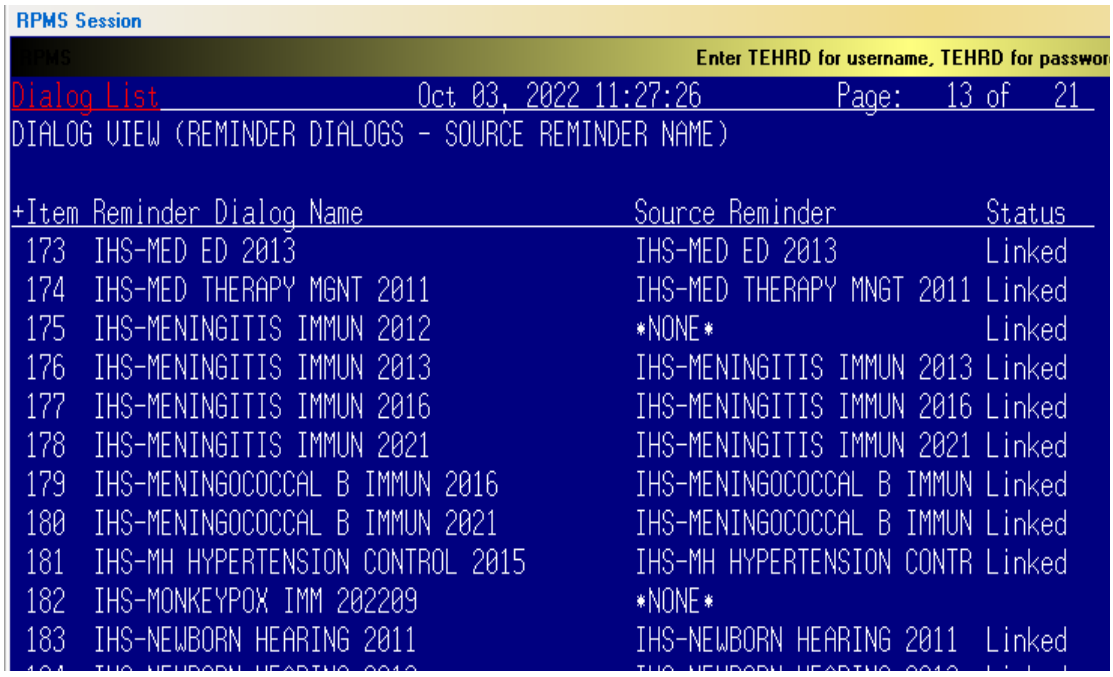

Figure 4-13: Dialog Edit List Window

5. Select the dialog. It will say **Disabled** instead of **Linked**.
6. Choose **ED (Edit/Delete Dialog)**.
   - The second prompt will state:

```
DISABLE: DISABLE AND SEND MESSAGE//
```

7. Type the at (@) symbol to delete that text.

   You will then be asked:
   - "Are you sure you want to DELETE? YES." Press Enter.
8. Type a caret (^) to quit editing.

5.0 Update the TIU Templates

Several TIU templates were included in this dialog that must be edited and changed to reflect a particular site's data. After loading the dialog, go into the TIU template editor (Figure 5-1) and change the text for the following template fields:

1. Change to your site's information.

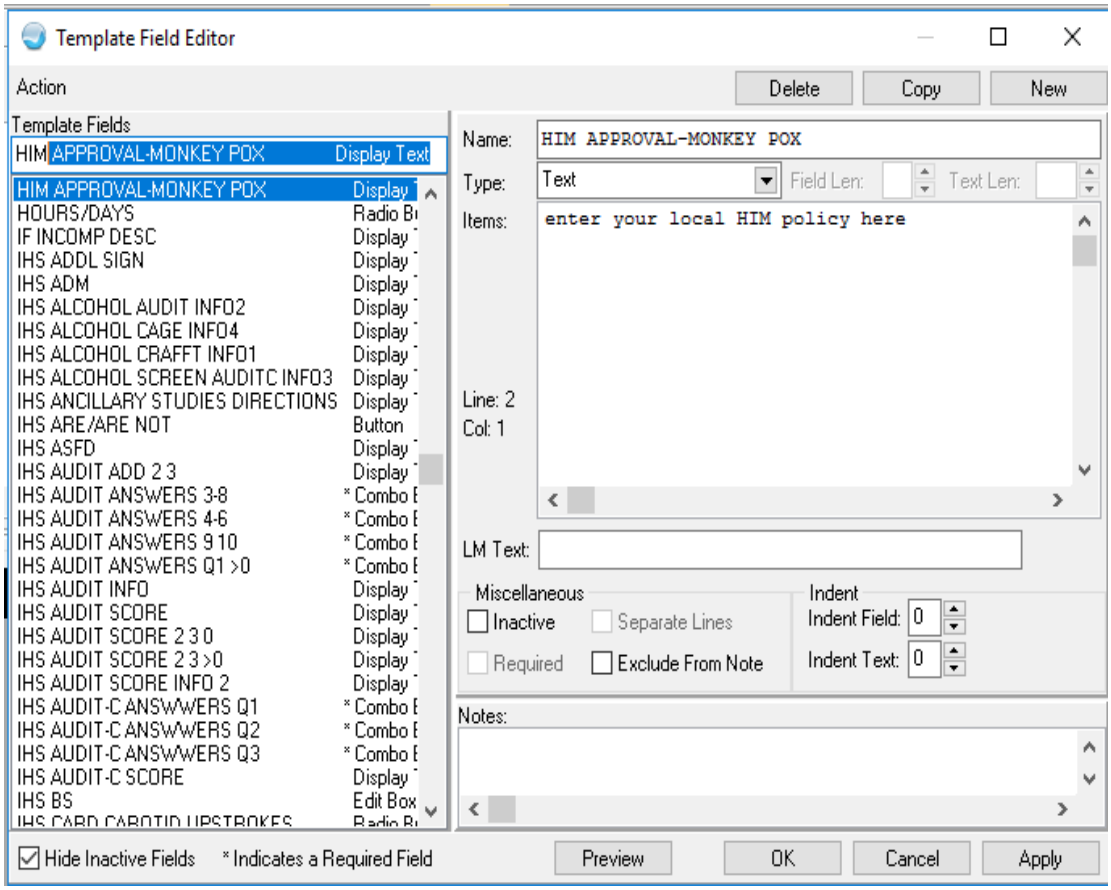

Figure 5-1: TIU Template Editor

2. Once the **dialog** has been added, add it to the **TIU parameter** so it can be selected in the EHR. Set this parameter at the system level.

   - TIU TEMPLATE REMINDER DIALOGS (Figure 5-2) may be set for the following:

```
     1   User           USR    [choose from NEW PERSON]
     3   Service        SRV    [choose from SERVICE/SECTION]
     4   Division       DIV    [choose from INSTITUTION]
     5   System         SYS    [DEMO.MEDSPHERE.COM]

Enter selection: 5   System   DEMO.MEDSPHERE.COM
```

```
--- Setting TIU TEMPLATE REMINDER DIALOGS for System: DEMO.MEDSPHERE.COM -
```

Figure 5-2: Setting TIU TEMPLATE REMINDER DIALOGS

3. Add a new sequence number for this dialog (Figure 5-3).

```
Display Sequence: 22//    22
Clinical Reminder Dialog: IHS-MONKEYPOX IMM 202209
```

Figure 5-3: Display Sequence

5.1 Adding Note Title

In RPMS TIU, you may want to add a new note title Monkeypox Vaccine in Document Definitions for this vaccination.

```
DDM3   Create Document Definitions

2   PROGRESS NOTES                              CL

3   CLINICAL REMINDER DIALOG IMMUNIZATIONS   DC   <<This may need to be made ACTIVE

4   MONKEYPOX VACCINE            TL
```

Figure 5-4: Adding New Note Title

5.2 Attaching the Dialog to a TIU Note Title

1. In **TIU**, do the following:
   a. Edit the **Shared Templates** field or go to **Document Titles**.
   b. Click **New Template** and enter a name.
   c. In **Template Type**, select the **Reminder Dialog type** (Figure 5-5).
   d. In the **Reminder Dialog**, find the reminder dialog **MONKEYPOX VACCINE** in the drop-down list.
   e. Select the Associated Title (note title) **MONKEYPOX VACCINE**. It can also be saved as a shared template if you do not want to add it to a note title.
2. Do not forget to click Apply and Save.

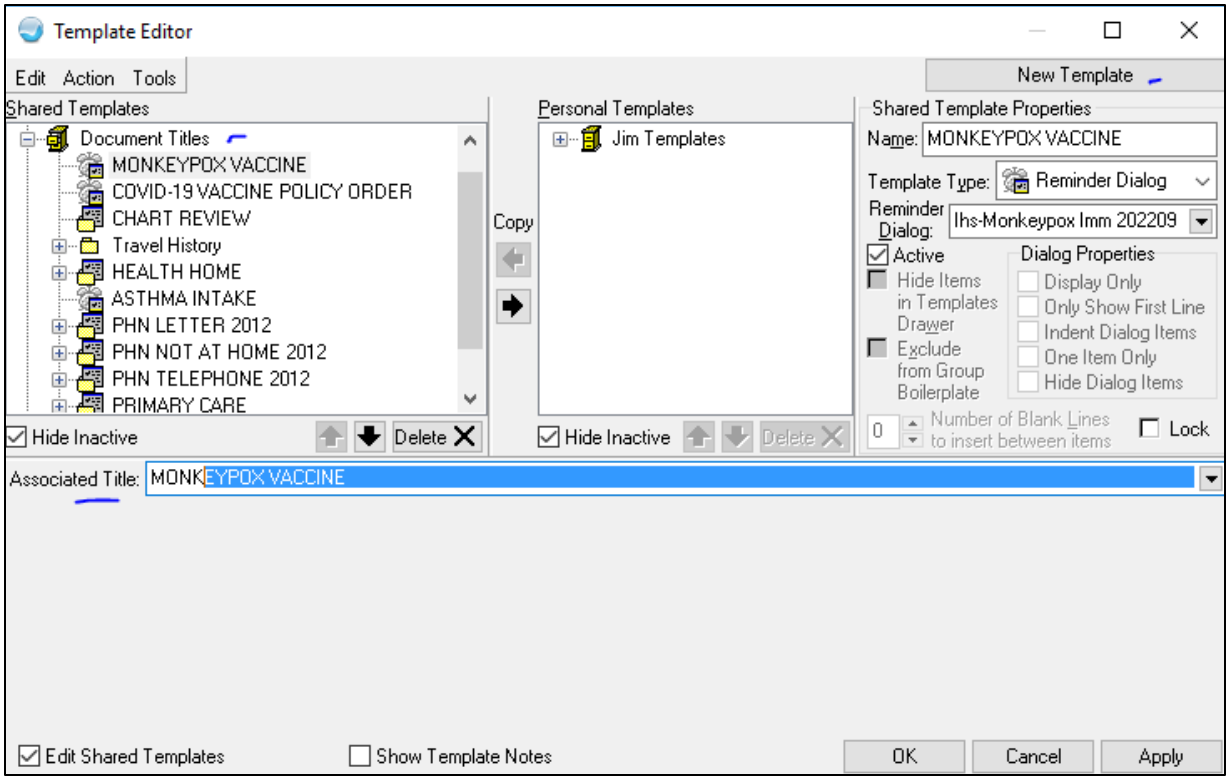

Figure 5-5: Template Editor for Reminder Dialogs

3. Users may also want to attach this template to a Note Title or to a Quick Note (Figure 5-6).

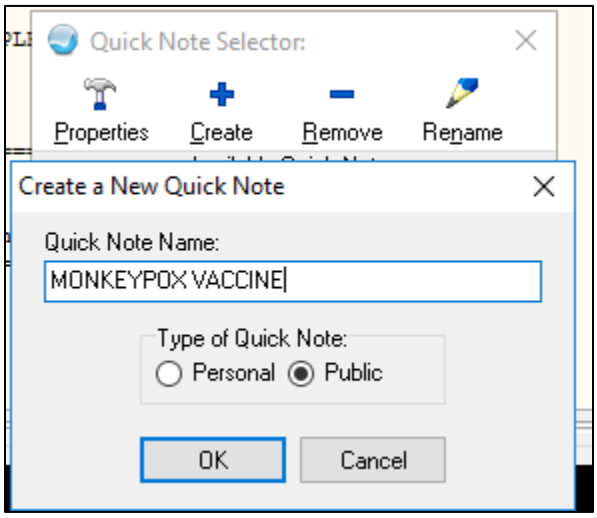

Figure 5-6: Quick Note Creator - MONKEYPOX VACCINE

Please do ***NOT*** check the boilerplate box when you are using a template.

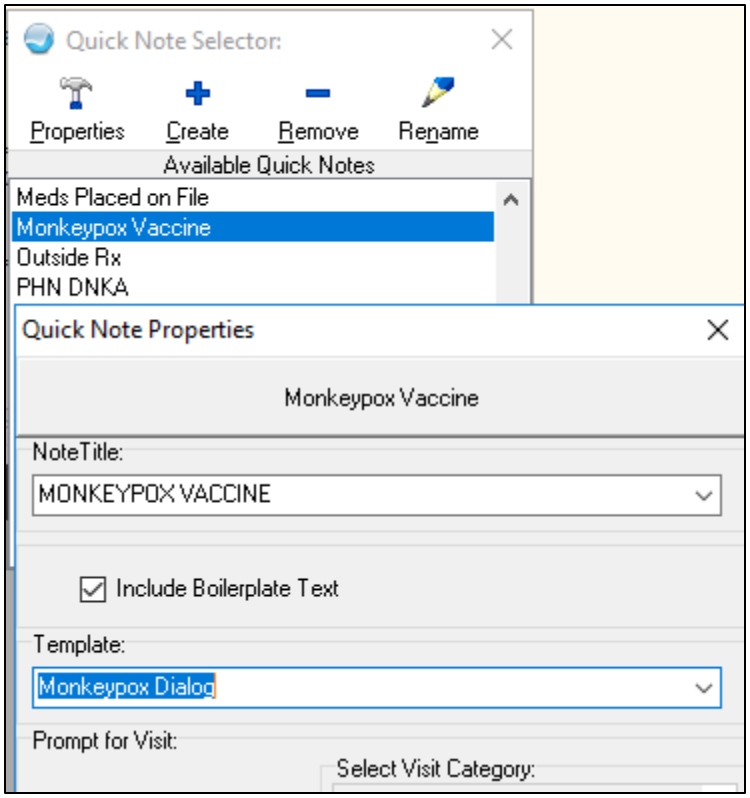

Figure 5-7: Quick Note dialog

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.2 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 personal computer (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.2.1 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.2.2 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 PC.
- 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.2.3 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.2.4 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.2.5 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.2.6 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.2.7 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.2.8 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.2.9 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.2.10 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.2.11 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.2.12 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.2.13 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.2.14 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
EHR	Electronic Health Record
IHS	Indian Health Service
BEDD	Emergency Room Dashboard
CCDA	Continuity of Care Document Architecture
MMC	Microsoft Management Console
IIS	Internet Information Services
SSL	Secure Sockets Layer
DNS	Domain Name Server
IE	Internet Explorer
IT	Informatics Team

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