



RESOURCE AND PATIENT MANAGEMENT SYSTEM

Clinical Reminders

(PXRM)

COVID Vaccine Reminder Dialog Supplemental User Guide

Version 2.0 Patch 1011
March 2021

Office of Information Technology
Division of Information Technology

Table of Contents

1.0	Introduction.....	1
1.1	Clinical Reminders Resources.....	1
2.0	COVID-19 Reminder Dialog.....	2
2.1	TIU v1.0 Patch 1023.....	2
2.1.1	Document Class and Note Title.....	2
2.1.2	Prerequisites for TIU v1.0 p1023.....	3
2.2	PXRМ v2.0 Patch 1010 and PXRМ v2.0 Patch 1011.....	3
2.2.1	Prerequisites.....	3
3.0	Install the KIDS Build	5
4.0	Create the Quick Orders	6
4.1	Create the Orderable Item.....	6
4.2	Make the Quick Orders.....	7
5.0	Install the Dialog.....	8
5.1	Installing the Item from Exchange.....	8
5.2	Installing Dialog – Part 1.....	9
5.3	Install Dialog – Part 2.....	11
5.4	Taxonomy Error.....	13
5.5	Activate the Dialog.....	13
5.5.1	Reminder Dialog Management (DLG).....	13
6.0	Update the TIU Templates.....	15
6.1	Activate Note Title.....	16
6.2	Attaching the Dialog to a TIU Note Title.....	16
6.3	Adding the Janssen Vaccine to the TIU Object	18
7.0	Troubleshooting	21
7.1	If the Finish Button Remain Greyed Out.....	21
7.2	Missing Purpose of Visit (POV).....	21
7.3	Immunizations Missing Documentation	22
Appendix A	Rules of Behavior	19
A.1	All RPMS Users	19
A.2	Access	20
A.2.1	Information Accessibility	20
A.2.2	Accountability	21
A.2.3	Confidentiality.....	21
A.2.4	Integrity.....	21
A.2.5	System Logon.....	22
A.2.6	Passwords.....	22
A.2.7	Backups.....	23
A.2.8	Reporting.....	23

A.2.9	Session Timeouts	23
A.2.10	Hardware	24
A.2.11	Awareness.....	24
A.2.12	Remote Access	24
A.2.13	RPMS Developers	25
A.2.14	Privileged Users	26
Acronym List	28
Contact Information	29

Preface

This documentation applies to those reminders distributed in Version 2.0, Patch 1010 and 2011 of Clinical Reminders.

1.0 Introduction

This guide was designed to supplement the patch installation notes and provide guidance for setting up the Clinical Reminders contained in the PXRМ V2.0 1010 and PXRМ v2.0 1011 patches. We strongly recommend reviewing this entire document before installing and setting up the Clinical Reminders Version 2.0 Patch 1010 and 1011.

It is intended to be used by the following individuals who are responsible for installing, supporting, maintaining, and testing this package:

- Information Resources Management (IRM)
- Clinical Application Coordinator (CAC)

1.1 Clinical Reminders Resources

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 (PXRМ) section.

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

2.0 COVID-19 Reminder Dialog

This section provides an overview of the major changes in the Clinical Reminders patch 1010 and 1011. The new reminders are:

IHS-IMMUNIZATION COVID POLICY ORDERS
IHS-IMMUNIZATION COVID POLICY ORDERS-202103

2.1 TIU v1.0 Patch 1023

This patch is a dialog only and can be attached to the **COVID-19 VACCINE POLICY ORDER** note title that is included in TIU*1.0*1023. See the [Attaching the Dialog to a TIU Note](#) section for instructions. This is *not* required but highly desirable.

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

2.1.1 Document Class and Note Title

A new document class and note title are included in the TIU v1.0 p1023 patch.

- The document class is:
CLINICAL REMINDER DIALOG IMMUNIZATIONS
- The note title is:
COVID-19 VACCINE POLICY ORDER

These items will come **DISABLED** and need to be enabled at the site before use. The note title is connected to the national note title of **IMMUNIZATION NOTE** (Figure 2-1).

Visit: 12/17/20 COVID-19 VACCINE POLICY ORDER, ERPENBACH, [REDACTED] (Dec 17,20@12:23)	
LOCAL TITLE: COVID-19 VACCINE POLICY ORDER	
STANDARD TITLE: IMMUNIZATION NOTE	
DATE OF NOTE: DEC 17, 2020@12:23	ENTRY DATE: DEC 17, 2020@12:23:30
AUTHOR: [REDACTED]	EXP COSIGNER:
URGENCY:	STATUS: UNSIGNED

Figure 2-1: Sample Immunization Note window

There is a post-signature action on this note title. It will create a problem with **SNOMED 713404003** if it does not already exist and a **POV of Z23** for the visit.

If the **COVID-19** reminder dialog is attached to this note title, all the documentation of a COVID-19 immunization can be done in one place.

2.1.2 Prerequisites for TIU v1.0 p1023

The following are prerequisites for TIU v1.0 p1023:

- TIU*1.0*1022
- Kernel (XU) v8.0 patch 1018 or later
- FileMan (DI) v22.0 patch 1018 or later

2.2 PXRM v2.0 Patch 1010 and PXRM v2.0 Patch 1011

This patch contains the reminder dialog designed to document the administration of the COVID-19 vaccinations.

The first two vaccinations are included in Patch 1010:

- Moderna and Pfizer

Patch 1011 adds in the Janssen vaccination.

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

This reminder dialog adds the following:

- Orders
- 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 [Update the TIU Templates](#) section in this document.

2.2.1 Prerequisites

2.2.1.1 PXRM 1010

- BI*8.5*1000
- ACPT*2.20*9 – The COVID codes *must* have been activated before installing
See acpt2020.09n for data on activating the codes.
- LEX*2.0*1011
- TIU*1.0*1023
- PXRM*2.0*1009

2.2.1.2 PXRM 1011

- ACPT 2.21 – The COVID codes *must* have been activated before installing
- BI*8.5*1001
- PXRM*2.0*1010

3.0 Install the KIDS Build

Installation of **PXRМ 1010/1011** should be done by the appropriate IRМ personnel using the instructions in the patch notes. Users may be on the system.

Installation of **Patch 1010/1011** will put the reminder dialog into the **REMINDER EXCHANGE** file.

Note: It does *not* install it.

The new dialog will not work until it is installed and activated.

Important: If both patches are being installed at the same time and the reminder dialog contained in patch 1010 has not yet been installed and used, the site does **NOT** need to install this dialog. They can go directly to installing the latest dialog which includes the Janssen immunization. Patch 1010 still does need to be installed.

4.0 Create the Quick Orders

This dialog uses two quick orders that cannot be uploaded using Reminder Exchange.

Prior to installing the dialog, create the **quick orders**.

4.1 Create the Orderable Item

1. From the **RPMS-EHR CONFIGURATION MENU**, select **ORD**.
2. Then select **MNU Order Menu Management** (Figure 4-1).

```
DOC    Delayed Orders Configuration ...
KEY    Key Management ...
MNU  Order Menu Management ...
OCX    Order Check Configuration ...
PAR    Order Parameters ...
PRN    Print/Report Parameters ...
RPT    Order Reports ...
```

Figure 4-1: Order Menu

3. On this menu (Figure 4-2), select **OIC** to make the orderable item.

```
ACT    Create/Modify Actions
DIS    Enable/Disable Order Dialogs
GEN    Create/Modify Generic Orders
LST    List Primary Order Menus
MNU    Create/Modify Order Menus
OIC  Create/Modify Orderable Items <<- Use for orderable item
PAR    Menu Parameters ...
PMT    Create/Modify Prompts
PRI    Assign Primary Order Menu
PRT    Convert Protocols
QOC    Create/Modify Quick Orders ← Use for quick order
QOR    Create/Modify QO Restrictions
SET    Create/Modify Order Sets
SNO    Unconverted Clinical Indication to SNOMED
SRC    Search/Replace Components
SRO    Search/Replace Orderables
```

Figure 4-2: Order Menu Management

4. Select **Order Menu Management <TEST ACCOUNT> Option: OIC Create/Modify Orderable Items** (Figure 4-3).

```
Type of Orderable: NURSING
Select ORDERABLE ITEMS: COVID-19 VACCINE
Are you adding 'COVID-19 VACCINE' as a new ORDERABLE ITEMS (the 4063RD)?
No//Y
(Yes)
NAME: COVID-19 VACCINE//
```

Figure 4-3: Type of Orderable

4.2 Make the Quick Orders

All the quick orders can use the same orderable item so other than the names, the rest will be identical. Make one for Pfizer, one for Moderna, and one for Janssen. If the site wishes to make three (3) orderable items, that is acceptable as well.

The quick orders must have the same names as the one in the reminder dialog, which are:

```

ORZ POLICY COVID_19 PFIZER IMMUNIZATION
ORZ POLICY COVID_19 MODERNA IMMUNIZATION
ORZ POLICY COVID_19 JANSSEN IMMUNIZATION

```

Figure 4-4: Quick Order Names

1. Select **QOC** from the above menu (Figure 4-2). Figure 4-5 displays.

```

Select QUICK ORDER NAME: ORZ POLICY COVID_19 IMMUNIZATION
  Are you adding 'ORZ POLICY COVID_19 PFIZER IMMUNIZATION' as
    a new ORDER DIALOG? No// Y (Yes)
TYPE OF QUICK ORDER: NURSING
NAME: ORZ POLICY COVID_19 PFIZER IMMUNIZATION  Replace
DISPLAY TEXT: Covid_19 Pfizer Immunization
VERIFY ORDER:
DESCRIPTION:
  No existing text
  Edit? NO//
ENTRY ACTION:

Enter a patient care item.

Patient Care: COVID-19 VACCINE
Instructions: Give per protocol
Start Date/Time: NOW//
Stop Date/Time: T+1

-----
                Patient Care: COVID-19 VACCINE
                Instructions: Give per protocol
                Start Date/Time: NOW
-----

(P)lace, (E)dit, or (C)ancel this quick order? PLACE//
Auto-accept this order? NO//

```

Figure 4-5: Create/Modify Quick Orders

Note: Adding a Stop Date will allow for the order to expire and drop off from the Orders Tab.

5.0 Install the Dialog

Follow these instructions to install the **National COVID** dialog. The CAC or another designated person should install it using **REMINDER EXCHANGE**.

5.1 Installing the Item from Exchange

1. Select **Reminder Exchange** from the **Reminder Configuration** menu (Figure 5-1). You will be presented with a list of packed reminders that reside in the RPMS file system.

+Item	Reminder Dialog Name	Source Reminder	Status
117	IHS-IMMUNIZATION COVID POLICY ORDERS	*NONE*	
118	IHS-IMMUNIZATION COVID POLICY ORDERS-20	*NONE*	
119	IHS-INFLUENZA IMMUN 2008	IHS-INFLUENZA IMMUN 2008	Disabled
120	IHS-INFLUENZA IMMUN 2011	IHS-INFLUENZA IMMUN 2011	Linked
121	IHS-INFLUENZA IMMUN 2017	IHS-INFLUENZA IMMUN 2017	Disabled
122	IHS-INFLUENZA IMMUNIZATION	IHS-INFLUENZA IMMUNIZATIO	Disabled
123	IHS-INFLUENZA IMMUNIZATION 2007	IHS-INFLUENZA IMMUNIZATIO	Disabled
124	IHS-LIPID FEMALE	IHS-LIPID FEMALE	Linked
125	IHS-LIPID FEMALE 2012	IHS-LIPID FEMALE 2012	Linked
126	IHS-LIPID MALE	IHS-LIPID MALE	Linked
127	IHS-LIPID MALE 2012	IHS-LIPID MALE 2012	Linked
128	IHS-MAMMOGRAM	IHS-MAMMOGRAM	Disabled
129	IHS-MAMMOGRAM 2007	IHS-MAMMOGRAM 2007	Disabled
130	IHS-MAMMOGRAM 2008	IHS-MAMMOGRAM 2008	Disabled

Figure 5-1: Exchange List of Reminders

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

2. If you are searching for a specific reminder, use the command **SL** to search for the **reminder name**. For patch 1011, it is **IHS-IMMUNIZATION COVID POLICY ORDERS-202103**.

```
Select Action: Next Screen// SL
Search for: //COVID
```

Figure 5-2: SL Command

3. Select **IFE – Install Exchange File Entry** to install the reminder.
4. Enter the **number of the reminder** (Figure 5-3) to install.

```

Cache TRM:17592 (ENSEMBLE)
File Edit Help
Clinical Reminder Exchange  Dec 09, 2020 16:10:13  Page: 6 of 13
Exchange File Entries.

+Item  Entry                               Source                               Date Packed
-----  -
53  IHS-IMMUNIZATION COVID POLICY  USER@DEMO HOSPITA  12/09/2020@15:44
    ORDERS
54  IHS-IMMUNIZATION FORECAST 2013  USER@DEMO HOSPITA  04/21/2014@14:44
55  IHS-INFLUENZA IMMUN 2013        USER@DEMO HOSPITA  04/21/2014@14:44
56  IHS-LIPID FEMALE 2015           USER@DEMO HOSPITA  11/05/2015@13:02
57  IHS-LIPID MALE 2015             USER@DEMO HOSPITA  11/05/2015@13:02
58  IHS-MAMMOGRAM 40-49 2017        USER@DEMO HOSPITA  05/03/2018@08:56
59  IHS-MAMMOGRAM 50-74 2017        USER@DEMO HOSPITA  05/03/2018@08:56
60  IHS-MAMMOGRAM 75-100 2017       USER@DEMO HOSPITA  05/03/2018@08:57
61  IHS-MED ED 2013                 USER@DEMO HOSPITA  04/21/2014@14:46

+  + Next Screen  - Prev Screen  ?? More Actions  >>>
CFE Create Exchange File Entry  LHF Load Host File
CHF Create Host File            LMM Load MailMan Message
CMM Create MailMan Message       LR List Reminder Definitions
DFE Delete Exchange File Entry   LWH Load Web Host File
IFE Install Exchange File Entry  RI Reminder Definition Inquiry
IH Installation History

Select Action: Next Screen// IFE Install Exchange File Entry
Enter a list or range of numbers (1-118): 53

```

Figure 5-3: Reminder List with number selected.

5.2 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 5-4). You can use either the up and down arrows on the keyboard or just select return to view all the items.

```

Cache TRM:17592 (ENSEMBLE)
File Edit Help
Exchange File Components      Dec 09, 2020 16:12:39      Page: 4 of 6
+-----Component-----+-----Category-----+Exists-
      ORZ POLICY COVID_19 IMMUNIZATION                                X

TIU TEMPLATE FIELD
 1  GEN TEXT 50                                                       X
 2  OCA IMM NO REACTION V1                                           X
 3  OCA IMM ASSESSMENT V2                                            X
 4  GEN WORD INDENT 2                                                X
 5  GEN YES/NO RADIO                                                 X
 6  OCA COVID-19 MANUFACTURER                                        X
 7  GEN DATE                                                         X
 8  OCA COVID-19 IF 2ND DOSE                                         X
 9  DATE AND TIME V1                                                 X
10  OCA YES/NO/DON'T KNOW DEF NO                                     X
11  IHS COVID19IMM POLICY DATE                                       X
12  IHS COVID19IMM POLICY ID                                         X
13  IHS COVID19IMM POLICY NAME                                       X

Enter RETURN to continue or '^' to exit:

```

Figure 5-4: 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 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 5-5) in this dialog. Install all of them. Take the default and install them.

```

TIU TEMPLATE FIELD entry GEN TEXT 50 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// nstall

TIU TEMPLATE FIELD entry OCA IMM NO REACTION V1 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// nstall

```

Figure 5-5: TIU Template Fields

2. There are also **some new taxonomies** (Figure 5-6) to be installed.

```

REMINDER TAXONOMY entry CPT IMM COVID19 2ND DOSE (JOHNSON & JOHNSON) 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//

```

Figure 5-6: Installing Taxonomies

3. Make sure that the **quick order** exists. If you forgot to create the quick order, you will see the following (Figure 5-7):

```

ADDITIONAL FINDING entry Q.ORZ POLICY COVID_19 IMMUNIZATION does not
exist.

      Select one of the following:

      D      Delete
      P      Replace with an existing entry
      Q      Quit the install

Enter response:

```

Figure 5-7: Missing Quick Order warning

You can do one of the following:

- Quit the install, make the quick order, and start over.
- Open another session, make the quick order, and then select **P Replace with an existing entry** to replace the one in the install with the one you just made on your system.

5.3 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 5-8: 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 5-9). If they are identical, it will not update the item on your database.

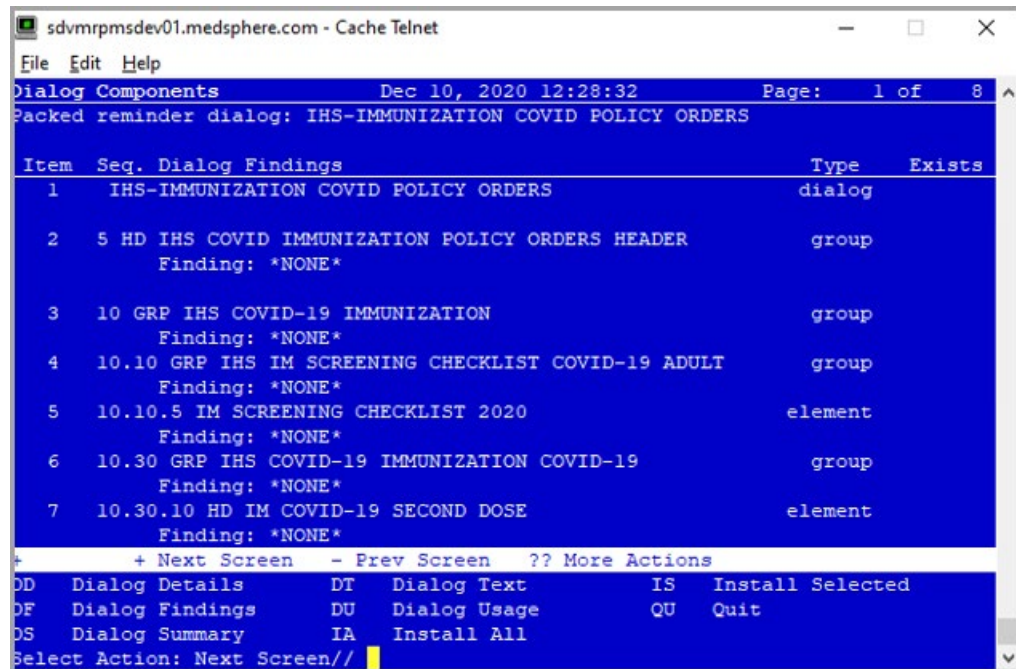


Figure 5-9: Dialog Section

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.

5.4 Taxonomy Error

A taxonomy is a selection of **ICD procedure**, **ICD diagnosis**, and/or **CPT procedure codes**. The user inputs them from the starting code to the ending code. One taxonomy can have multiple selection lists of codes. In this patch, the codes are all CPT codes.

You *must* have activated the **CPT codes** in **ACPT*2.20*9** and **ACPT 2.21** before installing this patch. The codes will not install if they are inactive.

Also, until Lexicon patch 1011 is installed, you can only view the codes in the taxonomy using FileMan. This patch is not required but will make viewing of the codes easier.

5.5 Activate the Dialog

All dialogs are inactive if they are loaded from Reminder Exchange (Figure 5-10). This section describes how to activate the dialog so that they are visible within the EHR.

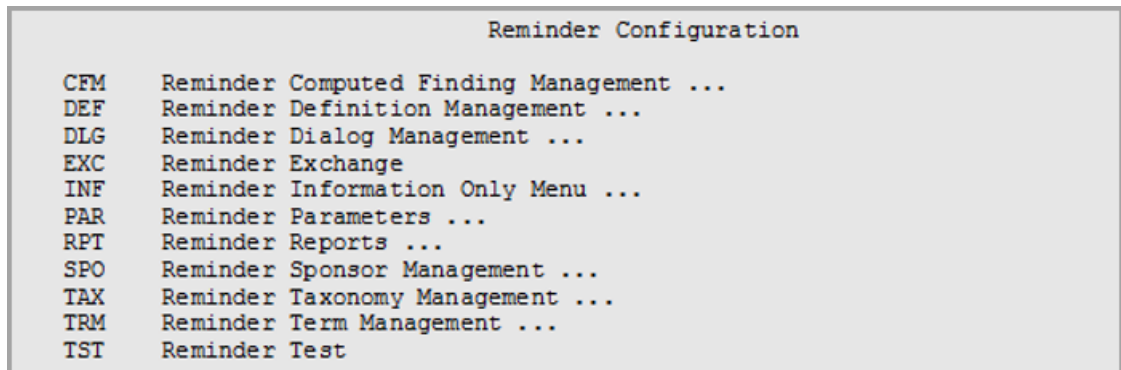


Figure 5-10: Reminder Menu

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

5.5.1 Reminder Dialog Management (DLG)

1. Select **Reminder Dialog Management** (Figure 5-11) from the **Reminder Configuration** menu.



Figure 5-11: Reminder Dialog Management

- Use the **DLG** option to access the options on the **Reminder Dialog Management** menu (Figure 5-12).

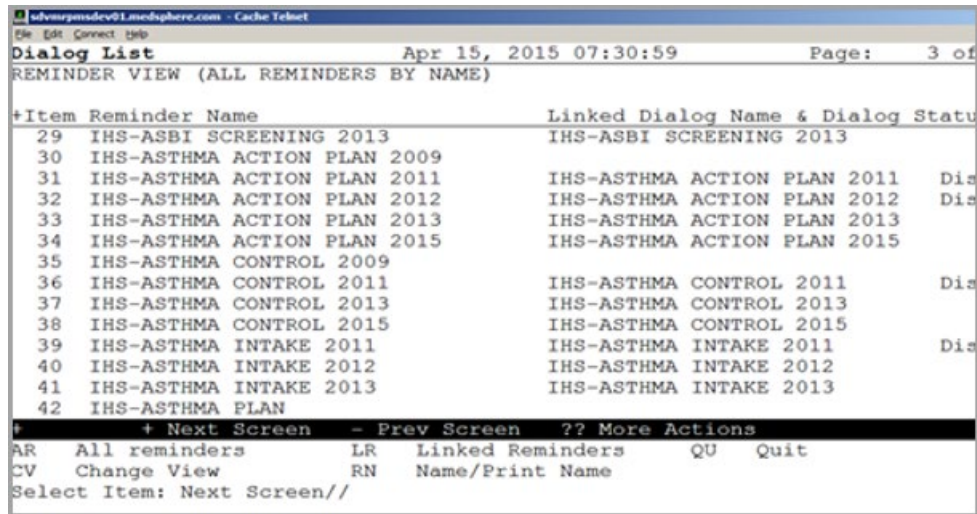


Figure 5-12: Sample Reminder View

- Choose **CV**, and then choose **D** for dialogs (Figure 5-13).

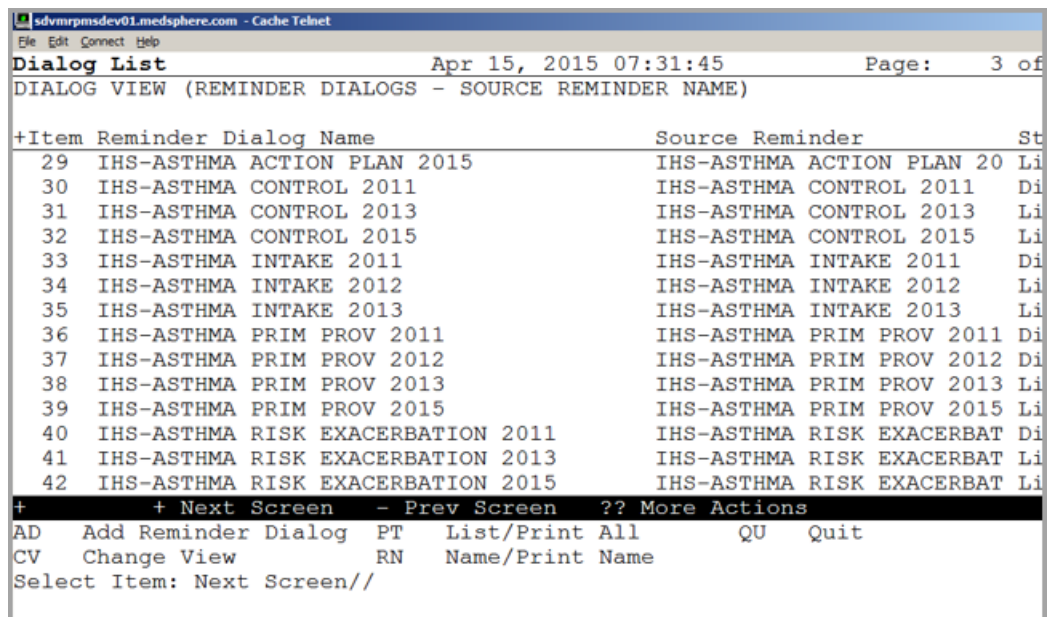


Figure 5-13: Sample Dialog View

- Select the **number** of the **item** you want to edit **IHS-IMMUNIZATION COVID POLICY ORDERS** (Figure 5-14).

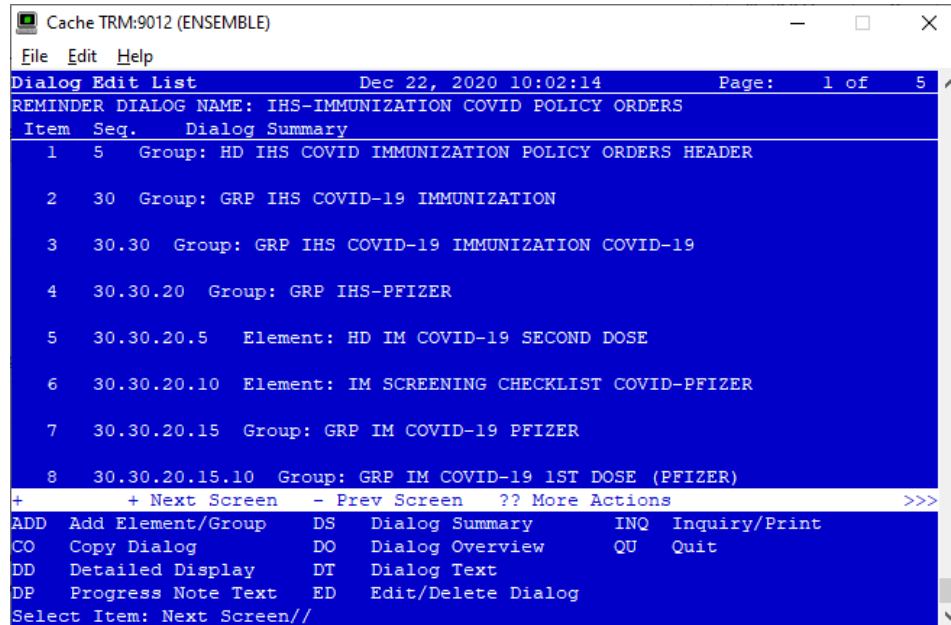


Figure 5-14: Dialog Edit List Window

- Select the **dialog**. It will say **Disabled** instead of **Linked**.
- Choose **ED (Edit/Delete Dialog)**.

The second prompt will state:

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

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

You will then be asked:

“Are you sure you want to DELETE?., YES.” Press Enter.

- Type a caret (^) to quit editing.

6.0 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. If patch 1010 has been installed, this piece should not need to be redone. After loading the dialog, go into the TIU template editor (Figure 6-2) and change the text for the following template fields:

```
IHS COVID 19 LOCATION
IHS COVID19 IMM SITE NAME
IHS COVID19IMM FORM NUMBER
IHS COVID19IMM POLICY NAME
IHS COVID19IMM POLICY ID
IHS COVID19IMM POLICY DATE
```

Figure 6-1: Template fields

1. Change to your site's information.

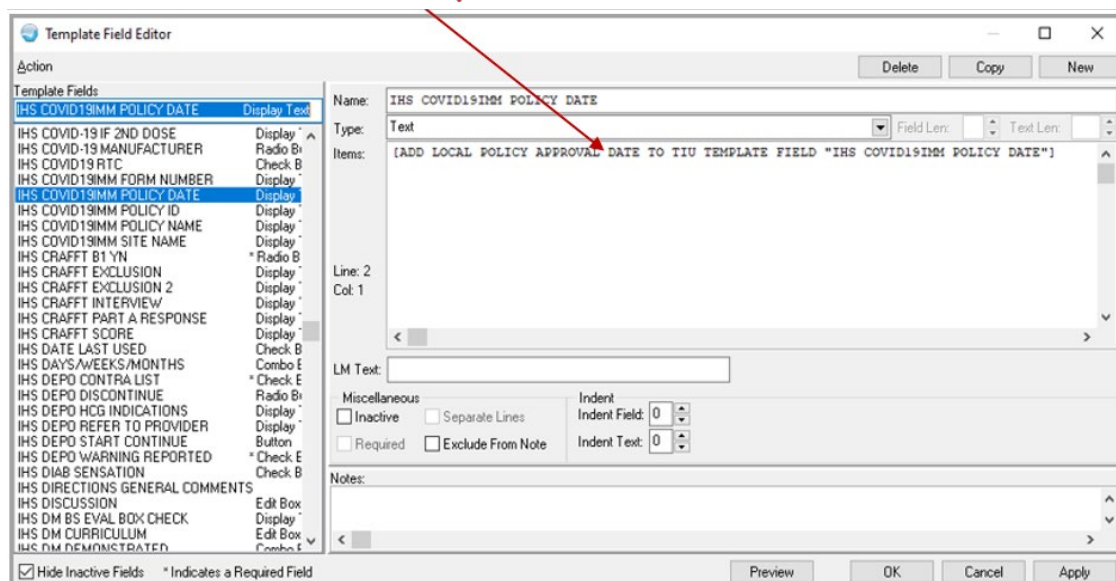


Figure 6-2: TIU Template Editor

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 6-3) 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 6-3: Setting TIU TEMPLATE REMINDER DIALOGS

3. Add a new **sequence number** for this dialog (Figure 6-4).

```

Display Sequence: 22//    22
Clinical Reminder Dialog: IHS-PED MMRV IMMUN 2013//

```

Figure 6-4: Display Sequence

6.1 Activate Note Title

In TIU, find and activate both the document definition and the note title.

Activate the note title **COVID-19 VACCINE POLICY ORDER** (Figure 6-5).

```

DDM3  Create Document Definitions

2  PROGRESS NOTES                CL
3  CLINICAL REMINDER DIALOG IMMUNIZATIONS  DC  <<This may need to be made ACTIVE
4  COVID-19 VACCINE POLICY ORDER      TL  <<This may need to be made ACTIVE

```

Figure 6-5: Activate Note Title

6.2 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 6-6).
 - d. In the **Reminder Dialog**, find the reminder dialog **COVID-19 VACCINE POLICY ORDER** in the drop-down list.
 - e. Select the **Associated Title** (note title) **COVID-19 VACCINE POLICY ORDER**. 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**.

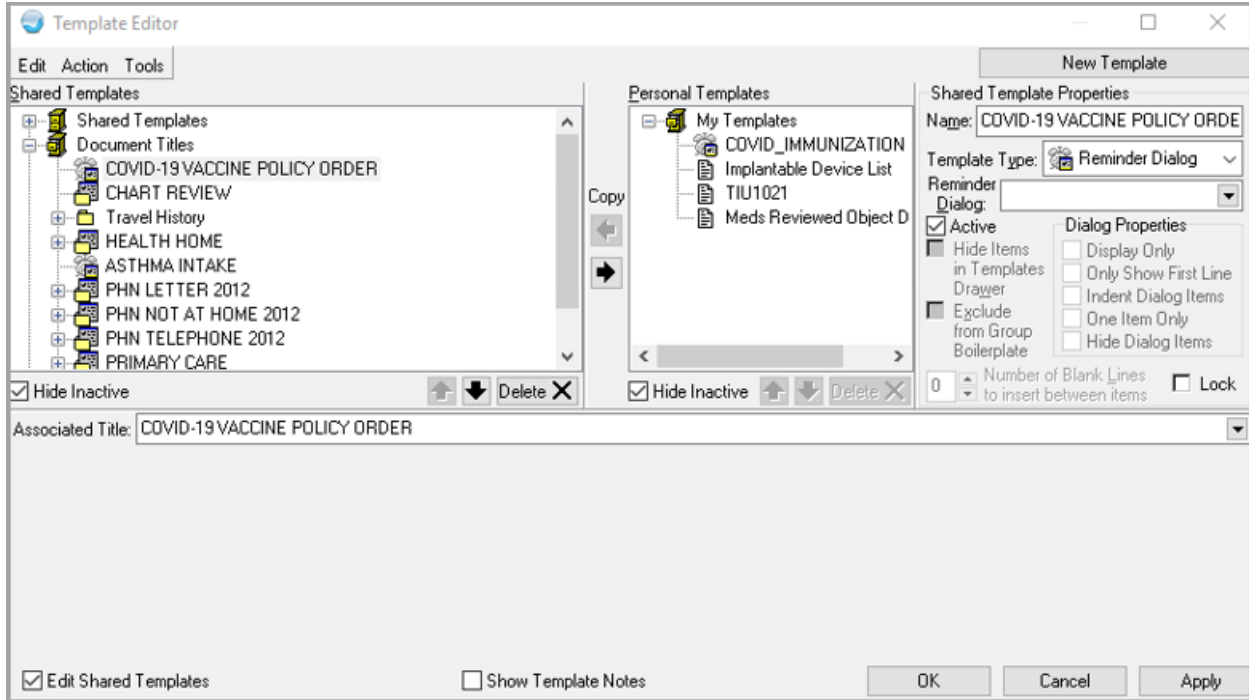


Figure 6-6: Template Editor for Reminder Dialogs

- Users may also want to attach this template to a **Note Title** or to a **Quick Note** (Figure 6-7).

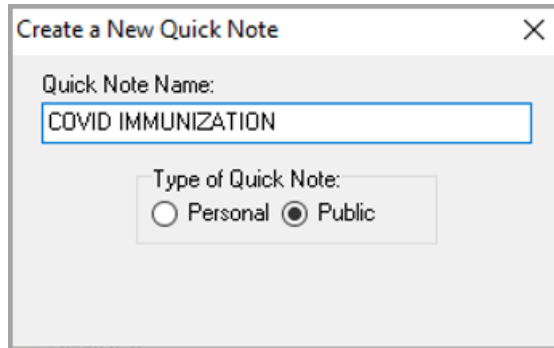


Figure 6-7: Quick Note Creator

- Use the TIU title in patch 1023, and the dialog (Figure 6-8) in this reminders patch.

Figure 6-8: Quick Note dialog

6.3 Adding the Janssen Vaccine to the TIU Object

Sites will need to add **CVX Code 212** to the **BPXRM COVID VACCINE TIU** object. To do this, follow the steps below:

1. Select the object menu.

```

1      Edit Document Definitions
2      Sort Document Definitions
3      Create Document Definitions
4      Create Objects
      Create TIU/Health Summary Objects

```

Figure 6-9: Object menu

2. Find the **BPXRM COVID VACCINE** in the list.

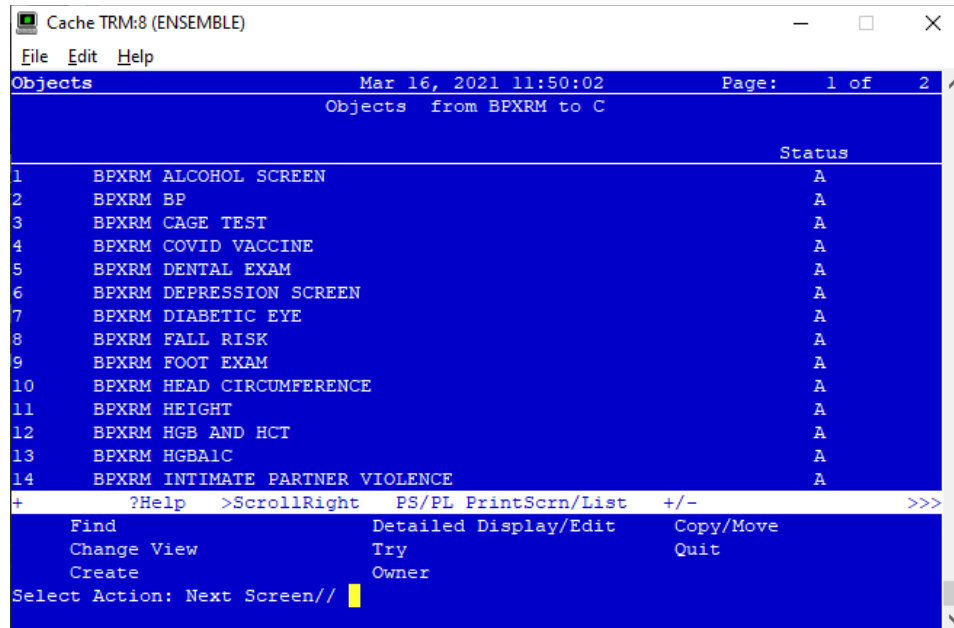


Figure 6-10: List of TIU objects

3. Edit the **BPXRM COVID VACCINE**.

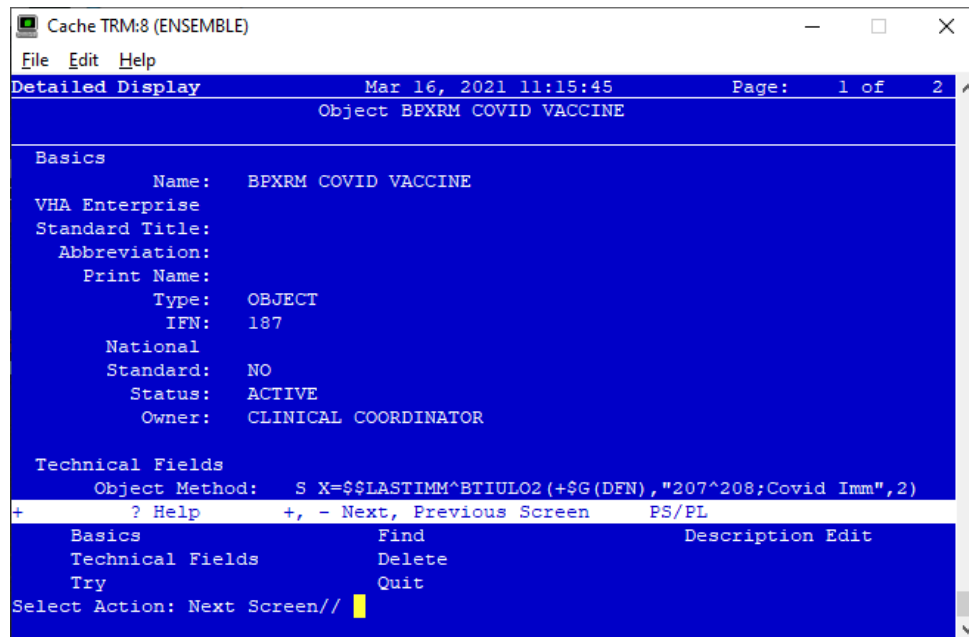


Figure 6-11: BPXRM COVID VACCINE object

4. Inactivate the object by selecting **Basics**.

Edit Owner and Status only, Entry not Inactive.


```

NAME: BPXRM COVID VACCINE//
ABBREVIATION:
PRINT NAME:
CLASS OWNER: CLINICAL COORDINATOR// CLINICAL COORDINATOR
STATUS: (A/I): ACTIVE// I INACTIVE Inactivated

```

Figure 6-12: Editing the Owner and the Status

5. Edit the Technical Field.

```

\
OBJECT METHOD: S X=$$LASTIMM^BTIULO2(+$G(DFN),"207^208;Covid Imm",2)
                Replace 208 With 208^212 Replace <RET>
                S X=$$LASTIMM^BTIULO2(+$G(DFN),"207^208^212;Covid Imm",2)

```

Figure 6-13: Editing the Technical Field

6. Reactivate the object by selecting Basics.

```

NAME: BPXRM COVID VACCINE//
ABBREVIATION:
PRINT NAME:
CLASS OWNER: CLINICAL COORDINATOR// CLINICAL COORDINATOR
STATUS: (A/I): INACTIVE// A

```

Figure 6-14: Reactivating the object

7.0 Troubleshooting

7.1 If the Finish Button Remain Greyed Out

Issue: In some instances, the **Finish** button at the bottom of the dialog remains greyed out even though the user has finished documenting.

Troubleshooting Issue:

1. Click the **Refresh** at the top of EHR.
2. A box will display that asks if the user would like to delete the note. Click **No**.
3. The **Finish** button should then reappear, and the user can finish your note without having to redo anything.

7.2 Missing Purpose of Visit (POV)

Issue: The POV is missing from the Integrated Problem List (IPL).

A check to the post-signature code was added to ensure that an immunization was documented in the immunization package for the selected visit before the POV would be added. If the POV has not been added to the IPL, review the following:

- Was an immunization documented at this visit? (The user may have cancelled out of the dialog early or missed the check box to actual add in the immunization.)
- Does the patient have multiple visits and perhaps the note title is on one and the immunization is documented in another? (This would not occur if documenting the immunization via the reminder dialog but could occur if someone was simply testing the note title.)
- Did the user actually sign the note? (Post-signature code will not fire until note is signed.)
- Does the note have a co-signer who has yet to sign? (Post-signature code will not fire until co-signer also signs.)

Troubleshooting issue

For a quick test at the site to confirm POV stuffing functionality:

1. Create a visit on a demo patient.
2. Document a new immunization record in the EHR immunization component.
3. Write a note using the **COVID-19 VACCINE POLICY ORDER** note title with text of “**test**” or something similar.
4. Sign the note.

5. Review the POV/visit details.

7.3 Immunizations Missing Documentation

Issue: Immunizers are missing the documentation of the immunization (lot, site, etc.) leading to deficiencies in the medical record.

The reason for immunizers missing the documenting of the immunization could be the following:

- The immunization documentation piece follows right after a long list of questionnaire answers and gets lost as the user scrolls down the questionnaire and onto the next item that is not indented.
- The user has clicked on the 1st or 2nd dose radio button, but not clicked the check box that displays the immunization documentation dialog.

Troubleshooting Issue:

- Site process to ensure no immunization are missed.
- Train immunizers on using the dialog and how to document the immunizations fully (including checking the immunization check box and the radio button for either the 1st or 2nd dose)
- Make sure that the documentation of the actual immunization is not missed.

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>.

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

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
CAC	Clinical Application Coordinator
CISO	Chief Information Security Officer
EHR	Electronic Health Record
HIPAA	Health Insurance Portability and Accountability Act
ID	Identification
IHS	Indian Health Service
IPL	Integrated Problem List
IRM	Information Resources Management
ISSO	Information System Security Officer
PC	Personal Computer
POV	Purpose of Visit
RPMS	Resource and Patient Management System
SAC	Standards and Conventions
TIU	Text Integrated Utility
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