RESOURCE AND PATIENT MANAGEMENT SYSTEM

Clinical Reminders

(PXRM)

Reminder
Supplemental User Guide

Version 2.0 Patch 2009
February 2023

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

This documentation applies to those reminders distributed in Version 2.0, Patch 2009 of Clinical Reminders.

1.0 Introduction

This guide was designed to supplement the patch installation notes and provide guidance for setting up the **IHS-SYPHILIS Reminder and Dialog** contained in the **PXRM v2.0 2009** patch. It is strongly recommended that users review this entire document before installing and setting up the **Version 2.0 Patch 2009**.

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 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 the **VA Clinical Reminders (PXRM)** section.

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

2.0 Reminder and Dialogs

This section provides an overview of the major changes in the **Reminder Patch 2009**.

2.1 New Syphilis testing Reminder & Dialog

This patch contains the reminder and dialog designed to document the Syphilis testing for ages 13-64.

The new Reminder is listed below:

IHS-SYPHILIS TEST-20221205

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

Sites can change the dialog to reflect the **facility name**, **policy**, **form**, **ID**, and **date**. These instructions can be found in Update the Dialog with Local Policies in this document.

Refer to the **Supplemental User Guide** for patches **1010**, **1011**, **1012**, and **1013** for further information.

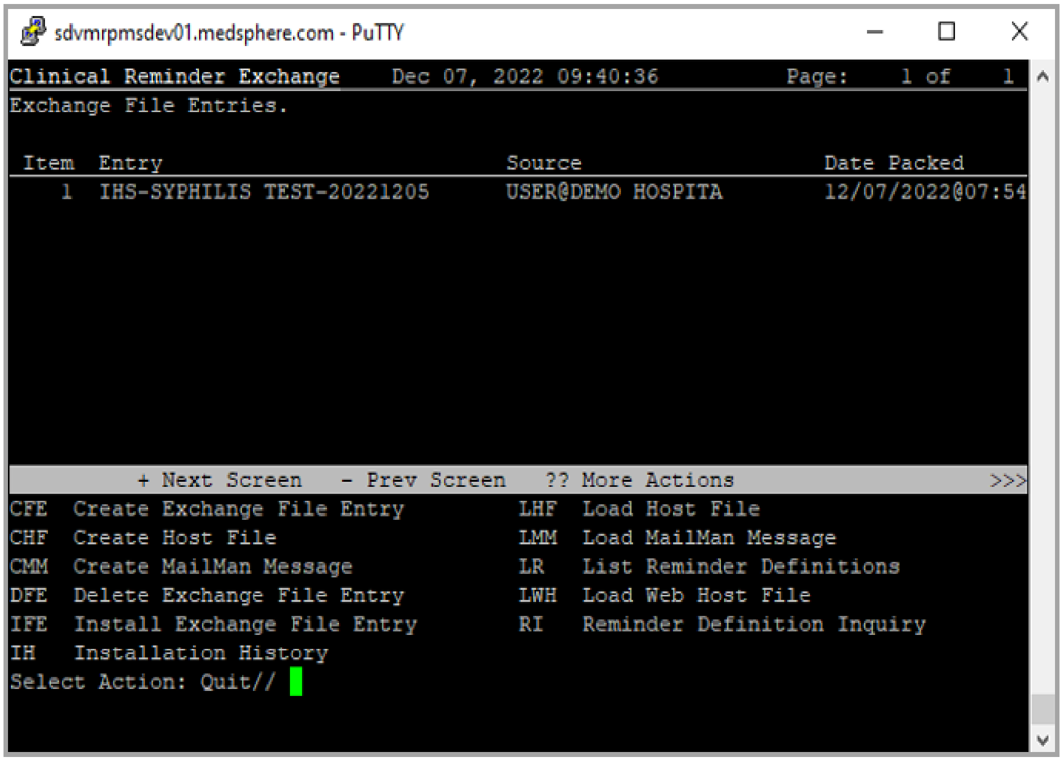
2.2 Prerequisites

- ACPT*2.22*10
- PXRM*2.0*2007
- BI*8.5*1010

3.0 Install the KIDS Build

Installation of **PXRM 2009** should be done by the appropriate IRM personnel using the instructions in the patch notes. Users may be on the system.

Installation of **Patch 2009** puts the reminder into the **REMINDER EXCHANGE** file.



```
Clinical Reminder Exchange    Dec 07, 2022 09:40:36          Page:    1 of    1
Exchange File Entries.

 Item  Entry                            Source                   Date Packed
    1  IHS-SYPHILIS TEST-20221205       USER@DEMO HOSPITA        12/07/2022@07:54










          + 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: Quit//
```

Figure 3-1: Reminder Exchange file

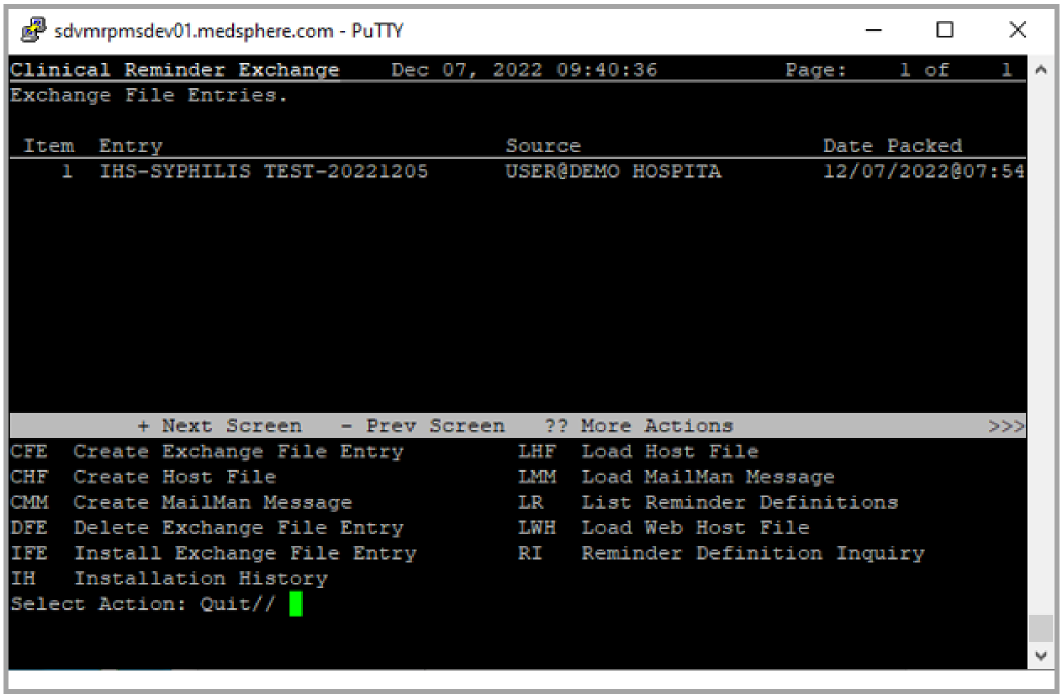
Important: This **DOES NOT** install the new reminders/dialogs. They will not work until they are installed and activated.

4.0 Installing the Reminder/Dialog

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

4.1 Installing the Item from Exchange

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



```
Clinical Reminder Exchange    Dec 07, 2022 09:40:36          Page:    1 of    1
Exchange File Entries.

 Item  Entry                              Source                   Date Packed
    1  IHS-SYPHILIS TEST-20221205         USER@DEMO HOSPITA        12/07/2022@07:54









          + 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: Quit//
```

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** (Figure 4-2) to search for the dialog name. For **patch 2009** there is one:

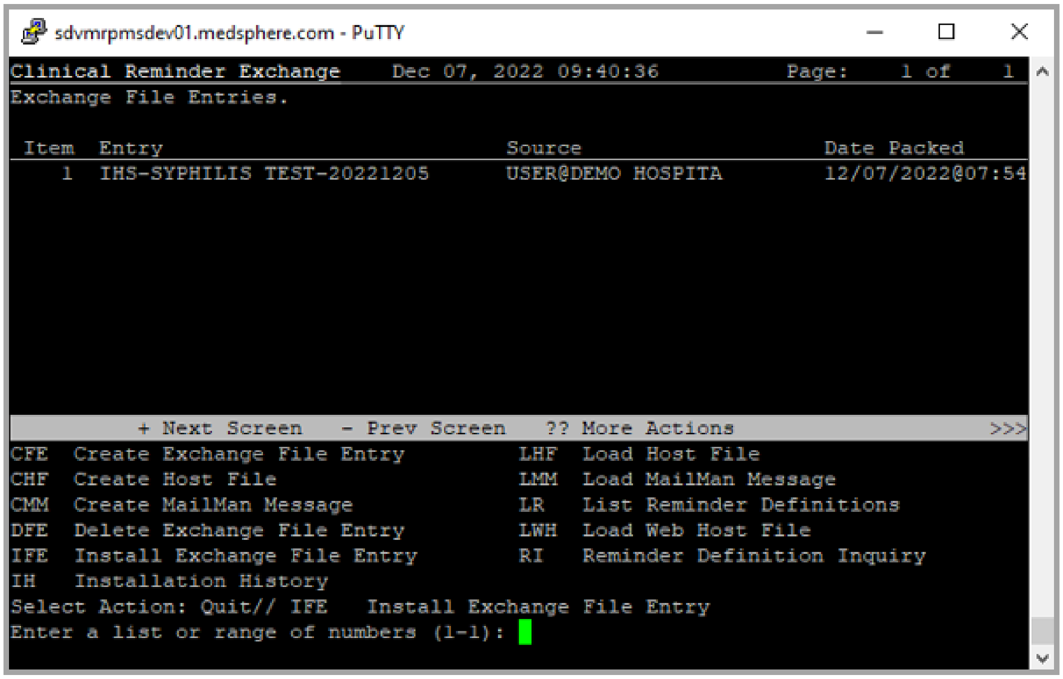
   IHS-SYPHILIS TEST-20221205

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

Figure 4-2: SL Command

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

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



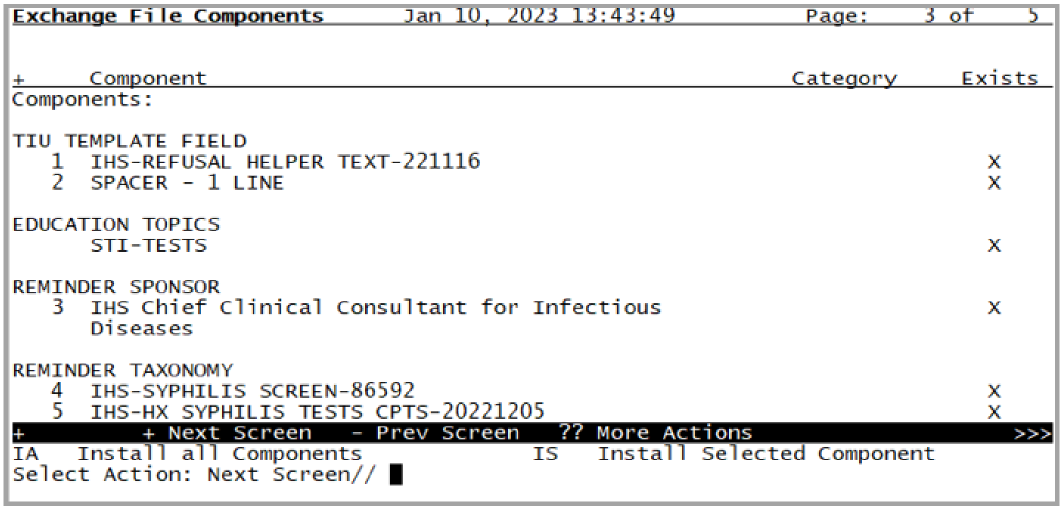
```
Clinical Reminder Exchange    Dec 07, 2022 09:40:36          Page:    1 of    1
Exchange File Entries.

 Item  Entry                             Source                   Date Packed
    1  IHS-SYPHILIS TEST-20221205        USER@DEMO HOSPITA        12/07/2022@07:54










          + 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: Quit// IFE   Install Exchange File Entry
Enter a list or range of numbers (1-1):
```

Figure 4-3: Reminder List with number selected

4.2 Installing Dialog – Part 1

Before starting an installation, users should examine the **list of components** in the packed reminder to determine which ones already exist on their system. Then 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). Use either the **Up** and **Down** arrows on the keyboard or just select return to view all the items.



```
Exchange File Components      Jan 10, 2023 13:43:49          Page:    3 of    5

+     Component                                               Category    Exists
Components:

TIU TEMPLATE FIELD
   1  IHS-REFUSAL HELPER TEXT-221116                                          X
   2  SPACER - 1 LINE                                                         X

EDUCATION TOPICS
      STI-TESTS                                                               X

REMINDER SPONSOR
   3  IHS Chief Clinical Consultant for Infectious                            X
      Diseases

REMINDER TAXONOMY
   4  IHS-SYPHILIS SCREEN-86592                                               X
   5  IHS-HX SYPHILIS TESTS CPTS-20221205                                     X
+         + Next Screen   - Prev Screen   ?? More Actions                   >>>
IA   Install all Components              IS   Install Selected Component
Select Action: Next Screen//
```

Figure 4-4: Exchange Entry screen

- Notice that for each item in the reminder, an **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 then starts.
- 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 (Figure 4-5).
- There are also some new **taxonomies** (Figure 4-5) to be installed. A message asking to install or overwrite is generated for most of the taxonomies. Select the default and install them.

```
REMINDER TAXONOMY entry CPT IMM COVID19 3RD DOSE (MODERNA) 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 4-5: Installing Taxonomies

4.3 Install Dialog – Part 2

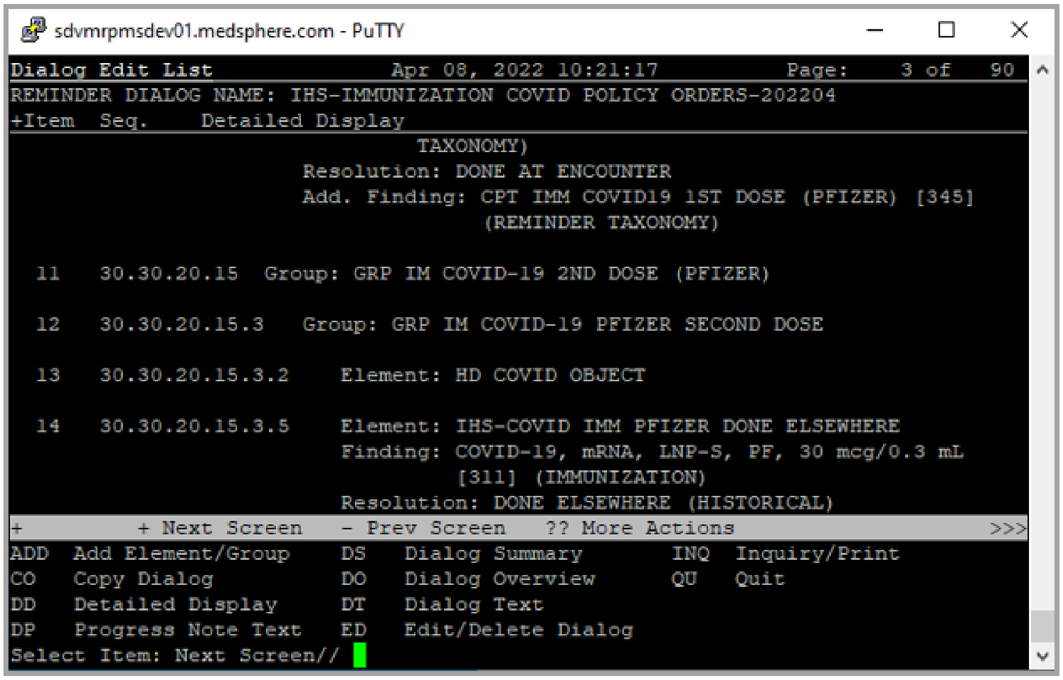
Users will see a **second screen** with a list of the **items** to install. When installing the dialog, there are multiple choices:

```
DD   Dialog Details       DT   Dialog Text          IS   Install Selected
DF   Dialog Findings      DU   Dialog Usage         QU   Quit
DS   Dialog Summary       IA   Install All
```

Figure 4-6: Installation items

1. Select **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 4-7). If they are identical, it will not update the item on your database.



```
Dialog Edit List              Apr 08, 2022 10:21:17          Page:    3 of   90
REMINDER DIALOG NAME: IHS-IMMUNIZATION COVID POLICY ORDERS-202204
+Item  Seq.    Detailed Display
                                TAXONOMY)
                       Resolution: DONE AT ENCOUNTER
                       Add. Finding: CPT IMM COVID19 1ST DOSE (PFIZER) [345]
                              (REMINDER TAXONOMY)

  11   30.30.20.15  Group: GRP IM COVID-19 2ND DOSE (PFIZER)

  12   30.30.20.15.3   Group: GRP IM COVID-19 PFIZER SECOND DOSE

  13   30.30.20.15.3.2    Element: HD COVID OBJECT

  14   30.30.20.15.3.5    Element: IHS-COVID IMM PFIZER DONE ELSEWHERE
                          Finding: COVID-19, mRNA, LNP-S, PF, 30 mcg/0.3 mL
                             [311] (IMMUNIZATION)
                          Resolution: DONE ELSEWHERE (HISTORICAL)
+         + Next Screen   - Prev Screen   ?? More Actions                     >>>
ADD  Add Element/Group    DS   Dialog Summary       INQ  Inquiry/Print
CO   Copy Dialog          DO   Dialog Overview      QU   Quit
DD   Detailed Display     DT   Dialog Text
DP   Progress Note Text   ED   Edit/Delete Dialog
Select Item: Next Screen//
```

Figure 4-7: Dialog Section

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

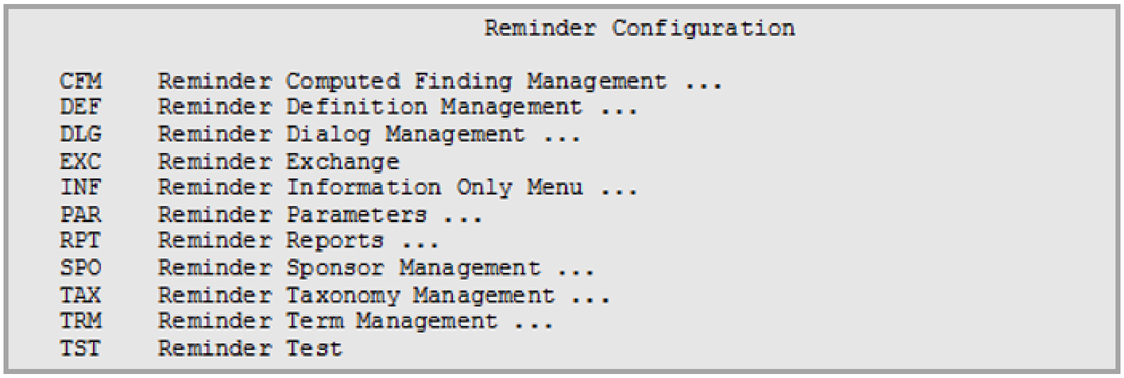
   - If it is not identical, the **application** asks what to do about all **elements** in this reminder. If it is new, the default is to install it.
   - Take all the **defaults** as the reminder is loaded unless a previous version of this reminder has been loaded. If a previous version of the reminder has been loaded, always re-install the reminder definition itself and overwrite any elements.

4.4 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**.

4.5 Activate the Dialog

All dialogs are inactive if they are loaded from **Reminder Exchange** (Figure 4-8). This section describes how to activate the dialog so that they are visible within the **EHR**.



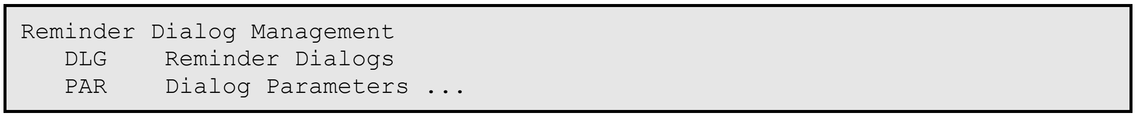
```
                                Reminder Configuration

   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 4-8: Reminder Menu

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

4.5.1 Reminder Dialog Management (DLG)

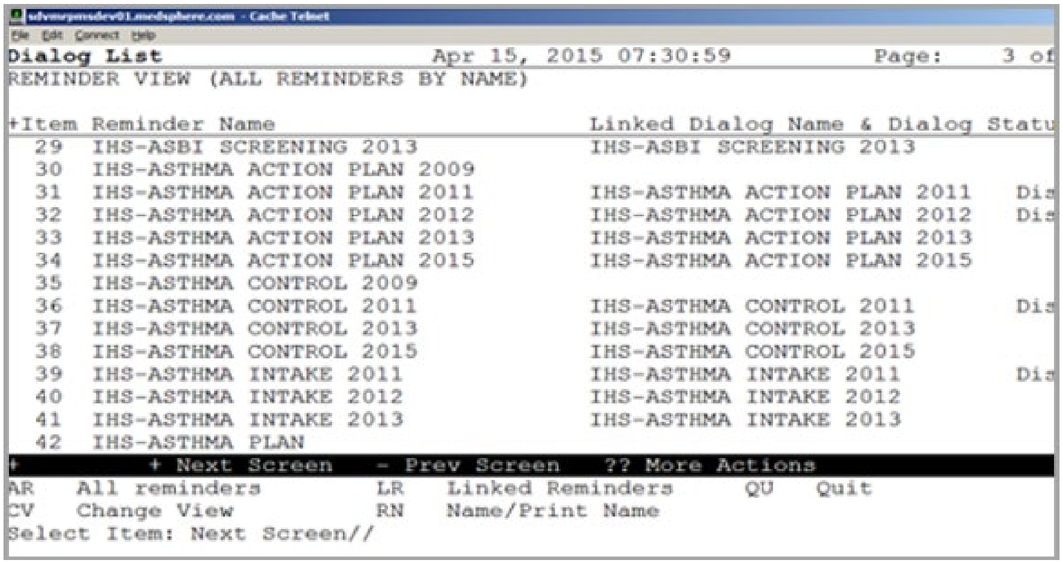
1. Select **Reminder Dialog Management** (Figure 4-9) from the Reminder Configuration menu.



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

Figure 4-9: Reminder Dialog Management

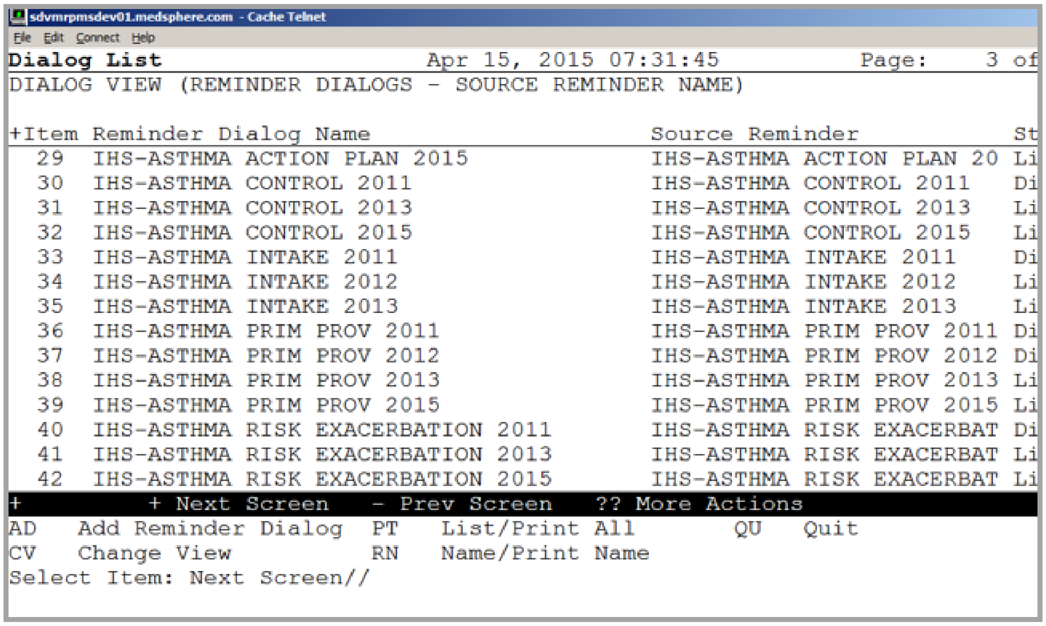
2. Use the **DLG option** to access the options on the **Reminder Dialog Management** menu (Figure 4-10).



```
Dialog List                  Apr 15, 2015 07:30:59          Page:    3 of
REMINDER VIEW (ALL REMINDERS BY NAME)

+Item Reminder Name                          Linked Dialog Name & Dialog Statu
  29  IHS-ASBI SCREENING 2013                IHS-ASBI SCREENING 2013
  30  IHS-ASTHMA ACTION PLAN 2009
  31  IHS-ASTHMA ACTION PLAN 2011            IHS-ASTHMA ACTION PLAN 2011   Dis
  32  IHS-ASTHMA ACTION PLAN 2012            IHS-ASTHMA ACTION PLAN 2012   Dis
  33  IHS-ASTHMA ACTION PLAN 2013            IHS-ASTHMA ACTION PLAN 2013
  34  IHS-ASTHMA ACTION PLAN 2015            IHS-ASTHMA ACTION PLAN 2015
  35  IHS-ASTHMA CONTROL 2009
  36  IHS-ASTHMA CONTROL 2011                IHS-ASTHMA CONTROL 2011       Dis
  37  IHS-ASTHMA CONTROL 2013                IHS-ASTHMA CONTROL 2013
  38  IHS-ASTHMA CONTROL 2015                IHS-ASTHMA CONTROL 2015
  39  IHS-ASTHMA INTAKE 2011                 IHS-ASTHMA INTAKE 2011        Dis
  40  IHS-ASTHMA INTAKE 2012                 IHS-ASTHMA INTAKE 2012
  41  IHS-ASTHMA INTAKE 2013                 IHS-ASTHMA INTAKE 2013
  42  IHS-ASTHMA PLAN
+         + Next Screen   - Prev Screen   ?? More Actions
AR   All reminders          LR   Linked Reminders      QU   Quit
CV   Change View            RN   Name/Print Name
Select Item: Next Screen//
```

Figure 4-10: Sample Reminder View

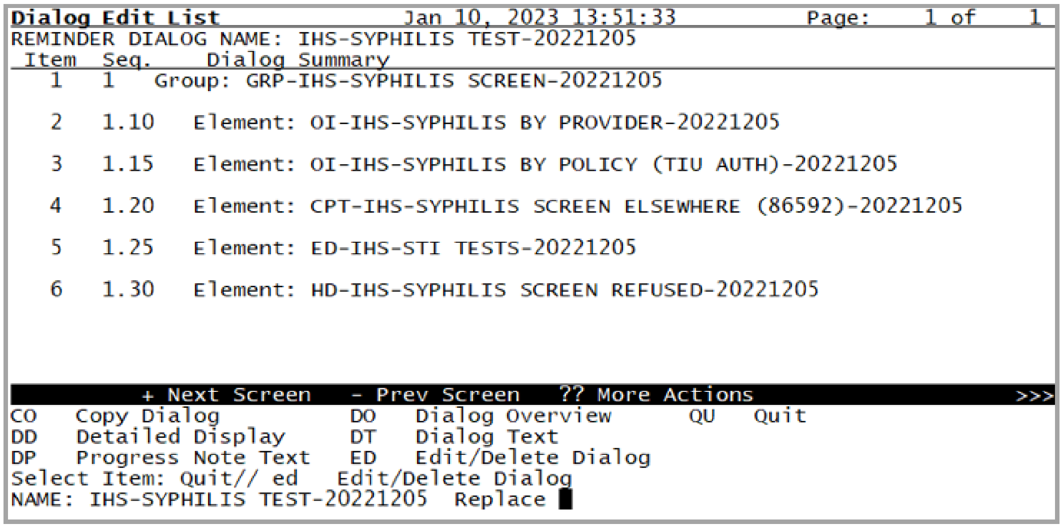
3. Select **CV** and then select **D** for **dialogs** (Figure 4-11).



```
Dialog List                 Apr 15, 2015 07:31:45          Page:    3 of
DIALOG VIEW (REMINDER DIALOGS - SOURCE REMINDER NAME)

+Item Reminder Dialog Name                   Source Reminder            St
  29  IHS-ASTHMA ACTION PLAN 2015            IHS-ASTHMA ACTION PLAN 20 Li
  30  IHS-ASTHMA CONTROL 2011                IHS-ASTHMA CONTROL 2011   Di
  31  IHS-ASTHMA CONTROL 2013                IHS-ASTHMA CONTROL 2013   Li
  32  IHS-ASTHMA CONTROL 2015                IHS-ASTHMA CONTROL 2015   Li
  33  IHS-ASTHMA INTAKE 2011                 IHS-ASTHMA INTAKE 2011    Di
  34  IHS-ASTHMA INTAKE 2012                 IHS-ASTHMA INTAKE 2012    Li
  35  IHS-ASTHMA INTAKE 2013                 IHS-ASTHMA INTAKE 2013    Li
  36  IHS-ASTHMA PRIM PROV 2011              IHS-ASTHMA PRIM PROV 2011 Di
  37  IHS-ASTHMA PRIM PROV 2012              IHS-ASTHMA PRIM PROV 2012 Di
  38  IHS-ASTHMA PRIM PROV 2013              IHS-ASTHMA PRIM PROV 2013 Li
  39  IHS-ASTHMA PRIM PROV 2015              IHS-ASTHMA PRIM PROV 2015 Li
  40  IHS-ASTHMA RISK EXACERBATION 2011      IHS-ASTHMA RISK EXACERBAT Di
  41  IHS-ASTHMA RISK EXACERBATION 2013      IHS-ASTHMA RISK EXACERBAT Li
  42  IHS-ASTHMA RISK EXACERBATION 2015      IHS-ASTHMA RISK EXACERBAT Li
+         + Next Screen   - Prev Screen   ?? More Actions
AD   Add Reminder Dialog   PT   List/Print All      QU   Quit
CV   Change View           RN   Name/Print Name
Select Item: Next Screen//
```

Figure 4-11: Sample Dialog View

4. Select the **number** of the **item** to edit **IHS-SYPHILIS TEST-20221205** (Figure 4-12).



```
Dialog Edit List              Jan 10, 2023 13:51:33          Page:    1 of    1
REMINDER DIALOG NAME: IHS-SYPHILIS TEST-20221205
 Item  Seq.     Dialog Summary
   1    1   Group: GRP-IHS-SYPHILIS SCREEN-20221205

   2    1.10    Element: OI-IHS-SYPHILIS BY PROVIDER-20221205

   3    1.15    Element: OI-IHS-SYPHILIS BY POLICY (TIU AUTH)-20221205

   4    1.20    Element: CPT-IHS-SYPHILIS SCREEN ELSEWHERE (86592)-20221205

   5    1.25    Element: ED-IHS-STI TESTS-20221205

   6    1.30    Element: HD-IHS-SYPHILIS SCREEN REFUSED-20221205



          + Next Screen    - Prev Screen    ?? More Actions                >>>
CO    Copy Dialog             DO    Dialog Overview       QU    Quit
DD    Detailed Display        DT    Dialog Text
DP    Progress Note Text      ED    Edit/Delete Dialog
Select Item: Quit// ed   Edit/Delete Dialog
NAME: IHS-SYPHILIS TEST-20221205   Replace
```

Figure 4-12: Dialog Edit List window

5. Select the **dialog**. It will say **Disabled** instead of **Linked**.

6. Choose **ED (Edit/Delete Dialog)**. The second prompt (Figure 4-13) will state:

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

Figure 4-13: Disable prompt

7. Type the **at (@)** symbol to delete that text. The system then responds (Figure 4-14):

```
Are you sure you want to DELETE?  YES.
```

Figure 4-14: Delete prompt

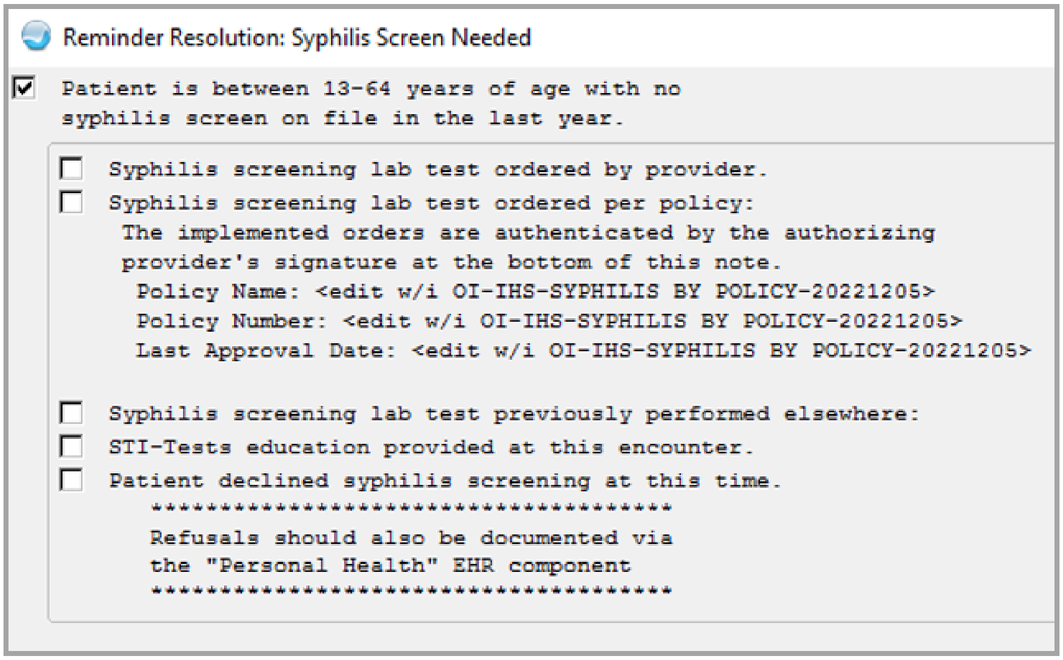
8. Press **Enter** to select **Yes**.

9. Type a **caret** (^) to quit editing.

5.0 The Dialog

5.1 The IHS-SYPHILIS TEST Dialog

The **IHS-SYPHILIS TEST** dialog (Figure 5-1) is new.



Reminder Resolution: Syphilis Screen Needed

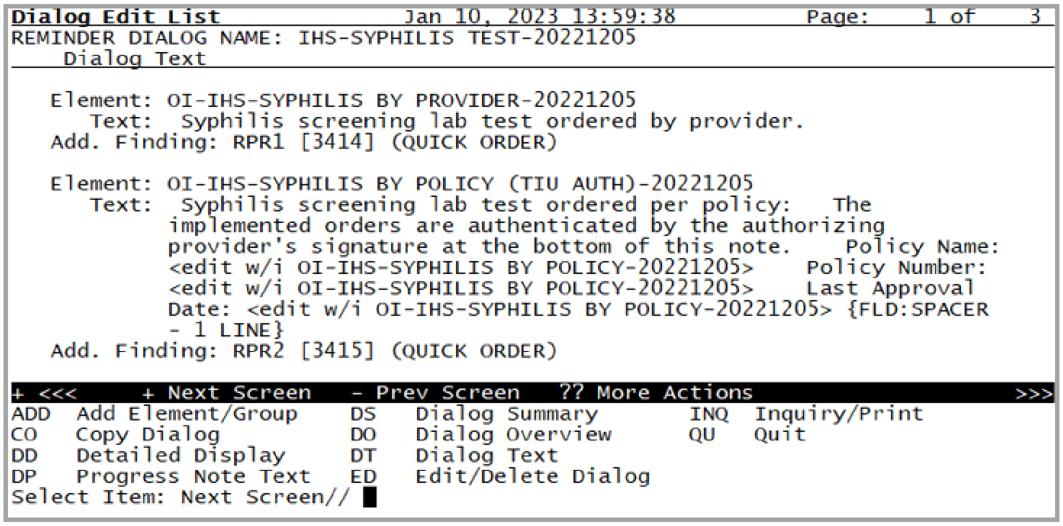
```
☑ Patient is between 13-64 years of age with no
  syphilis screen on file in the last year.

   □ Syphilis screening lab test ordered by provider.
   □ Syphilis screening lab test ordered per policy:
      The implemented orders are authenticated by the authorizing
      provider's signature at the bottom of this note.
       Policy Name: <edit w/i OI-IHS-SYPHILIS BY POLICY-20221205>
       Policy Number: <edit w/i OI-IHS-SYPHILIS BY POLICY-20221205>
       Last Approval Date: <edit w/i OI-IHS-SYPHILIS BY POLICY-20221205>

   □ Syphilis screening lab test previously performed elsewhere:
   □ STI-Tests education provided at this encounter.
   □ Patient declined syphilis screening at this time.
        **************************************
        Refusals should also be documented via
        the "Personal Health" EHR component
        **************************************
```

Figure 5-1: Entering in the IHS-Syphilis Test dialog

6.0 Update the Dialog with Local Policies

Find the following element in the dialog (Figure 6-1) to reflect your particular site's information:

Element: OI-IHS-SYPHILIS BY POLICY (TIU AUTH)-20221205



```
Dialog Edit List              Jan 10, 2023 13:59:38          Page:    1 of    3
REMINDER DIALOG NAME: IHS-SYPHILIS TEST-20221205
    Dialog Text

   Element: OI-IHS-SYPHILIS BY PROVIDER-20221205
      Text:  Syphilis screening lab test ordered by provider.
   Add. Finding: RPR1 [3414] (QUICK ORDER)

   Element: OI-IHS-SYPHILIS BY POLICY (TIU AUTH)-20221205
      Text:  Syphilis screening lab test ordered per policy:   The
            implemented orders are authenticated by the authorizing
            provider's signature at the bottom of this note.    Policy Name:
            <edit w/i OI-IHS-SYPHILIS BY POLICY-20221205>    Policy Number:
            <edit w/i OI-IHS-SYPHILIS BY POLICY-20221205>    Last Approval
            Date: <edit w/i OI-IHS-SYPHILIS BY POLICY-20221205> {FLD:SPACER
            - 1 LINE}
   Add. Finding: RPR2 [3415] (QUICK ORDER)

+ <<<      + Next Screen    - Prev Screen    ?? More Actions                 >>>
ADD  Add Element/Group     DS   Dialog Summary        INQ  Inquiry/Print
CO   Copy Dialog           DO   Dialog Overview       QU   Quit
DD   Detailed Display      DT   Dialog Text
DP   Progress Note Text    ED   Edit/Delete Dialog
Select Item: Next Screen//
```

Figure 6-1: Edit List dialog

1. 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 6-2) 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 6-2: Setting TIU TEMPLATE REMINDER DIALOGS

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

```
Display Sequence: 22//    22
Clinical Reminder Dialog: IHS-SYPHILIS TEST-20221205//
```

Figure 6-3: Display Sequence

6.1 Populate the Reminder Term with Local Syphilis Screening Lab Tests

1. From the **TRM Reminder Term Management** menu (Figure 6-4), find the term **IHS-SYPHILIS SCREENING LABS-20221205** and add the site's local labs related to syphilis testing.

```
Select Reminder Term: IHS-SYPHILIS SCREENING LABS-20221205       LOCAL
         ...OK? Yes//   (Yes)
NAME: IHS-SYPHILIS SCREENING LABS-20221205  Replace
SPONSOR: IHS Chief Clinical Consultant for Infectious Diseases
         //
REVIEW DATE: DEC 1,2025//

Reminder Term has no findings!

Select Finding: <<<< add all of your syphilis testing labs here.
Examples below;

LT RPR                                                 Finding #   1
LT RPR, QUANT.                                         Finding #   3
LT TREPONEMA PALLDIUM Abs                              Finding #   2
LT VDRL                                                Finding #   4
Select Finding:
```

Figure 6-4: TRM Reminder Term Management menu

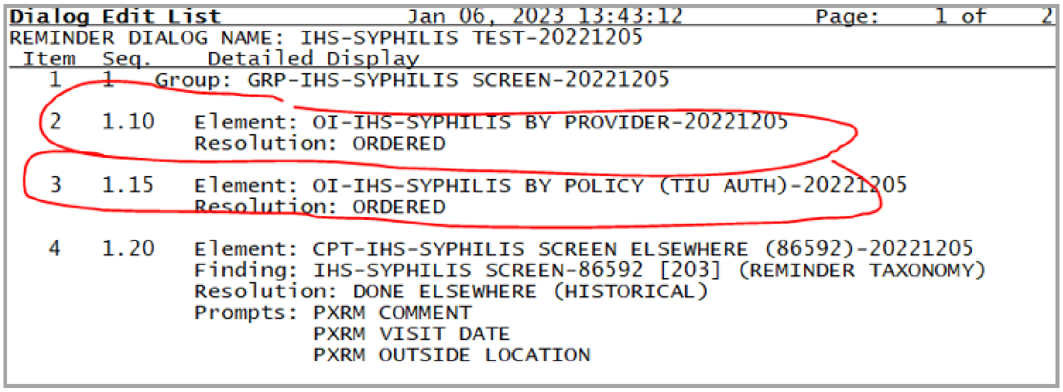
2. Identify or create the **Quick Orders** (Figure 6-5) for the preferred **Syphilis screening test(s)** above.

```
From the Enter/edit quick orders  [ORCM QUICK ORDERS]   (QO) menu in RPMS

Select Order Menu Management Option: QO  Enter/edit quick orders
Select QUICK ORDER NAME:  – examples below;
LRZ SYPHYLLIS
LRZ TREPONEMA PALLDIUM
```

Figure 6-5: Identify Quick Orders

3. Add the **Quick Order** to the dialog.

4. From the **Reminder Dialog Management** menu (Figure 6-6), find **ELEMENT OI-IHS-SYPHILIS BY PROVIDER** and **ELEMENT OI-IHS-SYPHILIS BY POLICY**. Add the **Syphilis Lab Quick Orders** to each of these elements as **FINDING ITEMS** and **ADDITIONAL FINDING ITEMS** if needed.



```
Dialog Edit List              Jan 06, 2023 13:43:12          Page:     1 of    2
REMINDER DIALOG NAME: IHS-SYPHILIS TEST-20221205
 Item  Seq.     Detailed Display
   1    1     Group: GRP-IHS-SYPHILIS SCREEN-20221205

   2   1.10     Element: OI-IHS-SYPHILIS BY PROVIDER-20221205
                Resolution: ORDERED

   3   1.15     Element: OI-IHS-SYPHILIS BY POLICY (TIU AUTH)-20221205
                Resolution: ORDERED

   4   1.20     Element: CPT-IHS-SYPHILIS SCREEN ELSEWHERE (86592)-20221205
                Finding: IHS-SYPHILIS SCREEN-86592 [203] (REMINDER TAXONOMY)
                Resolution: DONE ELSEWHERE (HISTORICAL)
                Prompts: PXRM COMMENT
                         PXRM VISIT DATE
                         PXRM OUTSIDE LOCATION
```

Figure 6-6: Reminder Dialog Management Menu

6.2 Add New Reminder to List

Use the **EHR** option of **Edit Cover Sheet Reminder List** (Figure 6-7) to add the new reminder of **Syphilis Screen Needed (IHS-SYPHILIS TEST-20221205)** to the visible list for users.

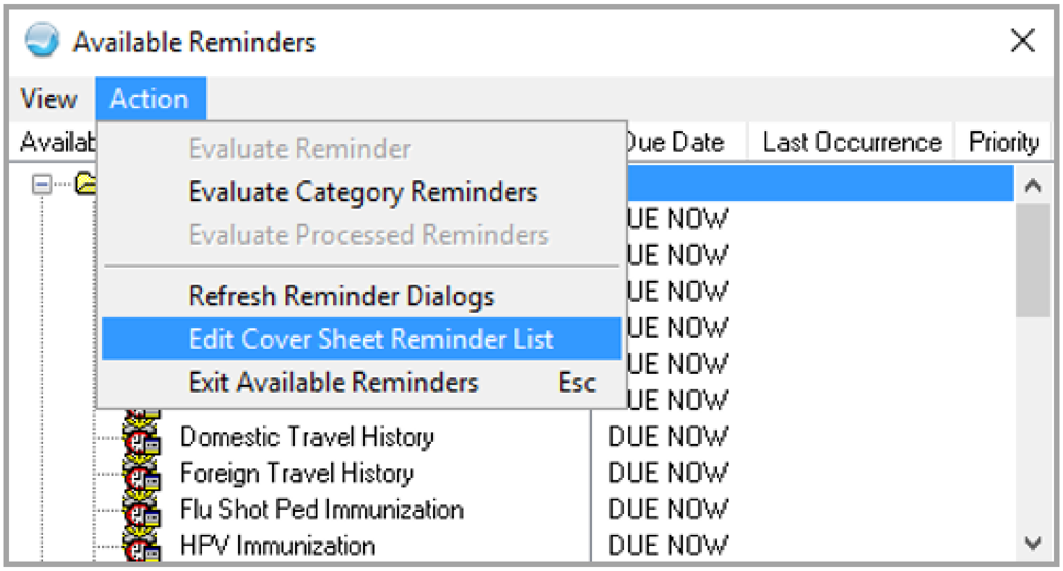

Available Reminders
View
Action
Availab
Evaluate Reminder
Evaluate Category Reminders
Evaluate Processed Reminders
Refresh Reminder Dialogs
Edit Cover Sheet Reminder List
Exit Available Reminders Esc
Due Date
Last Occurrence
Priority
UE NOW
UE NOW
UE NOW
UE NOW
UE NOW
UE NOW
Domestic Travel History DUE NOW
Foreign Travel History DUE NOW
Flu Shot Ped Immunization DUE NOW
HPV Immunization DUE NOW

Figure 6-7: Edit Cover Sheet Reminder List 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.1.1 Access

RPMS users shall:

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

RPMS users shall not:

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

A.1.2 Information Accessibility

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

RPMS users shall:

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

A.1.3 Accountability

RPMS users shall:

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

A.1.4 Confidentiality

RPMS users shall:

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

RPMS users shall not:

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

A.1.5 Integrity

RPMS users shall:

- Protect their systems against viruses and similar malicious programs.
- Observe all software license agreements.

- Follow industry standard procedures for maintaining and managing RPMS hardware, operating system software, application software, and/or database software and database tables.
- Comply with all copyright regulations and license agreements associated with RPMS software.

RPMS users shall not:

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

A.1.6 System Logon

RPMS users shall:

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

A.1.7 Passwords

RPMS users shall:

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

RPMS users shall not:

- Use common words found in any dictionary as a password.

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

A.1.8 Backups

RPMS users shall:

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

A.1.9 Reporting

RPMS users shall:

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

RPMS users shall not:

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

A.1.10 Session Timeouts

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

RPMS users shall:

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

A.1.11 Hardware

RPMS users shall:

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).
- Keep an inventory of all system equipment.
- Keep records of maintenance/repairs performed on system equipment.

RPMS users shall not

- Eat or drink near system equipment.

A.1.12 Awareness

RPMS users shall:

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

A.1.13 Remote Access

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

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

- Establish mechanisms to back up data created and/or stored at alternate work locations.

Remote RPMS users shall:

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

Remote RPMS users shall not:

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

A.2 RPMS Developers

RPMS developers shall:

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

RPMS developers shall not:

- Write any code that adversely impacts RPMS, such as backdoor access, “Easter eggs,” time bombs, or any other malicious code or make inappropriate comments within the code, manuals, or help frames.

- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

A.3 Privileged Users

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

Privileged RPMS users shall:

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government personnel and contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance.
- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to RPMS that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to RPMS.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the ISSO, Chief Information Security Officer (CISO), and systems owner.
- Protect the supervisor, superuser, or system administrator passwords.
- Avoid instances where the same individual has responsibility for several functions (i.e., transaction entry and transaction approval).
- Watch for unscheduled, unusual, and unauthorized programs.
- Help train system users on the appropriate use and security of the system.

- Establish protective controls to ensure the accountability, integrity, confidentiality, and availability of the system.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible from the time that the user is no longer authorized system. Passwords forgotten by their owner should be replaced, not reissued.
- Terminate user accounts when a user transfers or has been terminated. If the user has authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel logon IDs and passwords and delete or reassign related active and backup files.
- Use a suspend program to prevent an unauthorized user from logging on with the current user's ID if the system is left on and unattended.
- Verify the identity of the user when resetting passwords. This can be done either in person or having the user answer a question that can be compared to one in the administrator’s database.
- Shall follow industry best standards for systems they are assigned to and abide by all Department and Agency policies and procedures.

Privileged RPMS users shall not:

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

Acronym List

Acronym	Term Meaning
CAC	Clinical Application Coordinator
IHS	Indian Health Service
IA	Install All
IS	Install Selected
IRM	Information Resources Management
RPMS	Resource and Patient Management System

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