

RESOURCE AND PATIENT MANAGEMENT SYSTEM

Clinical Reminders

(PXRM)

COVID Reminder Supplemental User Guide

Version 2.0 Patch 2001 December 2021

Office of Information Technology Division of Information Technology

Table of Contents

1.0	Introdu	ction	1
	1.1	Clinical Reminders Resources	. 1
2.0	COVID	19 Reminder and Dialogs	2
	2.1 2.2	Updated COVID Immunization Dialog Prerequisites	
3.0	Install t	the KIDS Build	3
4.0	Installi	ng the Reminders/Dialogs	4
	4.1 4.2 4.3 4.4 4.5 4.5.1	Installing the Item from Exchange Installing Dialog – Part 1 Install Dialog – Part 2 Taxonomy Error Activate the Dialog Reminder Dialog Management (DLG)	5 8 9 9
5.0	The Dia	alogs	12
	5.1 5.2	The Adult Immunization Dialog The Pediatric Vaccine Dialog	12
6.0	Update	the TIU Templates	16
	6.1	Activate Note Title	
	6.2	Attaching the Dialog to a TIU Note Title	18
Apper	ndix A	Rules of Behavior	21
	A.1	All RPMS Users	
	A.2 A.2.1	Access Information Accessibility	
	A.2.1 A.2.2	Accountability	
	A.2.3	Confidentiality	
	A.2.4	Integrity	23
	A.2.5	System Logon	
	A.2.6	Passwords	
	A.2.7 A.2.8	Backups Reporting	
	A.2.0		
	-	Hardware	
		Awareness	
		Remote Access	
		RPMS Developers	
		Privileged Users	
Acron	ym List		30

ntact Information

Preface

This documentation applies to those reminders distributed in Version 2.0, Patch 2001 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 PXRM v2.0 2001 patches. We strongly recommend reviewing this entire document before installing and setting up the Clinical Reminders Version 2.0 Patch 2001.

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 (PXRM) section.

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

2.0 COVID-19 Reminder and Dialogs

This section provides an overview of the major changes in the Clinical Reminders patch 2001.

2.1 Updated COVID Immunization Dialog

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

The updated dialog is listed below and will replace the existing one.

IHS-IMMUNIZATION COVID POLICY ORDERS-202112

All thee (3) immunizations Moderna, Pfizer, and Janssen are included.

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 Section 6.0 in this document.

The changes in this patch include:

- 1. Making changes to the checklist.
- 2. Adding additional doses of COVID-19 vaccinations for the Pfizer tris-sucrose formulation.
- 3. Allowing users to historically enter previous COVID-19 immunizations done at outside sites.
- 4. A new dialog for pediatric doses of Pfizer vaccine.

Please see the Supplemental User Guide for patches 1010, 1011, 1012, and 1013 for further information.

2.2 Prerequisites

- ACPT*2.21*10
- PXRM*2.0*1013

3.0 Install the KIDS Build

Installation of **PXRM 2001** should be done by the appropriate IRM personnel using the instructions in the patch notes. Users may be on the system.

Installation of **Patch 2001** will put the reminder into the **REMINDER EXCHANGE** file.

Note: It does *not* install them.

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

4.0 Installing the Reminders/Dialogs

Follow these instructions to install the two (2) items 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.

ile <u>E</u> d	al Reminder Exchange	Nov 22,	2021 1	1.20.20	Page:	1 of	1
	ge File Entries.	NOV 22,	2021 1	1:30:30	Page:	1 01	
Cinam	ge file indites.						
tem	Entry		Sourc	2	Date	Packed	
1	IHS-IMMUNIZATION COVID ORDERS-202112	POLICY	USER@	DEMO HOSPITA	11/22	/2021@1	4:29
2	IHS-PED COVID IMMUNIZAT	ION	USER@	DEMO HOSPITA	11/22	/2021@1	4:3
	+ Next Screen - Pr			More Actions			>>:
	reate Exchange File Entr		LHF	Load Host Fil			>>:
F C	reate Exchange File Entr reate Host File		LHF LMM	Load Host Fil Load MailMan	Message		>>:
F C M C	reate Exchange File Entr reate Host File reate MailMan Message	Y	LHF LMM LR	Load Host Fil Load MailMan I List Reminder	- Message Definition	15	>>
F C: M C: E D	reate Exchange File Entr reate Host File	У	LHF LMM LR LWH	Load Host Fil Load MailMan	Message Definition File		>>:

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 2001 there are two (2):

IHS-IMMUNIZATION COVID POLICY ORDERS-202112

IHS-PED COVID IMMUNIZATION

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

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.

🛛 Ca	che TRM:10648 (ENSEMBLE)						
ile	<u>E</u> dit <u>H</u> elp						
lini	cal Reminder Exchange	Nov 22,	2021 14:30	:30	Page:	1 of	1
cha	nge File Entries.						
tem			Source			e Packed	
1	. IHS-IMMUNIZATION COVI ORDERS-202112	D POLICY	USER@DEMC	HOSPITA	11/:	22/20210	14:29
2	IHS-PED COVID IMMUNIZ	ATION	USER@DEMC	HOSPITA	11/3	22/2021@	14:3
	+ Next Screen -	Pret Scre	en 22 Mor	e Actions			~~~
Ē	+ Next Screen - Create Exchange File En				e		>>:
	+ Next Screen - Create Exchange File En Create Host File		LHF Loa	d Host Fil			>>:
IF	Create Exchange File En		LHF Loa LMM Loa		Message	ons	>>:
IF M	Create Exchange File En Create Host File	try	LHF Loa LMM Loa	d Host Fil d MailMan t Reminder	Message Definiti	ons	>>:
IF IM TE	Create Exchange File En Create Host File Create MailMan Message	try try	LHF Loa LMM Loa LR Lis LWH Loa	d Host Fil d MailMan t Reminder	Message Definiti File		>>:
IF IM TE TE I	Create Exchange File En Create Host File Create MailMan Message Delete Exchange File En Install Exchange File E Installation History	try try ntry	LHF Loa LMM Loa LR Lis LWH Loa RI Ren	d Host Fil d MailMan t Reminder d Web Host dinder Defi	Message Definiti File		>>:
IF M TE I I elec	Create Exchange File En Create Host File Create MailMan Message Delete Exchange File En Install Exchange File E	try try ntry Install E	LHF Loa LMM Loa LR Lis LWH Loa RI Rem xchange Fil	d Host Fil d MailMan t Reminder d Web Host dinder Defi	Message Definiti File		>>:

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.

Note: The adult reminder/dialog – **IHS-IMMUNIZATION COVID POLICY ORDERS-202112** will take a LONG time to load due to the many immunizations included in it.

	<u>E</u> dit <u>H</u>			
xcha	nge r	ile Components Nov 18, 2021 15:43:27	7 Page:	6 of 9
-	Comp	onent	Category	Exists
11	IHS-	COVID DOSES		Х
12	COVI	D VACCINE NAME		Х
13	IHS	YES/NO/DON'T KNOW		Х
14	IHS	YES/NO/DON'T KNOW DEF NO		Х
15	GEN	WORD INDENT 2		Х
16	GEN	YES/NO RADIO		Х
17	DATE	AND TIME V1		Х
18	IHS	COVID19IMM POLICY DATE		Х
19	IHS	COVID19IMM POLICY ID		Х
20	IHS	COVID19IMM POLICY NAME		Х
21		WORD PROCESSING INDENT 2		Х
22		COVID19IMM CONSENT		Х
23		TEXT BOX		Х
24		COVID 19IMM LOCATION		Х
25		COVID19IMM SITE NAME		Х
26	IHS	COVID19IMM FORM NUMBER		Х
		+ Next Screen - Prev Screen ?? More A		>>>
A :	Insta	ll all Components IS Instal ion: Next Screen//	Il Selected Compone:	nt

Figure 4-4: Exchange entry

- Notice that for each item in the reminder, an X (S) 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 several TIU template fields (Figure 4-5) in this dialog. Most of them were installed in earlier versions of this dialog. Take the default and install them.

```
TIU TEMPLATE FIELD entry IHS COVID19IMM CONSENT 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 4-5: TIU Template Fields

Supplemental User Guide December 2021

2. There are also some **new taxonomies** to be installed. Most of the taxonomies will ask you to overwrite. Take the default.

```
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 4-6: Installing Taxonomies

3. Make sure that the **quick order** exists. If you forgot to create the quick order, you will see the following (Figure 4-7):

```
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 4-7: 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.
- You need thee (3) quick orders

```
1 ORZ POLICY COVID_19 JOHNSON&JOHNSON IMMUNIZATION
2 ORZ POLICY COVID_19 MODERNA IMMUNIZATION
3 ORZ POLICY COVID_19 PFIZER IMMUNIZATION
```

Figure 4-8: Quick Orders

Review the Moderna quick order you made to check for dosage data.

You may need to remove it or make an additional quick order.

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:

```
DDDialog DetailsDTDialog TextISInstall SelectedDFDialog FindingsDUDialog UsageQUQuitDSDialog SummaryIAInstall All
```

Figure 4-9: 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 4-10). If they are identical, it will not update the item on your database.

Cach	e TRM:3004 (ENSEMBLE)		_	□ ×
<u>F</u> ile <u>E</u> d	lit <u>H</u> elp			
		Nov 18, 2021 15:47:30	Page: 3	of 8
acked	reminder dialog:	IHS-PED COVID IMMUNIZATION		
-Item	Seg. Dialog Findi	0.00	Type	Exists
1 ocm	Finding: *NO		1 1 1 2	LAISUS
17		IMM COVID19 (PFIZER - PEDS) 1ST	element	x
	DOSE	,		
	Finding: CPT	IMM COVID19 (PFIZER- PEDS) (REMINDE	R TAXONOMY)	х
18	10.30.20.15 GRP I	M COVID-19 2ND DOSE (PFIZER - PEDS)	group	Х
	Finding: *NO			
19		IM COVID-19 PFIZER - PEDS SECOND	group	х
	DOSE			
20	Finding: *NO		- 1	v
20	10.30.20.15.3.2 H Finding: *NO		element	х
21		HS-COVID IMM PFIZER - PEDS DONE	element	x
	ELSEWHERE		CICINCIIO	
	Finding: COV	ID-19, mRNA, LNP-S, PF, 10 mcg/0.2 m	L dose,	х
	tris-sucrose	(IMMUNIZATION)		
	+ Next Screen	- Prev Screen ?? More Actions		
		DT Dialog Text IS Ins		≥d
		DU Dialog Usage QU Qui	t	
		IA Install All		
elect	Action: Next Scre	en//		

Figure 4-10: 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 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 4-11). 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 ...
      Reminder Term Management ...
TRM
TST
    Reminder Test
```

Figure 4-11: 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 4-12) from the **Reminder Configuration** menu.

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

Figure 4-12: Reminder Dialog Management

2. Use the **DLG** option to access the options on the **Reminder Dialog Management** menu (Figure 4-13).

Dialog	g List	Apr 15,	2015 07:30:59		Page:	3 01
REMINI	DER VIEW (ALL REMIND	ERS BY NAME)				
Item	Reminder Name		Linked Dial	log Name	& Dialog	State
29	IHS-ASBI SCREENING	2013	IHS-ASBI SC	CREENING	2013	
30	IHS-ASTHMA ACTION P	LAN 2009				
31	IHS-ASTHMA ACTION P	LAN 2011	IHS-ASTHMA	ACTION	PLAN 2011	Di
32	IHS-ASTHMA ACTION P	LAN 2012	IHS-ASTHMA	ACTION	PLAN 2012	Di
33	IHS-ASTHMA ACTION P	LAN 2013	IHS-ASTHMA	ACTION	PLAN 2013	
34	IHS-ASTHMA ACTION P	LAN 2015	IHS-ASTHMA	ACTION	PLAN 2015	
35	IHS-ASTHMA CONTROL :					
36	IHS-ASTHMA CONTROL :	2011 2013	IHS-ASTHMA	CONTROL	2011	Di:
37	IHS-ASTHMA CONTROL :	2013	IHS-ASTHMA	CONTROL	2013	
38	IHS-ASTHMA CONTROL :		IHS-ASTHMA	CONTROL	2015	
39	IHS-ASTHMA INTAKE 2	011	IHS-ASTHMA	INTAKE	2011	Di
40	IHS-ASTHMA INTAKE 2	012	IHS-ASTHMA	INTAKE	2012	
41	IHS-ASTHMA INTAKE 2	013	IHS-ASTHMA	INTAKE	2013	
42	IHS-ASTHMA PLAN					
	+ Next Screen	- Prev Scree	en ?? More Ad	ctions		
AR /	All reminders	LR Linked	Reminders	QU Qu	it	
V (Change View	RN Name/P	rint Name			

Figure 4-13: Sample Reminder View

3. Choose CV, and then choose D for dialogs (Figure 4-14).

Ele Edit (<u>C</u> onnect <u>H</u> elp										
Dialo	g List			Ap	: 15, 20	015 07	:31:45	P	age:	3	C
DIALO	G VIEW (REM	INDER	DIAL	OGS - S	SOURCE I	REMINDE	ER NAME)				
+Item	Reminder D:	ialog	Name				Source Rem	inder			2
29	IHS-ASTHMA	ACTIC	ON PL	AN 201	5		IHS-ASTHMA	ACTIC	N PLA	AN 20	I
30	IHS-ASTHMA	CONTR	ROL 2	011			IHS-ASTHMA	CONTR	OL 20)11	Ι
31	IHS-ASTHMA	CONTR	ROL 2	013			IHS-ASTHMA	CONTR	OL 20)13	I
32	IHS-ASTHMA	CONTI	ROL 2	015			IHS-ASTHMA	CONTR	OL 20)15	1
33	IHS-ASTHMA	INTAR	KE 20	11			IHS-ASTHMA	INTAK	E 201	1	Ι
34	IHS-ASTHMA	INTA	KE 20	12			IHS-ASTHMA	INTAK	E 201	.2]
35	IHS-ASTHMA	INTAR	KE 20	13			IHS-ASTHMA	INTAK	E 201	.3	1
36	IHS-ASTHMA	PRIM	PROV	2011			IHS-ASTHMA	PRIM	PROV	2011	I
37	IHS-ASTHMA	PRIM	PROV	2012			IHS-ASTHMA	PRIM	PROV	2012	Ι
38	IHS-ASTHMA	PRIM	PROV	2013			IHS-ASTHMA	PRIM	PROV	2013	1
39	IHS-ASTHMA	PRIM	PROV	2015			IHS-ASTHMA	PRIM	PROV	2015	1
40	IHS-ASTHMA	RISK	EXAC	ERBATI	ON 2011		IHS-ASTHMA	RISK	EXACE	CRBAT	Ι
41	IHS-ASTHMA	RISK	EXAC	ERBATIC	ON 2013		IHS-ASTHMA	RISK	EXACE	RBAT	1
42	IHS-ASTHMA	RISK	EXAC	ERBATIC	ON 2015		IHS-ASTHMA	RISK	EXACE	CRBAT	I
+	+ Next	Scree	∋n	- Prev	Screen	?? 1	More Action	3			
AD	Add Reminde:	r Dial	Log	PT L:	ist/Prim	nt All	QU	Quit			
CV	Change View			RN Na	ame/Prim	nt Name	e				
Selec	t Item: Next	t Scre	een//								

Figure 4-14: Sample Dialog View

 Select the number of the item you want to edit IHS-PED COVID IMMUNIZATION or IHS-IMMUNIZATION COVID POLICY ORDERS 202112 (Figure 4-15).

🛄 C	ach	e TRM:8844 (ENSEMB	LE)					_		\times
<u>F</u> ile	Ec	lit <u>H</u> elp								
		Edit List							11	^
		ER DIALOG NAME:		NIZATION CO	VID POLICY	ORDE	RS-202108	(Disab	led)	
		Seq. Dialog								
1		5 Element: F	ID IHS COV	ID IMMUNIZA	TION ORDER	HEAD	ER			
2		30 Group: GRE	P IHS COVI	D-19 IMMUNI	ZATION					
3	3	30.10 Element	: IM SCRE	ENING CHECK	LIST COVID	-08/1	8/21			
4		30.20 Element	: IM SCRE	ENING DATE	8/20/2021					
5	5	30.30 Group:	GRP IHS C	OVID-19 IMM	UNIZATION (COVID	-19			
6	5	30.30.20 Grou	ap: GRP IM	COVID-19 P	FIZER					
7		30.30.20.10	Group: GRP	IM COVID-1	9 1ST DOSE	(PFI	ZER)			
8	3	30.30.20.10.5	Element	: IM COVIDI	9 (PFIZER)	1ST	DOSE DONE			
+		+ Next Scre								>>>
ADD		dd Element/Grou						Print		
co		opy Dialog			rview	QŬ	Quit			
		etailed Display								
		rogress Note Te Item: Next Sci		Edit/Delet	e Dialog					
Dete		TOCHT. NEXT DOI	centry							

Figure 4-15: 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 (a) 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 The Dialogs

5.1 The Adult Immunization Dialog

The check list was changed due to the CDC, and it is the same for all vaccines. It has been updated per CDC requirements as of November 16, 2021.

There are several questions which are now required fields:

Have you ever received a dose of COVID-19 vaccine, how many doses have you received, and did you bring your vaccination card or other documentation?

```
🥑 Reminder Dialog Template: Updated Covid test
                                                                                       \times
  Pre-vaccination Checklist for COVID-19 Vaccines
                                                                                                 ^

    Are you feeling sick today?

          C Yes @ No C Don't Know

    Have you ever received a dose of COVID-19 vaccine?
    *C Yes C No C Don't Know

           If yes, which product?
          🏳 Pfizer 🗌 Moderna 🗖 Janssen 🗍 Another Product
          How many doses of COVID-19 vaccine have you received?
          *0
                 l ≑ I
          Did you bring your vaccination record card or other
          documentation?
           *C Yes C No
        3. Check all that apply:
          [ ] I live in a long-term care setting
           [] I have been diagnosed with a medical condition(s).
                Please list:
          [] I am a first responder.
           [ ] I work in a long-term care facility, correctional
                facility, hospital, restaurant, retail setting,
                school, or other setting with high exposure
                to the public.
        4. Do you have a health condition or are you undergoing
           treatment that makes you moderately or severely
          immunocompromised? (This would include treatment for cancer
          or HIV, receipt of organ transplant, immunosuppressive
           therapy or high-dose corticosteroids, CAR-T-cell therapy,
          hematocrit therapy [HCT], DiGeorge syndrome
                                                                              * Indicates a Bequired Field
Pre-vaccination Checklist for COVID-19 Vaccines
                                                                                                 ^
 1. Are you feeling sick today?
    No
 2. Have you ever received a dose of COVID-19 vaccine?
    If yes, which product?
                         ****
```

Figure 5-1: Immunization Dialog

Supplemental User Guide December 2021

Immunizations are now grouped together so they can more easily be selected and used. The additional doses have been added.

Patie	nt Criteria:
	nt meets requirement for COVID-19 immunization per CDC and ACIP mendations/guidelines.
recom	mendacions/guidelines.
	ous Covid-19 Immunizations: No Covid Immunization Found
	-19 Immunizations ZER Covid-19 Immunization Documentation
	COVID-19 immunization (Pfizer) - 1st Dose
	WVID-19 immunization (Pfizer) - 2nd Dose
	20VID-19 immunization (Pfizer) - Additional Dose for Immunocompromised Deople
	2071D-19 immunization (Pfizer) - Booster Dose
-	
	ZER (tris-sucrose) Covid-19 Immunization Documentation
	20VID-19 immunization (Pfizer tris-sucrose) - 1st Dose
	COVID-19 immunization (Pfizer tris-sucrose) - 2nd Dose
	XVID-19 immunization (Pfizer tris-sucrose) - Additional Dose for mmunocompromised people
	XVID-19 immunization (Pfizer tris-sucrose) - Booster Dose
O MOD	DERNA Covid-19 Immunization Documentation
C c	OVID-19 immunization (Moderna) - 1st Dose
	OVID-19 immunization (Moderna) - 2nd Dose
	OVID-19 immunization (Moderna) - Additional Dose for Immunocompromised
_	eople XVID-19 immunization (Moderna) - Booster Dose
· · ·	OVID-19 Immunization (noderna) - Booster bose
C Jan	issen Covid-19 Immunization Documentation
C c	:OVID-19 immunization (Johnson & Johnson) - 1st Dose
C c	20VID-19 immunization (Johnson & Johnson) Booster Dose
C Pat	ient refused Covid-19 immunization at this visit.
	Patient Education
	* Indicates a R
cinat:	ion Checklist for COVID-19 Vaccines
e you	feeling sick today?
	u ever received a dose of COVID-19 vaccine?
yes,	which product?

Figure 5-2: Immunization dialog part 2

The ability to document outside previous doses has been added for the vaccines. For the additional doses prompt, there is the ability to enter two (2) previous doses.

minu				\rightarrow
	ler Dialog Template: Updated Covid test			
Pre COVI COVI	evious Covid-19 Immunizations: ID,Mod : Aug 25, 2021 ID,Mod : Feb 09, 2021 VID-19 Immunizations PFIZER Covid-19 Immunization Documentation			
c c				
	✓ Previous dose data: □ Vaccine given locally Latest Covid-19 immunization: Last COVID,Mod: Aug 25, 2021 ✓ Document outside Pfizer Covid-19 Immunizations			
	 Patient indicates that Pfizer Covid immunization was received at another facility. Patient indicates that Pfizer Covid immunization was received at another facility. 			
	\Box Was there a unexpected reaction to the second dose? C $_{\rm Yes}$ C $_{\rm No}$			
	□ Was there a unexpected reaction to the second dose? C Yes C No □ Patient received COVID-19 immunization at this visit. □ Adminstration Time: 22			
0	Patient received COVID-19 immunization at this visit.			
C	Patient received COVID-19 immunization at this visit. Adminstration Time: MODERNA Covid-19 Immunization Documentation COVID-19 immunization (Moderna) - 1st Dose COVID-19 immunization (Moderna) - 2nd Dose	* Indicates (a Require	ed F
C C	Patient received COVID-19 immunization at this visit. Adminstration Time: MODERNA Covid-19 Immunization Documentation COVID-19 immunization (Moderna) - 1st Dose COVID-19 immunization (Moderna) - 2nd Dose	* Indicates (a Require	ed F
	Patient received COVID-19 immunization at this visit. Adminstration Time: MODERNA Covid-19 Immunization Documentation COVID-19 immunization (Moderna) - 1st Dose COVID-19 immunization (Moderna) - 2nd Dose	* Indicates (a Require	ed F
C	Patient received COVID-19 immunization at this visit. Adminstration Time: MODERNA Covid-19 Immunization Documentation COVID-19 immunization (Moderna) - 1st Dose COVID-19 immunization (Moderna) - 2nd Dose L FORM NUMBER TO TIU TEMPLATE FIELD "IHS COVID19IMM FORM NUMBER"]	* Indicates -	a Require	ed F

Figure 5-3: Entering outside immunizations

5.2 The Pediatric Vaccine Dialog

The pediatric dialog is very similar to the adult dialog. The first part of it is identical to the adult dialog along with the same questionnaire. The difference is that of the vaccines to select. At the present time, only Pfizer is available, and it is the pediatric vaccine and CPT codes that are added.

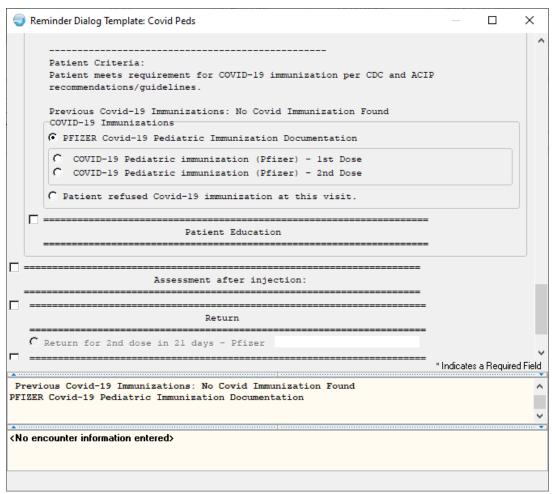


Figure 5-4: Entering pediatric COVID-19 immunizations

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 or 1011 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.

Template Field Editor						×
Action			Delete	Сору		New
Template Fields IHS COVID19IMM POLICY DATE Display Tex	Name:	THE COVIDIBINE POLICY DATE				
IHS COVID 19 IF 2ND DOSE IHS COVID 19 IF 2ND DOSE IHS COVID 19 MANUFACTURER IHS COVID 19 RTC IHS COVID 19 RTC IHS COVID 19 IMM FORM NUMBER Display	Type: Items:	Text (ADD LOCAL POLICY APPROVAL DATE TO TIU TEMPLATE FIELD "IHS	Field Len COVID191MM	A standard and	Text Len: DATE"]	^
IHS COVID19IMM POLICY ID Display" IHS COVID19IMM POLICY NAME Display IHS COVID19IMM STIE NAME Display IHS CRAFFT B1 YN Radio B IHS CRAFFT EXCLUSION Display IHS CRAFFT EXCLUSION 2 Display IHS CRAFFT INTERVIEW Display IHS CRAFFT PARTA RESPONSE Display	Line: 2 Col: 1					~
IHS CRAFFT SCORE Dipplay" IHS DATE LAST USED Check B IHS DAYS/WEEKS/MONTHS Combo E IHS DEPO CONTRA LIST * Check E IHS DEPO DISCONTINUE Radio B IHS DEPO DISCONTINUE Batton IHS DEPO START CONTINUE Button IHS DEPO START CONTINUE Button IHS DEPO START CONTINUE Button	LM Text Miscel Inac	re Separate Lines Indent Field:				>
IHS DIAS SENSATION HIS DIAS SENSATION HIS DIRECTIONS GENERAL COMMENTS HIS DISCUSSION Edd Box HIS DM DURRICULUM LIS DM DEMONSTRATED Combo E	Notes:					`
Hide Inactive Fields Indicates a Required Fiel	1	Preview	OK	Cancel		Apply

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 s	election: 5	System	DEMO.MEDSPHERE.COM
Set	ting TIU TEM	PLATE REMI	NDER 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</td>

      4
      COVID-19 VACCINE POLICY ORDER
      TL
      <<This may need to be made ACTIVE</td>
```

```
Figure 6-5: Activate Note Title
```

To have a separate Note Title for the **IHS-PED COVID IMMUNIZATION**, add a new Title under (TL) the document class of CLINICAL REMINDER DIALOG IMMUNIZATIONS document class (DC) (for example, it is named **PEDS-COVID DIALOG** below however, you can name it **IHS-PED COVID IMMUNIZATION**).

Create Document Definitions	Dec 07, 2021 11:42:32 BASICS	Page:	1 of	1
+ Name 2 PROGRESS NOTES 3 CLINICAL REMINDER 4 COVID-19 VACCIN 5 — PEDS-COVID-DIAL				Type CL DC TL TL

Figure 6-6: New Title

To enable the post-signature code function to the IHS-PEDS COVID dialog, which will enter the ICD-10 code of Z23 after the dialog is signed in EHR, after you make the note title, keep it inactive. Navigate to the TL of COVID-19 VACCINE POLICY ORDER's Technical Fields and copy the Post-signature Code:

D EN^BTIUIMSN(DFN,TIUDA,713404003,3289271014,"Z23."). And paste the code into the Technical Fields of the new title PEDS-COVID DIALOG TEST or **IHS-PED COVID IMMUNIZATION or what you chose to call it. Then be sure to activate the new Title (TL).**

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 6-7).
 - d. In the **Reminder Dialog**, find the reminder dialog **COVID-19 VACCINE POLICY ORDER or IHS-PED COVID IMMUNIZATION** in the dropdown list.
 - e. Select the Associated Title (note title) COVID-19 VACCINE POLICY ORDER or IHS-PED COVID IMMUNIZATION. 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.

Template Editor			— 🗆 X
Edit Action Tools			New Template
Shared Templates		Personal Templates	Shared Template Properties
Shared Templates Document Titles COVID-19 VACCINE POLICY ORDER CHART REVIEW CHART REVIEW	< >	Copy	Template Type: Image: State Provided Training Perminder Dialog Image: State Provided Training Dialog Properties Image: State Provided Training Image: Hide Items in Templates Display Only Image: Drawer Image: Drawer Image: Exclude from Group Boilerplate One Item Only Image: Hide Dialog Items Image: Drawer
Hide Inactive	👚 🖶 Delete 🗙	🗹 Hide Inactive 🔺 🕂 Delete 🗡	■ Number of Blank Lines Lock
Associated Title: COVID-19 VACCINE POLICY ORDER			•
Edit Shared Templates	Show Templa	te Notes	OK Cancel Apply

Figure 6-7: Template Editor for Reminder Dialogs

3. Users may also want to attach this template to a **Note Title** or to a **Quick Note** (Figure 6-8).

Create a New Quick Note	
Quick Note Name:	
COVID IMMUNIZATION	
Type of Quick Note: O Personal Public	

Figure 6-8: Quick Note Creator

- 4. Use the **TIU title** in **patch 1023**, and the **dialog** (Figure 6-9) in this **reminders patch**.
- 5. Please do *NOT* check the boilerplate box when you are using a template.

Quick Note Properties				
COVID IMMUNIZATION				
NoteTitle:				
COVID-19 VACCINE POLICY	ORDER ~			
Include Boilerplate T	ext			
Template:				
COVID 19 IMMUNIZATION	~			
Prompt for Visit:	Select Visit Category:			
🔲 Use Visit Dialog	Ambulatory ~			
Set Visit Context	Visit Location:			
Use current user for				
visit provider	Visit Provider:			
Save Cancel				

Figure 6-9: 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: <u>https://home.ihs.gov/security/index.cfm</u>

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
CAC	Clinical Application Coordinator
EHR	Electronic Health Record
HIPAA	Health Insurance Portability and Accountability Act
ID	Identification
IHS	Indian Health Service
IRM	Information Resources Management
ISSO	Information System Security Officer
PC	Personal Computer
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: <u>https://www.ihs.gov/itsupport/</u>
- Email: itsupport@ihs.gov