RESOURCE AND PATIENT MANAGEMENT SYSTEM

Electronic Health Record

(EHR)

Immunization Component (IMM) Addendum to User Manual

Version 1.1 Patch 29
September 2020

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

The Indian Health Service (IHS) Immunization component (IMM) in the Resource and Patient Management (RPMS) Electronic Health Record (EHR) has been redeveloped to meet criteria for the 2015 Edition certification.

1.0 Introduction

The new IMM component permits users to view the patient's immunization history and forecast as recorded in the state Immunization Information System (IIS), assuming the site has established a connection to the state. IMM allows users to view the state IIS information on demand, or to suppress this information if desired. Most of the features of the existing EHR Immunization component have been retained and are unchanged.

Please read all the documentation for EHR v1.1 patch 29 and associated patches. Documentation can be found at:

- RPMS Clinical Applications website: https://www.ihs.gov/rpms/applications/clinical/
- RPMS Trainings/Recordings: https://ihs.cosocloud.com/rpms-tr/event/event_info.html

> **Note**: If directed to enter a Username and Password, click **OK** to proceed to the Training Repository page.

- RPMS Training Course Materials: https://www.ihs.gov/rpms/training/course-materials/
- RPMS EHR online help can be located within the RPMS EHR

RPMS may be set up to exchange immunization data with more than one state. To use the state Forecast, sites must first establish a connection to their state's Immunization Registry.

New parameters that must be set up are discussed in the RPMS Immunization Data Exchange (BYIM) package training set up. The BYIM training and documents are separate from this document and include the following:

- Manage parameters that control state communications
- Manage the automatic trigger of queries to the state immunization information systems

Immunization coordinators and site managers can set these up. If your site has not set these up, or has issues, please have your Immunizations Coordinator or site manager contact your area for assistance.

2.0 Immunization Component

The new IMM component is released in conjunction with background features enabling RPMS to query the state IIS, retrieve and store IIS history and forecast data, making it available for any RPMS application. Potential settings for this capability may include:

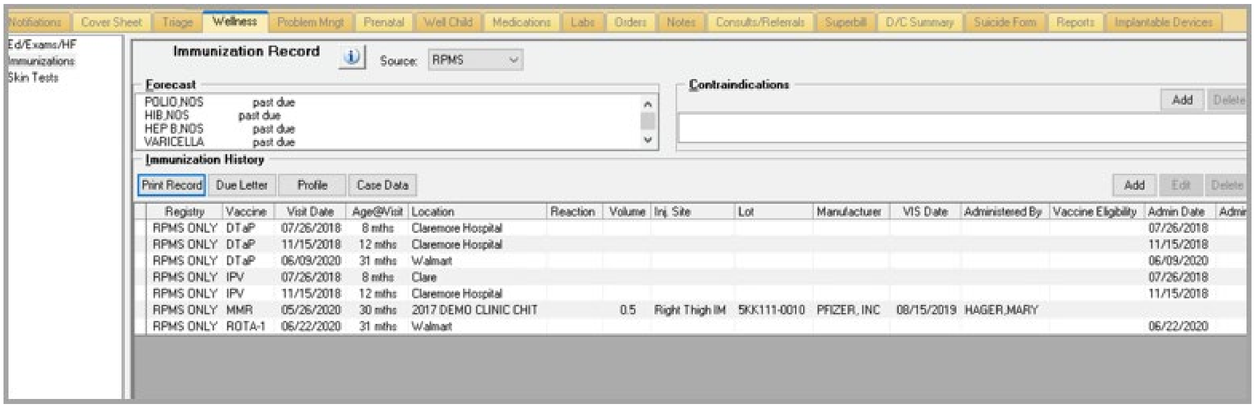
- Querying the state IIS for all patients with an upcoming (e.g., same day) appointment
- Querying the state IIS for a single patient upon check-in to a clinic
- Querying the state IIS for a single patient on demand by the nurse or provider

By comparing the local facility's immunization record and forecast with that from the state, users will have a more complete picture of the patient's immunization history, discover immunizations done elsewhere that should be added to the local record, and minimize the risk of over-immunization.

The Immunization component may be placed anywhere in the EHR. Typically, it would be co-located with other wellness-related components, such as Patient Education and Skin Tests.

2.1 Opening Window

The opening screen is similar to the legacy Immunization screen. Its functionality has not changed, except for the **Source** button, which displays additional state forecasts if the site has established a connection with the state IIS. This is discussed in the Section 2.3.



Source: RPMS

Forecast

POLIO,NOS past due
HIB,NOS past due
HEP B,NOS past due
VARICELLA past due

Registry	Vaccine	Visit Date	Age@Visit	Location	Reaction	Volume	Inj. Site	Lot	Manufacturer	VIS Date	Administered By	Vaccine Eligibility	Admin Date	Admi
RPMS ONLY	DTaP	07/26/2018	8 mths	Claremore Hospital									07/26/2018	
RPMS ONLY	DTaP	11/15/2018	12 mths	Claremore Hospital									11/15/2018	
RPMS ONLY	DTaP	06/09/2020	31 mths	Walmart									06/09/2020	
RPMS ONLY	IPV	07/26/2018	8 mths	Clare									07/26/2018	
RPMS ONLY	IPV	11/15/2018	12 mths	Claremore Hospital									11/15/2018	
RPMS ONLY	MMR	05/26/2020	30 mths	2017 DEMO CLINIC CHIT		0.5	Right Thigh IM	5KK111-0010	PFIZER, INC	08/15/2019	HAGER,MARY			
RPMS ONLY	ROTA-1	06/22/2020	31 mths	Walmart									06/22/2020	

Figure 2-1: Opening Immunization Record window

Other changes include:

- The **Vaccinations** field has been renamed **Immunization** History.

- 2015 Certification requires that additional information received from a state registry be included and visible. This displays when the user clicks the **State Profile** button and a site has established a state IIS connection. See Section 2.3.

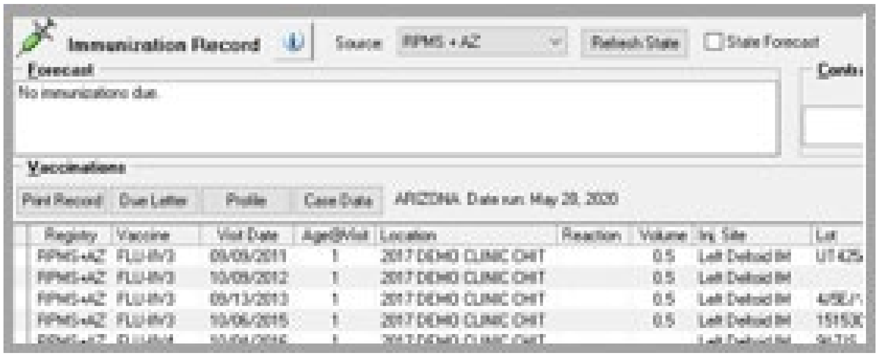
2.2 Information Button

The **Information** button (ℹ) launches a dialog allowing the user to search a variety of Web-based resources such as CDC, JAMA, and Medline for immunization-related information.

2.3 Source

- In the default view with RPMS as the source, the **Forecast** field displays forecasted immunizations according to the RPMS ICE forecaster. ICE (Immunization Calculation Engine) replaces the Texas Children's Hospital (TCH) forecaster that is no longer supported by TCH.
- If the patient may have received immunizations at locations other than yours, and your system is set up for immunization exchange with one or more states, changing the Source to **RPMS + <state>** causes additional information to be displayed as discussed below in the Section 2.6.

> **Note:** RPMS may be set up to exchange immunization data with more than one state, but only one state's information will be displayed at a time. Some functions (e.g., viewing visit detail for an immunization or editing or deleting an immunization) are disabled when viewing **RPMS + <state>** entries.



Source: RPMS + AZ

No immunizations due.

ARIZONA Date run: May 20, 2020

Registry	Vaccine	Visit Date	Age@Visit	Location	Reaction	Volume	Inj. Site	Lot
RPMS+AZ	FLU-IIV3	09/09/2011	1	2017 DEMO CLINIC CHIT		0.5	Left Deltoid IM	UT425
RPMS+AZ	FLU-IIV3	10/09/2012	1	2017 DEMO CLINIC CHIT		0.5	Left Deltoid IM	
RPMS+AZ	FLU-IIV3	09/13/2013	1	2017 DEMO CLINIC CHIT		0.5	Left Deltoid IM	4/5E/
RPMS+AZ	FLU-IIV3	10/06/2015	1	2017 DEMO CLINIC CHIT		0.5	Left Deltoid IM	15153C
RPMS+AZ	FLU-IIV4	10/04/2016	1	2017 DEMO CLINIC CHIT			Left Deltoid IM	9LT

Figure 2-2: Immunization Record window

2.4 Contraindications

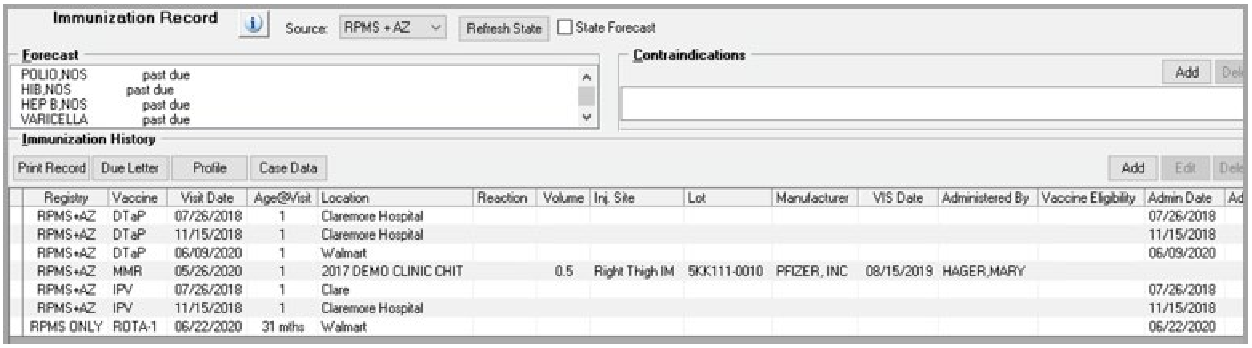
Contraindications has not changed. The following still applies:

- Lists any contraindications to immunizations that have been recorded in RPMS

- Offers options to **Add** or **Delete** contraindications

2.5 Immunization History

Immunization history displays in the **Immunization History** field.



Source: RPMS + AZ

☐ State Forecast

Forecast

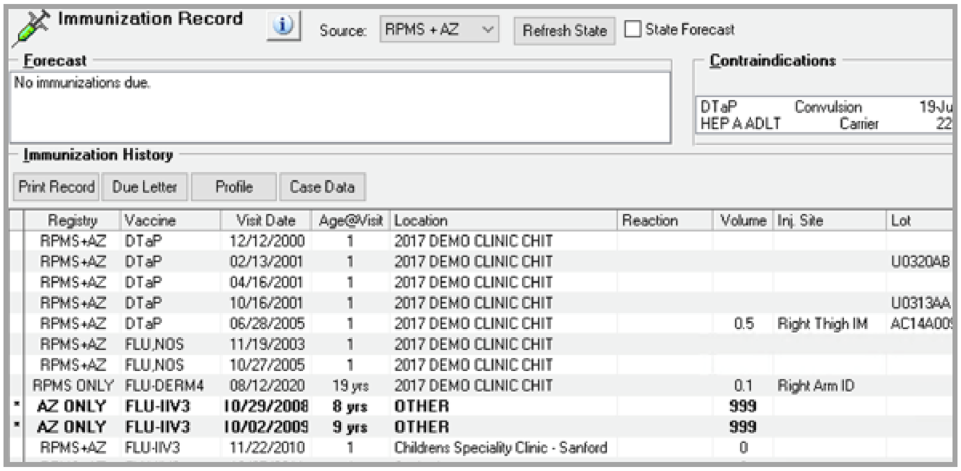
POLIO,NOS	past due
HIB,NOS	past due
HEP B,NOS	past due
VARICELLA	past due

Registry	Vaccine	Visit Date	Age@Visit	Location	Reaction	Volume	Inj. Site	Lot	Manufacturer	VIS Date	Administered By	Vaccine Eligibility	Admin Date	Ad
RPMS+AZ	DTaP	07/26/2018	1	Claremore Hospital									07/26/2018	
RPMS+AZ	DTaP	11/15/2018	1	Claremore Hospital									11/15/2018	
RPMS+AZ	DTaP	06/09/2020	1	Walmart									06/09/2020	
RPMS+AZ	MMR	05/26/2020	1	2017 DEMO CLINIC CHIT		0.5	Right Thigh IM	5KK111-0010	PFIZER, INC	08/15/2019	HAGER,MARY			
RPMS+AZ	IPV	07/26/2018	1	Clare									07/26/2018	
RPMS+AZ	IPV	11/15/2018	1	Claremore Hospital									11/15/2018	
RPMS ONLY	ROTA-1	06/22/2020	31 mths	Walmart									06/22/2020	

Figure 2-3: Immunization History window

- Includes all information data imported from state. It is typically generated before visit or in the nightly job for sites with a connection to a state registry. Sites can select how this is done.
  - The default sort is by the **Visit Date** (date of immunization), most recent first.
  - Clicking any column header re-sorts the rows as desired.
- Buttons at the top of the **Immunization History** field allow users to print a copy of the record, print a due letter, view or print a profile (including all immunizations received and due in the future), and case data displaying information about the patient.
- There is one additional button, **State Profile**, that will display if the source is set to **RPMS + <state>**, and the **State Forecast** check box is selected. This displays comprehensive information received from the state registry in a report format.
- Two new columns appear on this grid – a small blank column on the left, and a column labeled **Registry**.
  - The small blank column is used to display a flag if an immunization is received from the state that is ***not*** included in RPMS.
  - The **Registry** column displays the location of the immunization data.
    - Most entries should be **RPMS + <state>**, indicating that the immunization is recorded in both RPMS and in the state registry.

- **RPMS Only** displays when an immunization is included in RPMS but is ***not*** included in the state registry. This may indicate that the transmission to the state was unsuccessful (or has not been established). Site managers will be able to look at state IIS export data to help troubleshoot these errors. Tech support can be contacted to be sure the exchange connection is functioning.
- **<State>** Only displays when an immunization was given at a different site and is included in the state download but was not found in RPMS. These entries may be duplicates of existing entries that the system did not identify, or they may be truly unique. **<State>only** entries will be in bold type and flagged to alert users that these entries may need to be manually entered into RPMS as historical immunizations. This is seen below in Figure 2-4



Source: RPMS + AZ

□ State Forecast

Forecast

No immunizations due.

Contraindications

DTaP Convulsion 19-Ju
HEP A ADLT Carrier 22

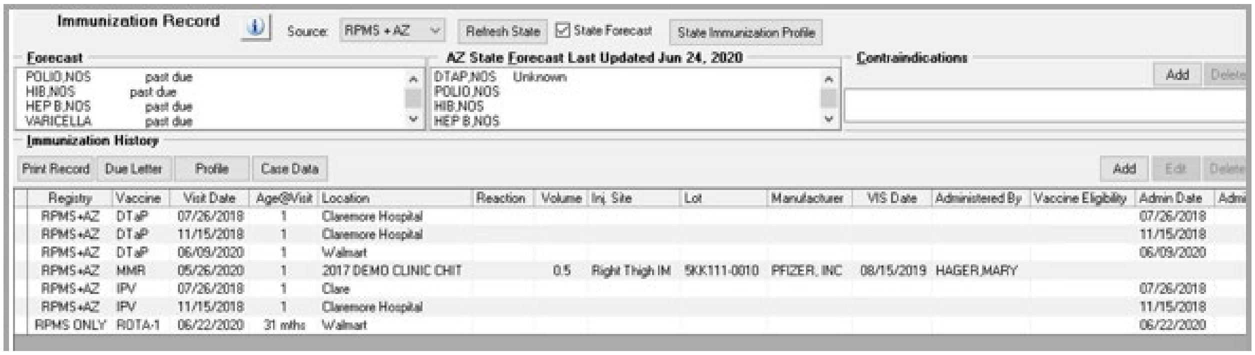
Immunization History

	Registry	Vaccine	Visit Date	Age@Visit	Location	Reaction	Volume	Inj. Site	Lot
	RPMS+AZ	DTaP	12/12/2000	1	2017 DEMO CLINIC CHIT				
	RPMS+AZ	DTaP	02/13/2001	1	2017 DEMO CLINIC CHIT				U0320AB
	RPMS+AZ	DTaP	04/16/2001	1	2017 DEMO CLINIC CHIT				
	RPMS+AZ	DTaP	10/16/2001	1	2017 DEMO CLINIC CHIT				U0313AA
	RPMS+AZ	DTaP	06/28/2005	1	2017 DEMO CLINIC CHIT		0.5	Right Thigh IM	AC14A00
	RPMS+AZ	FLU,NOS	11/19/2003	1	2017 DEMO CLINIC CHIT				
	RPMS+AZ	FLU,NOS	10/27/2005	1	2017 DEMO CLINIC CHIT				
	RPMS ONLY	FLU-DERM4	08/12/2020	19 yrs	2017 DEMO CLINIC CHIT		0.1	Right Arm ID	
*	**AZ ONLY**	**FLU-IIV3**	**10/29/2008**	**8 yrs**	**OTHER**		**999**		
*	**AZ ONLY**	**FLU-IIV3**	**10/02/2009**	**9 yrs**	**OTHER**		**999**		
	RPMS+AZ	FLU-IIV3	11/22/2010	1	Childrens Speciality Clinic - Sanford		0		

Figure 2-4: History Window Displaying AZ ONLY Entries

2.6 State Forecast

If the user selects the **State Forecast** check box, the state forecast displays (Figure 2-5).



Source: RPMS + AZ

☑ State Forecast

Forecast

POLIO,NOS past due
HIB,NOS past due
HEP B,NOS past due
VARICELLA past due

AZ State Forecast Last Updated Jun 24, 2020

DTAP,NOS Unknown
POLIO,NOS
HIB,NOS
HEP B,NOS

Contraindications

Immunization History

Registry	Vaccine	Visit Date	Age@Visit	Location	Reaction	Volume	Inj. Site	Lot	Manufacturer	VIS Date	Administered By	Vaccine Eligibility	Admin Date	Admi
RPMS+AZ	DTaP	07/26/2018	1	Claremore Hospital									07/26/2018	
RPMS+AZ	DTaP	11/15/2018	1	Claremore Hospital									11/15/2018	
RPMS+AZ	DTaP	06/09/2020	1	Walmart									06/09/2020	
RPMS+AZ	MMR	05/26/2020	1	2017 DEMO CLINIC CHIT		0.5	Right Thigh IM	5KK111-0010	PFIZER, INC	08/15/2019	HAGER,MARY			
RPMS+AZ	IPV	07/26/2018	1	Clare									07/26/2018	
RPMS+AZ	IPV	11/15/2018	1	Claremore Hospital									11/15/2018	
RPMS ONLY	ROTA-1	06/22/2020	31 mths	Walmart									06/22/2020	

Figure 2-5: State Forecast window

- Displays the state name (e.g., Arizona)
- Displays the Date on which the state forecast was last updated
- Offers a **Refresh** button that allows the user to request a new query to the state IIS, which is useful if the Date displayed is not recent

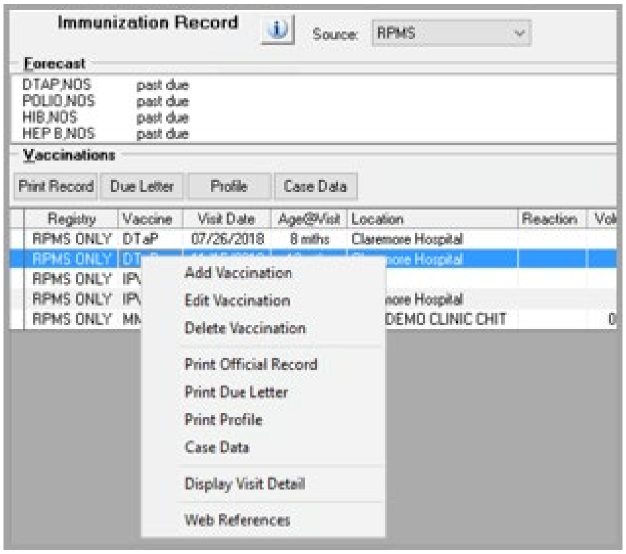
> **Note:** Clicking the **Refresh** button refreshes both the State Forecast and the State Immunization History elements.

- Lists the current immunization forecast as supplied by the state IIS
  - This text area displays **Error** if the last query to the state IIS failed to return data.
  - If **Error** displays, the user should attempt a new query by clicking **Refresh**. Error details display and more information can be found in the **IMM Package** in RPMS.

2.7 Context Menu Options

Users can right-click any row of immunizations to display a context menu of additional options.

> **Note:** This only displays for immunizations listed as **RPMS Only**. Those listed as **<state> Only** or **RPMS + <state>** will not display.



Immunization Record

Source: RPMS

Forecast

DTAP,NOS	past due
POLIO,NOS	past due
HIB,NOS	past due
HEP B,NOS	past due

Vaccinations

Registry	Vaccine	Visit Date	Age@Visit	Location	Reaction	Vol
RPMS ONLY	DTaP	07/26/2018	8 mths	Claremore Hospital		
RPMS ONLY	DT			nore Hospital		
RPMS ONLY	IP					
RPMS ONLY	IP			nore Hospital		
RPMS ONLY	MM			DEMO CLINIC CHIT		0

Figure 2-6: Immunizations context menu example

- **Add Vaccination**
- **Edit Vaccination (Only for recent visits)**

- **Delete Vaccination (Only for recent visits)**
- **Print Official Record**
- **Print Due Letter**
- **Print Profile**
- **Case Data**
- **Display Visit Detail:** This option launches a text-only dialog containing the details of the selected visit. This is the same as the information that displays when clicking a visit on the cover sheet.
- **Web Reference:** This option launches the same dialog as when the user clicks the **Web Resources** button at the top of the component.

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 Web site: 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 ROB 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	Meaning
ICE	Immunization Calculation Engine
IIS	Immunization Information System
IHS	Indian Health Service
RPMS	Resource and Patient Management System
TCH	Texas Children’s Hospital

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