RESOURCE AND PATIENT MANAGEMENT SYSTEM

Adverse Reaction Tracking

(GMRA)

Addendum to User Manual

Version 4.0 Patch 1010
October 2022

Office of Information Technology
Division of Information Resource Management

Table of Contents

Preface

The purpose of this manual is to provide the user with guidance on changes and needed configuration updates for functionality included in **GMRA v4.0 patch 1010.**

Recommended Users

This document addresses the needs of Clinical Informaticists, as well as end-users of the Indian Health Service (IHS) Resource Patient Management System (RPMS) Electronic Health Record (EHR).

Important:	Read each **Notes** file (**.n**) associated with the patches with the national release of **GMRA v4.0 p1010.**

1.0 Introduction

This document provides an overview of **GMRA v4.0 p1010** package and assumes that the site has already loaded patches up through **GMRA v4.0 p1009**. Read the installations notes and all accompanying documentation referring to **GMRA**. Thoroughly review this manual, patch notes, and requirements.

The **GMR ALLERGIES file (120.82)** and the **SIGN/SYMPTOMS (120.83)** files have been standardized. As a result of standardization, sites will no longer be allowed to add or edit entries in either of these files. In addition, users will no longer be able to add *free-text* reactants or signs/symptoms. With the move toward standardization and without the ability to add or edit the files, it is essential that **GMRA** content updates of new, outdated, or inactivated items are provided to the sites as new drugs, ingredients, and substances become available to patients. This patch contains updates to the files.

GMRA v4.0 patch 1010 also contains changes to address the *Social Security Number Fraud Prevention Act of 2017 (Public Law # 115-59)* requiring Federal Government agencies to discontinue including **Social Security Numbers (SSN)** on documents sent by United States mail no later than September 15, 2022.

> **Note**: This act does not mean that SSNs cannot be sent at all, they just must be sent by a traceable method, like **FedEx**, **United Parcel Service (UPS)**, or **United States Postal Service (USPS) Priority Mail®** with **Delivery Confirmation.**

1.1 Overview of Changes

1.1.1 Bug Fixes

The GMRA package has been updated to meet regulatory needs and address a bug. Changes include:

- Modify routines that display **SSN** in **GMRA** reports.
- Modify **patient identifier** to the **Health Record Number**.
- Correct issue with **Adverse Reaction Order Check**.

1.1.2 Enhancements/Updates

GMRA v4.0 p1010 enhancements include:

- Updates to the **GMR ALLERGIES file (120.82)**
- Updates to the **SIGN/SYMPTOMS file (120.83)**

1.2 Contents of Distribution

File	Description
gmra0400.1010k	IHS KIDS build containing the VistA updates
gmra0400.1010n	The notes file
gmra0400.1010o.pdf	This addendum to the user manual

1.3 Required Resources

- VA Kernel (XU) v8.0 patch 1019 or later
- VA FileMan (DI) v22.0 patch 1018 or later
- GMRA v4.0 patch 1009

1.4 Preinstall Instructions

Before **GMRA v4.0 patch 1010** is installed, ensure that at least one person or group is assigned to the **GMRA REQUEST NEW REACTANT Mailman** group. If another group is assigned to the **GMRA REQUEST NEW REACTANT Mailman** group, ensure that at least one person is assigned to that member group. The **Mailman** bulletins sent to this group are extremely important to review and act upon.

1.5 Install Instructions

Read all **Installation Notes** associated with GMRA v4.0 patch 1010. Users may be on the system during installation of this patch, though it should be loaded during non-peak hours to minimize disruption to users.

2.0 Changes for this Patch

The following sections provide general information about the fixes and enhancements for **GMRA v4.0 p1010**.

2.1 Sign/Symptoms File (File 120.83)

All changes to the **Sign/Symptoms** file are listed in Appendix A.

2.2 GMR Allergies File (File 120.82)

All changes to the **GMR Allergies** file are listed in Appendix B.

2.3 Changes related to Social Security Number Reduction

For certain reports, the patient identifier was displaying the first letter of the patient's **last name** and the last 4 numbers of the patient's **SSN**. This has been changed back to the patient's health record number. Reports affected include:

- **P&T Committee ADR Outcome Report**
- **P&T Committee ADR Report**
- **Print an FDA Report for a Patient**
- **Print All FDA Events within a D/T Range**

2.4 Adverse Reaction Order Check

An issue with the adverse reaction order check triggering was reported. For a situation where a given patient had a new adverse reaction entered for the same **ingredient** or **VA Drug Class** code as an existing inactivated reaction, when a prescriber was ordering medications the order checks were stopping after checking the inactive reaction and not checking against the newer, active reaction. Changes were made to the **GMRAOR** routine so that the newer active reaction is checked during the ordering process.

Appendix A Sign/Symptoms File Changes

A.1 New Entries

Name	Synonym	Status	VUID	Master VUID
AMPUTATION DUE TO INFECTION		ACTIVE	5325828	YES
EXCESSIVE THIRST	THIRST, EXCESSIVE	ACTIVE	5330749	YES
EYE IRRITATION		ACTIVE	4538655	YES
FASCIITIS		ACTIVE	5325824	YES
FOURNIER'S GANGRENE		ACTIVE	5325822	YES
GANGRENE		ACTIVE	5325826	YES
GENITAL INFECTION		ACTIVE	5333967	YES
HEMATOCHEZIA		ACTIVE	4539269	YES
INSUFFICIENT THERAPY RESPONSE		ACTIVE	5248401	YES
LIPOATROPHY		ACTIVE	5214528	YES
LUPUS, DRUG INDUCED	DRUG INDUCED LUPUS ERYTHEMATOS	ACTIVE	4539798	YES
	SYSTEMIC LUPUS ERYTHEMATOSUS			
LYMPHOCYTOPENIA		ACTIVE	5199163	YES
NONARTERITIC ANT ISC OPT NEURO	NAION	ACTIVE	4712463	YES
	NON-ARTERITIC ANTER... (NAION)			
	NONARTERITIC ANTER... (NAION)			
PROSTATE PAIN		ACTIVE	5258490	YES
TARDIVE MYOCLONUS	MYOCLONUS, TARDIVE	ACTIVE	5259143	YES
TENDONITIS		ACTIVE	5246472	YES
TINEA CAPITIS		ACTIVE	5333959	YES
TINEA CORPORIS		ACTIVE	5333963	YES
TINEA CRURIS		ACTIVE	5333955	YES
TINEA PEDIS		ACTIVE	5333961	YES
TINEA UNGULUM		ACTIVE	5333957	YES
URINARY TRACT INFECTION		ACTIVE	5325830	YES

VASOVAGAL REACTION		ACTIVE	5327535	YES

A.2 Inactivated Entries

Name	Status
FETAL DEATH	INACTIVE
INSUFFICIENT RESPONSE	INACTIVE

A.3 Changed Entries

Name	Edit type
BLACK TONGUE	Remove synonym:
	LINGUA NIGRA
DIAPHORESIS	Remove synonym:
	SWEATING EXCESSIVE
EXCESSIVE SEXUAL FANTASIES	Reactivate
	Add VUID:
	5237332
	Mark as Master for VUID
INCREASED SERUM CREATININE	Add synonym:
	SERUM CREATININE INCREASED
SORE THROAT	Remove all synonyms
SWELLING OF THROAT	Remove all synonyms
THROAT IRRITATION	Remove synonym:
	ITCHING OF THROAT

Appendix B GMR Allergies Changes

A.4 New Entries

Name	Allergy Type	Synonym	Drug Ingredient	VA Drug Class	Status	VUID	Master VUID
ABSORBABLE SUTURES	OTHER	DISSOLVABLE STITCHES			ACTIVE	4540927	YES
		SUTURES, ABSORBABLE					
ALFALFA POLLEN	OTHER	ALFALFA			ACTIVE	5315018	YES
ALGAE	DRUG, FOOD		BLUE GREEN ALGAE		ACTIVE	4541697	YES
			BROWN ALGAE				
			RED MARINE ALGAE				
ANT VENOM	OTHER	ANT BITES			ACTIVE	5315045	YES
		ANTS					
ANTITHROMBOEMBOLIC STOCKINGS	OTHER	TED HOSE			ACTIVE	5315019	YES
ARROWROOT	FOOD				ACTIVE	5259147	YES
ARTEMISININS	DRUG				ACTIVE	5335445	YES
BAMBOO	DRUG, FOOD				ACTIVE	5339495	YES
BEAN SPROUTS	FOOD	SPROUTS, BEAN			ACTIVE	5246470	YES
BEECH POLLEN	OTHER				ACTIVE	5327723	YES
BIRCH POLLEN	OTHER	BIRCH TREES			ACTIVE	5315021	YES
BIRD	OTHER				ACTIVE	5332148	YES

Name	Allergy Type	Synonym	Drug Ingredient	VA Drug Class	Status	VUID	Master VUID
BIRD DROPPINGS	OTHER	BIRD FECES			ACTIVE	5332146	YES
BLACK WIDOW SPIDER VENOM	OTHER	BLACK WIDOW SPIDER BITES			ACTIVE	5315022	YES
		BLACK WIDOW SPIDERS					
BONE CEMENT	DRUG	CEMENT			ACTIVE	5315024	YES
		CEMENT, BONE					
BUMBLE BEE VENOM	OTHER	BUMBLE BEE STINGS			ACTIVE	5315025	YES
		BUMBLE BEES					
CANNABIS	DRUG, FOOD		MARIJUANA		ACTIVE	4541236	YES
CARBA MIX	DRUG	CARBA-MIX	NITRILE		ACTIVE	4541248	YES
		CARBAMATES	LATEX				
			IODOPROPYNYL BUTYLCARBAMATE				
CARDAMOM	FOOD	CARDAMON			ACTIVE	5254433	YES
		CARDAMUM					
CEMENT, INDUSTRIAL	OTHER	CEMENT			ACTIVE	5315027	YES
CHALK	OTHER				ACTIVE	4539909	YES
CHIGGER MATERIAL	OTHER	CHIGGERS			ACTIVE	5315028	YES
CHRYSANTHEMUM	DRUG, FOOD	PYRETHRUM	ALLERGENIC EXTRACT, PYRETHRUM		ACTIVE	5327960	YES

Name	Allergy Type	Synonym	Drug Ingredient	VA Drug Class	Status	VUID	Master VUID
			PYRETHRUM OLEO RESIN				
CHRYSANTHEMUM POLLEN	OTHER				ACTIVE	5327962	YES
COCKROACH MATERIAL	OTHER	COCKROACHES			ACTIVE	5315029	YES
COMMON MILLET	FOOD	MILLET			ACTIVE	5332366	YES
COTTONWOOD POLLEN	OTHER	COTTONWOOD TREES			ACTIVE	5315031	YES
CYANOACRYLATE ADHESIVES	OTHER	SUPER GLUE			ACTIVE	5315033	YES
		SUPERGLUE					
DAIRY FOODS	FOOD	DAIRY PRODUCTS			ACTIVE	5315034	YES
DEER FLY SALIVA	OTHER	DEER FLIES			ACTIVE	5315035	YES
		DEER FLY BITES					
DISINFECTANT	OTHER	LYSOL DISINFECTANT			ACTIVE	4541550	YES
		LYSOL DISINFECTANT SPRAY					
		LYSOL SPRAY					
DUCK MATERIAL	OTHER	DUCKS			ACTIVE	5315039	YES
DUCK MEAT	FOOD	DUCKS			ACTIVE	4540823	YES
ELECTRODE PAD	OTHER	ECG ELECTRODE PAD			ACTIVE	5214526	YES
		PAD, ELECTRODE					
ELM POLLEN	OTHER	ELM TREES			ACTIVE	5315043	YES

Name	Allergy Type	Synonym	Drug Ingredient	VA Drug Class	Status	VUID	Master VUID
ENDIVE	FOOD				ACTIVE	5214520	YES
FENNEL	DRUG, FOOD		FENNEL		ACTIVE	5214522	YES
FIRE ANT VENOM	OTHER	FIRE ANT BITES			ACTIVE	5315044	YES
		FIRE ANTS					
FRESH FRUITS	FOOD				ACTIVE	5315046	YES
FRUITS	FOOD				ACTIVE	5315047	YES
GOLDENROD POLLEN	OTHER				ACTIVE	5315016	YES
HEART OF PALM	FOOD				ACTIVE	5339491	YES
HEMODIALYSIS MEMBRANE	DRUG	DIALYSIS MEMBRANE			ACTIVE	5315048	YES
HICKORY NUTS	FOOD				ACTIVE	4541135	YES
HORNET VENOM	OTHER	HORNET STINGS			ACTIVE	5315050	YES
		HORNETS					
HORSE DANDER	OTHER	HORSE HAIR			ACTIVE	4541779	YES
		HORSES					
JACKFRUIT	FOOD				ACTIVE	4539336	YES
JELLYFISH VENOM	OTHER	JELLY FISH			ACTIVE	5315053	YES
		JELLYFISH STINGS					
KISSING BUG MATERIAL	OTHER	KISSING BUG BITE			ACTIVE	5314996	YES
		KISSING BUGS					
KRATOM	OTHER				ACTIVE	5334061	YES
LEMONGRASS	FOOD				ACTIVE	5214524	YES

Name	Allergy Type	Synonym	Drug Ingredient	VA Drug Class	Status	VUID	Master VUID
LILAC POLLEN	OTHER	LILACS			ACTIVE	5315055	YES
MAPLE POLLEN	OTHER	MAPLE TREES			ACTIVE	5315057	YES
MEAT, MAMMALIAN HOOVED	FOOD				ACTIVE	5325820	YES
MERALLURIDE	DRUG	MERCURHYDRIN	MERCURY		ACTIVE	5315060	YES
MESQUITE	FOOD				ACTIVE	4541769	YES
MINT HERB	DRUG, FOOD		PEPPERMINT OIL		ACTIVE	5315062	YES
			SPEARMINT				
			SPEARMINT OIL				
MOSQUITO SALIVA	OTHER	MOSQUITO BITES			ACTIVE	5314981	YES
MULBERRIES	FOOD	MULBERRY			ACTIVE	5314982	YES
OAK POLLEN	OTHER	OAK TREES			ACTIVE	4540054	YES
OLIVE TREE POLLEN	OTHER	OLIVE TREES			ACTIVE	5314986	YES
PECTIN	DRUG, FOOD		PECTIN		ACTIVE	5333965	YES
PEPPERMINT HERB	DRUG, FOOD		PEPPERMINT OIL		ACTIVE	5315059	YES
PEPPERMINT OIL	DRUG, FOOD		PEPPERMINT OIL		ACTIVE	5314988	YES
PIGEON DROPPINGS	OTHER				ACTIVE	4541781	YES
PLASTER OF PARIS	OTHER				ACTIVE	5314991	YES
PORTUGUESE MAN OF WAR VENOM	OTHER	PORTUGUESE MAN OF WAR STING			ACTIVE	5314989	YES
POWDER, HEVEA-LATEX GLOVE	OTHER	GLOVE (LATEX) POWDER			ACTIVE	5259149	YES

Name	Allergy Type	Synonym	Drug Ingredient	VA Drug Class	Status	VUID	Master VUID
		POWDER, LATEX GLOVE					
QUINOA	FOOD				ACTIVE	5199161	YES
RABBIT MATERIAL	OTHER	RABBITS			ACTIVE	5314995	YES
RABBIT MEAT	FOOD	RABBITS			ACTIVE	5314993	YES
RAW APPLES	FOOD				ACTIVE	4540725	YES
RAW CHERRIES	FOOD				ACTIVE	5330083	YES
REDWOOD POLLEN	OTHER	REDWOOD TREES			ACTIVE	5314998	YES
RODENT MATERIAL	OTHER	RODENTS			ACTIVE	5314999	YES
RUSSIAN OLIVE POLLEN	OTHER	RUSSIAN OLIVE TREES			ACTIVE	5315041	YES
RUSSIAN THISTLE POLLEN	OTHER				ACTIVE	5315001	YES
RYE GRASS POLLEN	OTHER	RYE GRASSES			ACTIVE	5315003	YES
SAGEBRUSH POLLEN	OTHER				ACTIVE	5315005	YES
SCORPION VENOM	OTHER	SCORPION STING			ACTIVE	5315006	YES
		SCORPIONS					
SILK MATERIAL	DRUG		SILK		ACTIVE	5259145	YES
SNAKE ANTIVENIN	DRUG	SNAKE SERUM	ANTIVENIN, LATRODECTUS MACTANS	IM300	ACTIVE	5259148	YES
			ANTIVENIN, CROTALIDAE POLYVALENT	IM400			

Name	Allergy Type	Synonym	Drug Ingredient	VA Drug Class	Status	VUID	Master VUID
STARFRUIT	FOOD	CARAMBOLA			ACTIVE	4543260	YES
		STAR FRUIT					
STRAW DUST	OTHER				ACTIVE	5315014	YES
STREPTODORNASE	DRUG				ACTIVE	5327611	YES
SUNFLOWER POLLEN	OTHER	SUNFLOWERS			ACTIVE	5315008	YES
THERMOPLASTIC POLYMER	OTHER				ACTIVE	5335453	YES
TICK VENOM	OTHER	TICK BITE			ACTIVE	5315009	YES
		TICKS					
TITANIUM	DRUG		TITANIUM DIOXIDE		ACTIVE	5214530	YES
TULIPS	OTHER				ACTIVE	5330710	YES
VESPID VENOM	OTHER	VESPID STINGS			ACTIVE	5315063	YES
		VESPIDS					
WALNUT POLLEN	OTHER	WALNUT TREES			ACTIVE	5315012	YES
YELLOW JACKET VENOM	OTHER	YELLOW JACKET STINGS			ACTIVE	5315010	YES
		YELLOW JACKETS					

A.5 Inactivated Entries

Name	Status
ALFALFA	INACTIVE
ANIMAL HAIR	INACTIVE
ANT BITES	INACTIVE
ANTS	INACTIVE
ARM & HAMMER DETERGENT	INACTIVE
ARTIFICIAL COLORS	INACTIVE

Name	Status
ASPIRIN	INACTIVE
BAND-AIDS	INACTIVE
BEE STINGS	INACTIVE
BEEF PRODUCTS	INACTIVE
BEES	INACTIVE
BIRCH TREES	INACTIVE
BLACK WIDOW SPIDER BITES	INACTIVE
BLACK WIDOW SPIDERS	INACTIVE
BOLD LAUNDRY DETERGENT	INACTIVE
BUMBLE BEE STINGS	INACTIVE
BUMBLE BEES	INACTIVE
BUTTERSCOTCH FLAVORING	INACTIVE
CARDBOARD	INACTIVE
CAT HAIR	INACTIVE
CATGUT	INACTIVE
CEMENT	INACTIVE
CETYL ALCOHOL	INACTIVE
CHEER LAUNDRY DETERGENT	INACTIVE
CHIGGERS	INACTIVE
CHILI PEPPER	INACTIVE
CIGARETTES	INACTIVE
CITRUS	INACTIVE
COCKROACHES	INACTIVE
CODEINE	INACTIVE
COFFEE BEANS	INACTIVE
COTTONWOOD TREES	INACTIVE
CREAM OF WHEAT	INACTIVE
DAIRY PRODUCTS	INACTIVE
DEER FLY BITES	INACTIVE
DEER HAIR	INACTIVE
DIAL SOAP	INACTIVE
DIALYSIS MEMBRANE	INACTIVE
DOG HAIR	INACTIVE

Name	Status
DOVE SOAP	INACTIVE
DUCK	INACTIVE
DUODERM	INACTIVE
DUST MITES	INACTIVE
EGG PRODUCTS	INACTIVE
ELM TREES	INACTIVE
ERA LAUNDRY DETERGENT	INACTIVE
ERYTHROMYCIN	INACTIVE
FAT EMULSIONS	INACTIVE
FIRE ANT BITES	INACTIVE
FIRE ANTS	INACTIVE
FRESH FRUIT	INACTIVE
FROGS	INACTIVE
FRUIT	INACTIVE
GAIN LAUNDRY DETERGENT	INACTIVE
GOLDENROD	INACTIVE
GORE-TEX	INACTIVE
GRASS	INACTIVE
GREEN VEGETABLES	INACTIVE
HAND LOTION	INACTIVE
HICKORY	INACTIVE
HONEY BEE STINGS	INACTIVE
HONEY BEES	INACTIVE
HORNETS	INACTIVE
HORSE HAIR	INACTIVE
HOT PEPPER	INACTIVE
HYMENOPTERA	INACTIVE
HYMENOPTERA STINGS	INACTIVE
INSECT STINGS	INACTIVE
INSECTS	INACTIVE
IRISH SPRING SOAP	INACTIVE
IVORY SOAP	INACTIVE
JELLYFISH STING	INACTIVE

Name	Status
KISSING BUG BITE	INACTIVE
LIFEBUOY SOAP	INACTIVE
LILACS	INACTIVE
LUX SOAP	INACTIVE
LYSOL DISINFECTANT	INACTIVE
MAPLE TREES	INACTIVE
MERCUHYDRIN	INACTIVE
MINT	INACTIVE
MOSQUITO BITES	INACTIVE
MULBERRY	INACTIVE
OAK TREES	INACTIVE
OLIVE TREES	INACTIVE
PASTA	INACTIVE
PENICILLIN	INACTIVE
PEPPER	INACTIVE
PEPPERMINT	INACTIVE
PEPPERONI	INACTIVE
PET HAIR	INACTIVE
PINE NEEDLES	INACTIVE
PINE PRODUCTS	INACTIVE
PORK PRODUCTS	INACTIVE
PORTUGUESE MAN OF WAR STING	INACTIVE
POWDERED CREAMER	INACTIVE
RABBIT	INACTIVE
REDWOOD TREES	INACTIVE
RODENTS	INACTIVE
RUSSIAN OLIVE TREES	INACTIVE
RYE GRASSES	INACTIVE
SAFEGUARD SOAP	INACTIVE
SAGEBRUSH	INACTIVE
SCORPION STING	INACTIVE
SESAME	INACTIVE

Name	Status
SNAKE SERUM	INACTIVE
SOY	INACTIVE
SOY PRODUCTS	INACTIVE
SPAM	INACTIVE
SPIDER BITES	INACTIVE
SPIDERS	INACTIVE
STRAW	INACTIVE
SUNFLOWERS	INACTIVE
SUPER GLUE	INACTIVE
SWEET'N LOW	INACTIVE
TED HOSE	INACTIVE
TEGADERM	INACTIVE
TICK BITE	INACTIVE
TIDE LAUNDRY DETERGENT	INACTIVE
TOMATO PRODUCTS	INACTIVE
TREES	INACTIVE
TUMERIC	INACTIVE
VESPID STINGS	INACTIVE
VESPIDS	INACTIVE
WALNUT TREES	INACTIVE
WASP STINGS	INACTIVE
WASPS	INACTIVE
WEEDS	INACTIVE
WISK LAUNDRY DETERGENT	INACTIVE
YELLOW JACKET STINGS	INACTIVE
ZEST SOAP	INACTIVE

A.6 Changed Entries

Name	Edit type
ADHESIVE TAPE	Add synonym:
	BAND-AIDS
	TAPE

Name	Edit type
ANIMAL DANDER	Add synonym:
	ANIMAL HAIR
	ANIMALS
	PET HAIR
APPLE JUICE	Remove synonym:
	APPLE JUICES
ASPARTAME (SWEETENER)	Add synonym:
	NUTRA-SWEET
BANANAS	Remove synonym:
	BANANA
BEE VENOM	Add synonym:
	BEE STINGS
	BEES
BLACK DYES	Change Allergy Type:
	FOOD
CAT DANDER	Add synonym:
	CAT HAIR
	CATS
CHICKPEAS	Add synonym:
	GARBANZO BEANS
CIGARETTE SMOKE	Add synonym:
	CIGARETTES
CONTRAST MEDIA	Add drug ingredient:
	FERROUS CITRATE,FE-59
DEER HIDE	Add synonym:
	DEER HAIR
DEET	Change Allergy Type:
	DRUG
	Add drug ingredient:
	DEET N,N-DIETHYL-META-TOLUAMIDE
DOG DANDER	Add synonym:
	DOG HAIR

Name	Edit type
	DOGS
DUST MITE FECES	Add synonym:
	DUST MITES
EGGNOG	Remove drug ingredient:
	EGG
EGGSHELLS	Change Allergy Type:
	DRUG
ETHYL ALCOHOL	Remove drug ingredient:
	ALCOHOL
FEATHERS	Add synonym:
	GOOSE FEATHERS
FOOD DYES	Change Allergy Type:
	FOOD
	Add synonym:
	ARTIFICIAL COLORS
FROG LEGS	Add synonym:
	FROGS
GRAPEFRUIT	Add drug ingredient:
	GRAPEFRUIT EXTRACT
HONEY BEE VENOM	Add synonym:
	HONEY BEE STINGS
	HONEY BEES
HYMENOPTERA VENOM	Add synonym:
	HYMENOPTERA STINGS
INSECT VENOM	Add synonym:
	INSECT STINGS
	INSECTS
LOTION	Add synonym:
	HAND LOTION
METOCLOPRAMIDE	Reactivate
MONOSODIUM GLUTAMATE	Add synonym:
	MONOSODIUM GLUTAMATES

Name	Edit type
NITRITES	Change Allergy Type:
	FOOD
	Add synonym:
	NITRATES
	POTASSIUM NITRATE
	SODIUM NITRATE
NON-DAIRY CREAMER	Add synonym:
	POWDERED CREAMER
OATMEAL	Change Allergy Type:
	FOOD
PAPER	Add synonym:
	CARDBOARD
PINE SAP	Add synonym:
	PINE NEEDLES
PINE TREES	Add synonym:
	PINE NEEDLES
PINEAPPLES	Remove synonym:
	PINEAPPLE
PINK DYES	Change Allergy Type:
	FOOD
PORK	Change Allergy Type:
	DRUG, FOOD
	Add drug ingredient:
	ENOXAPARIN
	DALTEPARIN SODIUM
	HEPARIN
PROCESSED MEATS	Add synonym:
	BALOGNA
	HOT DOGS
	PEPPERONI
	SPAM
PURPLE DYES	Change Allergy Type:
	FOOD

Name	Edit type
RATTLESNAKE VENOM	Add synonym:
	RATTLESNAKES
RED WINE	Remove drug ingredient:
	ALCOHOL
RUM	Remove drug ingredient:
	ALCOHOL
SCOTCH	Remove drug ingredient:
	ALCOHOL
SESAME OIL	Mark as Master for VUID
SNAKE VENOM	Add synonym:
	SNAKE BITES
	SNAKES
SOFT DRINKS	Remove synonym:
	POP
SOYBEANS	Add synonym:
	SOY
SPIDER VENOM	Add synonym:
	SPIDER BITES
	SPIDERS
SULFA DRUGS	Remove drug ingredient:
	SULFISOXAZOLE
	SUMATRIPTAN
TEFLON	Add synonym:
	GORE-TEX
TREE POLLEN	Add synonym:
	TREES
VODKA	Remove drug ingredient:
	ALCOHOL
WASP VENOM	Add synonym:
	WASP STINGS
	WASPS
WEED POLLEN	Add synonym:
	WEEDS

Name	Edit type
WHEAT	Add synonym:
	CREAM OF WHEAT
WHITE BEANS	Add synonym:
	HARICOT BEANS
	NAVY BEANS
WHITE PEPPER	Add synonym:
	PEPPER
WHITE WINE	Remove drug ingredient:
	ALCOHOL
YOGURT	Reactivate

Appendix C 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.7 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.8 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.8.1 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.8.2 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.8.3 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.8.4 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.8.5 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.8.6 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.8.7 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.8.8 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.8.9 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.8.10 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.8.11 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.8.12 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.8.13 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.8.14 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
ADR	Adverse Drug Reaction
CISO	Chief Information Security Officer
EHR	Electronic Health Record
FDA	Food and Drug Administration
GMR	General Medical Record
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
ID	Identification
IHS	Indian Health Service
ISSO	Information System Security Officer
IT	Information Technology
KIDS	Kernel Installation and Distribution System
P&T	Pharmacy and Therapeutics
PC	Personal Computer
RoB	Rules of Behavior
RPMS	Resource and Patient Management System
SAC	Standards and Conventions
SSN	Social Security Number
UPS	United Parcel Service
USPS	United States Postal Service
VA	Veterans Administration
VPN	Virtual Private Network

Contact Information

If you have any questions or comments regarding this distribution, please contact the IHS IT Service Desk.

Phone: (888) 830-7280 (toll free)

Web: https://www.ihs.gov/itsupport/

Email: itsupport@ihs.gov