RESOURCE AND PATIENT MANAGEMENT SYSTEM

Monthly Health Information Technology

(HIT)

Systems Assessment Guide Methods Section 30-34

Version 1.0
August 2025

Office of Information Technology
Division of Information Technology

Table of Contents

Version History

Version 1: Due to the current state of the HIT system in the Indian Health Service this version is focused on the Electronic Medical Record (EMR) that is currently in use (RPMS/EHR). Future versions will encompass other EMRs.

Purpose

To assist the local HIT team by providing a review of definitions, recommendations, methods, and associated reports to assess the local HIT systems status.

Vision

To provide the local HIT team a resource to aid in HIT systems optimization and help the local HIT team to create a plan to address deficiencies identified by system review.

Value

To prioritize humble and transparent collaboration within the local HIT team to aid in systems optimization.

Mailman Group Review

- RPMS tool that alerts and communicates with SMEs about issues or actions.
- Identifies who gets alerts via locally defined groups.
- Configuration and ongoing updates are needed to ensure the right information is shared with the correct stakeholders.

Method

Print FileMan File "Mail Group" and do "[CAP". Perform review of personnel assigned to each group. Update as needed.

- Currently recognized important mailman to consider for use.

Pharmacy:

- APSP EPRESCRIBING
- APSQ DRUG AWP/AAC NOTIFICATION
- BCMA ISSUES
- BEHO EPCS INCIDENT RESPONSE
- BOP MAILGROUP
- BPDM EXPORT MANAGEMENT
- CMOP MANAGERS
- GMRA MARK CHART
- GMRA P&T COMMITTEE FDA
- GMRA REQUEST NEW REACTANT
- GMRA VERIFY DRUG ALLERGY
- GMRA VERIFY FOOD ALLERGY
- GMRA VERIFY OTHER ALLERGY
- NDF DATA
- PSO DRUG

Informatics:

- PXRM ERRORS (Reminder errors).

Health Information Management:

- BEHOCCD HIMS TOC
- DGPF LOCAL FLAG REVIEW

- TIU MIS ALERTS (Is used in missing cosigner TaskMan)

Laboratory Informaticist:

- BLRLINK.
- LAB HIGH URGENCY NOTIFICATION
- LAB MESSAGING
- LAB QUALITATIVE ALERT

Purchased/Referred Care:

- BMC CHS ALERT
- BMC IHS ALERT
- BMC INHOUSE ALERT
- BMC OTHER ALERT

Others:

- AGMPI
- BLR LAB PATIENT MERGE
- BYIM EXPORT/IMPORT GROUP
- DIABETIC COORDINATOR (not clear if this still works)
- LMI
- RPMS Dental – Dentrix if used

Report Example

SPI NOTIFICATION (Surescripts Provider Identification) MAIL GROUP LIST

```
---------------------------------------------------------------------------


NAME: ADEX-ABEND

NAME: ADEX-COMPLETE

NAME: ADEX-START

NAME: AGMP MPI                          TYPE: public
COORDINATOR: ADAM,ADAM
 DESCRIPTION:   This mail group will receive alerts when there is an error in MPI
message processing. Members should include those who would be fixing and
reprocessing messages that contain errors.
  ORGANIZER: ADAM,ADAM

NAME: AMER ER PATIENT MERGE ALERTS      TYPE: public
ALLOW SELF ENROLLMENT?: YES             RESTRICTIONS: UNRESTRICTED
COORDINATOR: ADAM,ADAM
```

```
 DESCRIPTION:   This is the mail group is used to distribute ERS Patient Merge Alert
messages
  ORGANIZER: ADAM,ADAM

NAME: APSP EPRESCRIBING                 TYPE: private
ALLOW SELF ENROLLMENT?: NO              RESTRICTIONS: UNRESTRICTED
COORDINATOR: POSTMASTER
 DESCRIPTION:   Contains recipients of bulletins regarding the status of e-
Prescribing messages.
  ORGANIZER: POSTMASTER
```

Figure 30-1: Mail Group List Report Example

VueCentric Template (EHR GUI) Review

- VueCentric Template is the graphical user interface of RPMS EHR.
- "Ease of Use" and readability should be evaluated to improve usability and to ensure optimal use of RPMS EHR.
- Standardization can facilitate troubleshooting, improve the user experience, and simplify training.

Method

Use VcManager and Template Registry Tab to:

- Select "association" and review current VueCentric template assignments. Use the "defaults" button to better organize how your system is laid out.
- Export or Import VueCentric Templates.

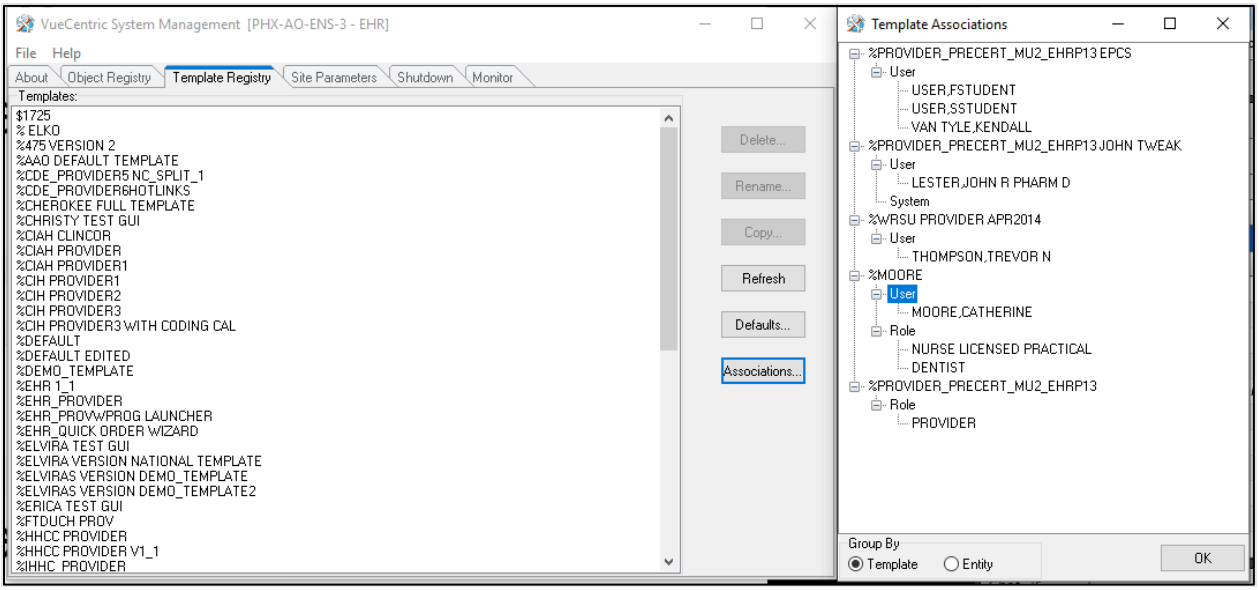

Figure 31-1: Template Registry tab

User in the System

- Up-to-date and accurate user profiles ensure that a profile is functional and that users are appropriately identified and mapped in RPMS EHR.
- When a user leaves, their RPMS EHR account needs to be disabled, and their user class and keys removed (follow off-boarding recommendations for timing).
- Proper off-boarding procedures declutters the available provider choices in RPMS EHR.

Method

- Review onboarding/off-boarding process annually.
- Determine the use of “Deactivate User” and “Inactivate User”.
- Review System Set up.
- Ensure the XX Parameter “XU645” is set to “Yes”.
- Review TaskMan Task “XUAUTODEACTIVATE” is set to “run daily”, or however often identified by your RPMS manager.
- Run the following Reports and Review for appropriateness (e.g., Suffix, Service Section, Provider Class, User Class).
- Go to VA FileMan -> Print File entries
- FileMan file = USR CLASS MEMBERSHIP
- Consider General FileMan if the report does not generate
- Ensure your telnet session is setup to handle 300 columns
- Copy from the top until the line right above 0;300;999999999
- Paste at the “OUTPUT FROM WHAT FILE: //”

Active Users:

```
USR CLASS MEMBERSHIP
@NUMBER
FIRST

"Internal Entry Number"_"^";X
"Provider Name"_"^";X
"Service / Section"_"^";X
"Provider Class"_"^";X
"Last Sign On"_"^";X
"Termination Date"_"^";X
"Termination Reason"_"^";X
"Disuser"_"^";X
"Inactive Date"_"^";X
"Time Read"_"^";X
"User Class"_"^";X

@
NCI ACTIVE USER REVIEW HEADER
Y
Y
^

P
USR CLASS MEMBERSHIP
NEW PERSON:
@.01
FIRST
NEW PERSON:
@Disuser
@
@
Y

NCI ACTIVE USER REVIEW SORT 2
Y
NO

NEW PERSON:
NUMBER_"^";R2;C1
(#.01)_"^";X;R2
(#29)_"^";X;R2
Y
(#53.5)_"^";X;R2
Y
(#202)_"^";X;R2
Y
(#9.2)_"^";X;R2
Y
(#9.4)_"^";X;R2
Y
(#7)_"^";X;R2
Y
(#53.4)_"^";X;R2
Y
(#200.1)_"^";X
Y

USER CLASS_"^";X;R2
```

```
USR CLASS MEMBERSHIP LIST
[NCI ACTIVE USER REVIEW HEADER

NCI ACTIVE USER REVIEW PRINT
Y
1
0;300;999999999999
```

Figure 32-1: USR CLASS MEMBERSHIP FileMan Print Copy/Paste Entries

- Consider Session logging the information via a telnet client (e.g. SecureCRT, Netterm) or directly printing the information by sending it to an RPMS Printer.
- Import into Excel and delimitate by "^".
  - Open Excel then go to data tab.
  - Select from text/CSV.
  - Select your file.
  - Import file.
  - Delimiter-custom "^".
  - Data Type Detection- select based on entire dataset.
  - Load.

Alternative Option:

```
Go to Va FileMan -> Print File entries
OUTPUT FROM WHAT FILE: USR CLASS MEMBERSHIP// USR CLASS MEMBERSHIP
                                            (448 entries)
SORT BY: NUMBER// NEW PERSON:
NEW PERSON FIELD: @.01  NAME
START WITH NAME: FIRST// FIRST
  WITHIN NAME, SORT BY: NEW PERSON:
  NEW PERSON FIELD: @Disuser
  START WITH DISUSER: FIRST// @
  GO TO DISUSER: LAST// @
    WITHIN DISUSER, SORT BY: Y??
    WITHIN DISUSER, SORT BY:
STORE IN 'SORT' TEMPLATE: NCI ACTIVE USER REVIEW SORT 2
                             (Aug 30, 2023@14:19) User #1723 File #8930.3  SORT
DATA ALREADY STORED THERE....OK TO PURGE? NO// YES
DESCRIPTION:
  No existing text
  Edit? NO// NO
SHOULD TEMPLATE USER BE ASKED 'FROM'-'TO' RANGE FOR 'DISUSER'? NO//
FIRST PRINT FIELD: NEW PERSON:
  THEN PRINT NEW PERSON FIELD: NUMBER_"^";R2;C1
  THEN PRINT NEW PERSON FIELD: (#.01)_"^";X;R2
  THEN PRINT NEW PERSON FIELD: (#29)_"^";X;R2
   By '#29', do you mean NEW PERSON 'SERVICE/SECTION'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#53.5)_"^";X;R2
   By '#53.5', do you mean NEW PERSON 'PROVIDER CLASS'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#202)_"^";X;R2
   By '#202', do you mean NEW PERSON 'LAST SIGN-ON DATE/TIME'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#9.2)_"^";X;R2
   By '#9.2', do you mean NEW PERSON 'TERMINATION DATE'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#9.4)_"^";X;R2
```

```
   By '#9.4', do you mean NEW PERSON 'Termination Reason'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#7)_"^";X;R2
   By '#7', do you mean NEW PERSON 'DISUSER'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#53.4)_"^";X;R2
   By '#53.4', do you mean NEW PERSON 'INACTIVE DATE'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#200.1)_"^";X
   By '#200.1', do you mean NEW PERSON 'TIMED READ (# OF SECONDS)'? Yes// Y
  (Yes)
  THEN PRINT NEW PERSON FIELD:
THEN PRINT FIELD: USER CLASS_"^";X;R2
THEN PRINT FIELD:
Heading (S/C): USR CLASS MEMBERSHIP LIST  Replace USR CLASS MEMBERSHIP LIST With
 [NCI ACTIVE USER REVIEW HEADER  Replace
   [NCI ACTIVE USER REVIEW HEADER
                              (Aug 30, 2023@14:20) User #1723 File #8930.3
STORE PRINT LOGIC IN TEMPLATE: NCI ACTIVE USER REVIEW PRINT
                              (Aug 30, 2023@14:19) User #1723 File #8930.3
TEMPLATE ALREADY STORED THERE.... OK TO REPLACE? Y  (Yes)
START AT PAGE: 1// 1
DEVICE: 0;300;9999999999
```

Figure 32-2: USR CLASS MEMBERSHIP FileMan Print Entries Detailed Steps

Inactive Users:

- Consider Session logging the information via a telnet client (e.g. SecureCRT, NetTerm) or directly printing the information by sending it to an RPMS Printer.
- Import into excel and delimitate by "^"
  - Open Excel then go to data tab
  - Select from text/CSV
  - Select your file
  - Import file
  - Delimiter-custom "^"
  - Data Type Detection- select based on entire dataset
  - Load

```
USR CLASS MEMBERSHIP
@NUMBER
FIRST

"Internal Entry Number"_"^";X
"Provider Name"_"^";X
"Service / Section"_"^";X
"Provider Class"_"^";X
"Last Sign On"_"^";X
"Termination Date"_"^";X
"Termination Reason"_"^";X
"Disuser"_"^";X
"Inactive Date"_"^";X
"Time Read"_"^";X
"User Class"_"^";X

@
NCI ACTIVE USER REVIEW HEADER
```

```
Y
Y
^

P
USR CLASS MEMBERSHIP
NEW PERSON:
@.01
FIRST
NEW PERSON:
@LAST SIGN-ON DATE/TIME<(TODAY-180)
Y

NCI ACTIVE USER REVIEW SORT 1
Y
NO

NEW PERSON:
NUMBER_"^";R2;C1
(#.01)_"^";X;R2
(#29)_"^";X;R2
Y
(#53.5)_"^";X;R2
Y
(#202)_"^";X;R2
Y
(#9.2)_"^";X;R2
Y
(#9.4)_"^";X;R2
Y
(#7)_"^";X;R2
Y
(#53.4)_"^";X;R2
Y
(#200.1)_"^";X
Y

USER CLASS_"^";X;R2

USR CLASS MEMBERSHIP LIST
[NCI ACTIVE USER REVIEW HEADER

NCI INACTIVE USER REVIEW PRINT
Y
1
0;300;99999999
```

Figure 32-3: USR CLASS MEMBERSHIP, NCI ACTIVE USER REVIEW FileMan Print Copy/Paste Entries

- Consider Session logging the information via a telnet client (e.g. SecureCRT, Netterm)or directly printing the information by sending it to an RPMS Printer.
- Import into excel and delimitate by "^"
  - Open Excel then go to data tab
  - Select from text/CSV
  - Select your file
  - Import file

- Delimiter-custom "^"
- Data Type Detection- select based on entire dataset
- Load

Alternative options:

```
OUTPUT FROM WHAT FILE: USR CLASS MEMBERSHIP// USR CLASS MEMBERSHIP
                                          (448 entries)
SORT BY: NUMBER// NEW PERSON:
NEW PERSON FIELD: @.01  NAME
START WITH NAME: FIRST// FIRST
  WITHIN NAME, SORT BY: NEW PERSON:
  NEW PERSON FIELD: @LAST SIGN-ON DATE/TIME<(TODAY-180)
   By 'LAST SIGN', do you mean NEW PERSON 'LAST SIGN-ON DATE/TIME'? Yes// Y
  (Yes)
    WITHIN LAST SIGN-ON DATE/TIME<(TODAY-180), SORT BY:
STORE IN 'SORT' TEMPLATE: NCI ACTIVE USER REVIEW SORT 1
  Are you adding 'NCI ACTIVE USER REVIEW SORT 1' as
    a new SORT TEMPLATE? No// Y  (Yes)
DESCRIPTION:
  No existing text
  Edit? NO// NO
FIRST PRINT FIELD:
FIRST PRINT FIELD: NEW PERSON:
  THEN PRINT NEW PERSON FIELD: NUMBER_"^";R2;C1
  THEN PRINT NEW PERSON FIELD: (#.01)_"^";X;R2
  THEN PRINT NEW PERSON FIELD: (#29)_"^";X;R2
   By '#29', do you mean NEW PERSON 'SERVICE/SECTION'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#53.5)_"^";X;R2
   By '#53.5', do you mean NEW PERSON 'PROVIDER CLASS'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#202)_"^";X;R2
   By '#202', do you mean NEW PERSON 'LAST SIGN-ON DATE/TIME'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#9.2)_"^";X;R2
   By '#9.2', do you mean NEW PERSON 'TERMINATION DATE'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#9.4)_"^";X;R2
   By '#9.4', do you mean NEW PERSON 'Termination Reason'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#7)_"^";X;R2
   By '#7', do you mean NEW PERSON 'DISUSER'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#53.4)_"^";X;R2
   By '#53.4', do you mean NEW PERSON 'INACTIVE DATE'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: (#200.1)_"^";X
   By '#200.1', do you mean NEW PERSON 'TIMED READ (# OF SECONDS)'? Yes// Y
  (Yes)
  THEN PRINT NEW PERSON FIELD:
THEN PRINT FIELD: USER CLASS_"^";X;R2
THEN PRINT FIELD:
Heading (S/C): USR CLASS MEMBERSHIP LIST  Replace USR CLASS MEMBERSHIP LIST With
 [NCI ACTIVE USER REVIEW HEADER  Replace
   [NCI ACTIVE USER REVIEW HEADER
                              (Aug 30, 2023@14:22) User #1723 File #8930.3

STORE PRINT LOGIC IN TEMPLATE: NCI INACTIVE USER REVIEW PRINT
  Are you adding 'NCI INACTIVE USER REVIEW PRINT' as
    a new PRINT TEMPLATE? No// Y  (Yes)
START AT PAGE: 1// 1
DEVICE:
```

Figure 32-4: USR CLASS MEMBERSHIP, NCI ACTIVE USER FileMan Print Entries Detailed Steps

Report Example

Active Users Report:

Internal E	User Name	Service / Section	Provider Class	Last Sign On	Terminati	Terminati	Disuser	Inactive Date
1	ADAM,ADAM	BUSINESS OFFICE		AUG 17,2021@19:41:24				
2072	xxxxxxxxx LPN	AMBULATORY CARE	LICENSED PRACTICAL NURSE	AUG 13,2021@08:10:46				
333	xxxxxxxxxxx J MD	AMBULATORY CARE	MD	AUG 18,2021@11:42:31				
333	xxxxxxxxxxx J MD	AMBULATORY CARE	MD	AUG 18,2021@11:42:31				
2649	Axxxxxxxxx	AMBULATORY CARE		AUG 18,2021@08:43:43				
2649	xxxxxxxxxxx J MD	AMBULATORY CARE		AUG 18,2021@08:43:43				
1020	xxxxxxxxx DDS	DENTAL	DENTIST	AUG 6,2021@14:18:54				
1020	xxxxxxxxxxxxxx DDS	DENTAL	DENTIST	AUG 6,2021@14:18:54				
2592	xxxxxxxxxxxxxx	AMBULATORY CARE	NUTRITIONIST	AUG 18,2021@08:52:57				

Figure 32-5: Active Users report in Excel

Inactive Users:

Internal Entry Number	User Name	Service / Section	Provider Class	Last Sign On	Termination Date
2296		PHARMACY	PHARMACIST	JAN 8,2019@08:07	JUN 6,2021
1484		AMBULATORY CARE	PSYCHOLOGIST	JUL 3,2013@08:58:14	
1762		OPTOMETRY	OPTOMETRY STUDENT	MAY 15,2015@13:02:51	
1985		MEDICAL RECORDS	CODING/DATA ENTRY	JUL 11,2017@07:20:46	MAR 29,2018
1704		AMBULATORY CARE	CLINIC RN	APR 27,2016@11:06	
1281		AMBULATORY CARE	MEDICAL TECHNOLOGIST	SEP 16,2011@15:11:58	OCT 23,2012
1830		AMBULATORY CARE	CLINIC RN	SEP 25,2015@14:45:50	
262		AMBULATORY CARE	OTHER	SEP 27,2019@13:00:58	SEP 29,2019
2443		AMBULATORY CARE	PHYSICIAN ASSISTANT	NOV 26,2019@14:00:10	DEC 19,2019

Figure 32-6: Inactive User in Excel

Signature Block Review

Signature Block is part of a signed TIU Progress Note and is used for Medical-Legal Authentication of notes and billing purposes.

Method

- Go to FileMan, Print File entries.
- FileMan file = USR CLASS MEMBERSHIP
- Copy from the top until the line right above 0;300;999999999
- Paste at the "OUTPUT FROM WHAT FILE: //"

```
USR CLASS MEMBERSHIP
@NUMBER
FIRST

"User Name^";C1
"Service/Section^";C11
"Provider Class^";C27
"Printed Name with Credentials - Signature Block Name^";C42
"Specialty - Signature Block Title^";C95

@
NCI SIG BLOCK REVIEW HEADER
Y
Y
^

P
USR CLASS MEMBERSHIP
NEW PERSON:
@.01
FIRST
NEW PERSON:
@Disuser
@
@
Y

NCI SIG BLOCK REVIEW SORT
Y
NO

NEW PERSON:
(#.01)_"^";X
SERVICE/SECTION_"^";X
Y
PROVIDER CLASS_"^";X
SIGNATURE BLOCK PRINTED NAME_"^";X
SIGNATURE BLOCK TITLE_"^";X


USR CLASS MEMBERSHIP LIST
[NCI SIG BLOCK REVIEW HEADER

NCI SIG BLOCK REVIEW PRINT
```

```
Y
1
0;300;99999999999
```

Figure 33-1: USR CLASS MEMBERSHIP, NCI SIG BLOCK REVIEW FileMan Print Copy/Paste Entries in excel

Alternatively:

```
OUTPUT FROM WHAT FILE: USR CLASS MEMBERSHIP// USR CLASS MEMBERSHIP
                                          (448 entries)
SORT BY: NUMBER// NEW PERSON:
NEW PERSON FIELD: @.01  NAME
START WITH NAME: FIRST// FIRST
  WITHIN NAME, SORT BY: NEW PERSON:
  NEW PERSON FIELD: @Disuser
  START WITH DISUSER: FIRST// @
  GO TO DISUSER: LAST// @
    WITHIN DISUSER, SORT BY: Y??
    WITHIN DISUSER, SORT BY:
STORE IN 'SORT' TEMPLATE: NCI SIG BLOCK REVIEW SORT
                            (Aug 30, 2023@14:31) User #1723 File #8930.3  SORT
DATA ALREADY STORED THERE....OK TO PURGE? NO// YES
DESCRIPTION:
  No existing text
  Edit? NO// NO
SHOULD TEMPLATE USER BE ASKED 'FROM'-'TO' RANGE FOR 'DISUSER'? NO//
FIRST PRINT FIELD: NEW PERSON:
  THEN PRINT NEW PERSON FIELD: (#.01)_"^";X
  THEN PRINT NEW PERSON FIELD: SERVICE/SECTION_"^";X
   By 'SERVICE', do you mean NEW PERSON 'SERVICE/SECTION'? Yes// Y  (Yes)
  THEN PRINT NEW PERSON FIELD: PROVIDER CLASS_"^";X
  THEN PRINT NEW PERSON FIELD: SIGNATURE BLOCK PRINTED NAME_"^";X
  THEN PRINT NEW PERSON FIELD: SIGNATURE BLOCK TITLE_"^";X
  THEN PRINT NEW PERSON FIELD:
THEN PRINT FIELD:
Heading (S/C): USR CLASS MEMBERSHIP LIST  Replace USR CLASS MEMBERSHIP LIST With
 [NCI SIG BLOCK REVIEW HEADER  Replace
   [NCI SIG BLOCK REVIEW HEADER
                            (Aug 30, 2023@14:31) User #1723 File #8930.3
STORE PRINT LOGIC IN TEMPLATE: NCI SIG BLOCK REVIEW PRINT
                            (Aug 30, 2023@14:31) User #1723 File #8930.3
TEMPLATE ALREADY STORED THERE.... OK TO REPLACE? Y  (Yes)
START AT PAGE: 1// 1
DEVICE:
```

Figure 33-2: Signature Block Review, alternative option

Report Example:

User Name	Service/Section	Provider Class	Printed Name with Crede	Specialty - Signature Block Title
ADAM,ADAM	BUSINESS OFFICE		ADAM ADAM	STUDENT
xxxxxxxxxxxx LPN	AMBULATORY CARE	LICENSED PRACTICAL NURSE	xxxxxxxx, LPN	
xxxxxxxJ MD	AMBULATORY CARE	MD	xxxxxxxxxxxxxxxxxxx	MD
	AMBULATORY CARE			
xxxxxxxxxxx DDS	DENTAL	DENTIST	xxxxxxxxxx, DDS	DDS
xxxxxxxxxxx	AMBULATORY CARE	NUTRITIONIST	xxxxxxxxxxxxxxxxxx	Registered Dietitian Nutritionist
xxxxxxxxxx	AMBULATORY CARE	CODING/DATA ENTRY		
Bxxxxxxxxx	AMBULATORY CARE			
xxxxxxx	AMBULATORY CARE		xxxxxxxxxxxxxxxxxx	
xxxxxxxxx	AMBULATORY CARE	DENTAL ASSISTANT		
xxxxxxxxxxxxx	AMBULATORY CARE	ADMINISTRATIVE		

Figure 33-3: Report Example in Excel

RPMS EHR Training Program Review

- Encompasses all aspects of the RPMS EHR components and applications
- Long enough to fully cover EHR component and functionality (i.e., a couple of days).
- Departments conduct further training and competency.
- Poor or inadequate training programs have contributed to patient safety and documentation issues.
- Training plan should be documented for all areas.
- Responsibility of the supervisor.

Method

Review Local General Training and discuss with departments their training and competency. Consider reviewing training options available in the RPMS Recordings and Materials Library.

- Go to: https://www.ihs.gov/rpms/training/recording-and-material-library
- Sign into your account or make one.

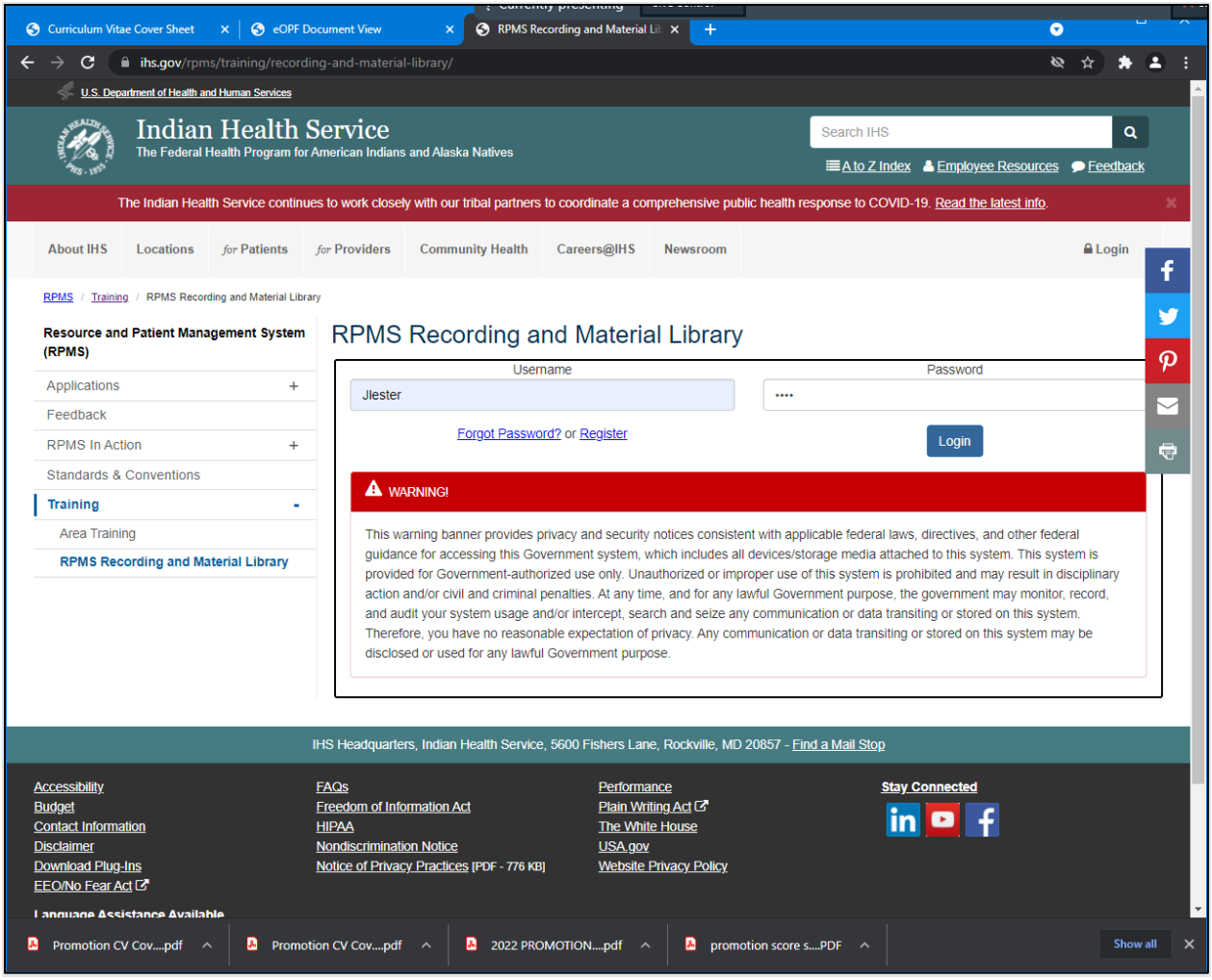

Figure 34-1: RPMS Recording and Material Library

Complete search for training needs.

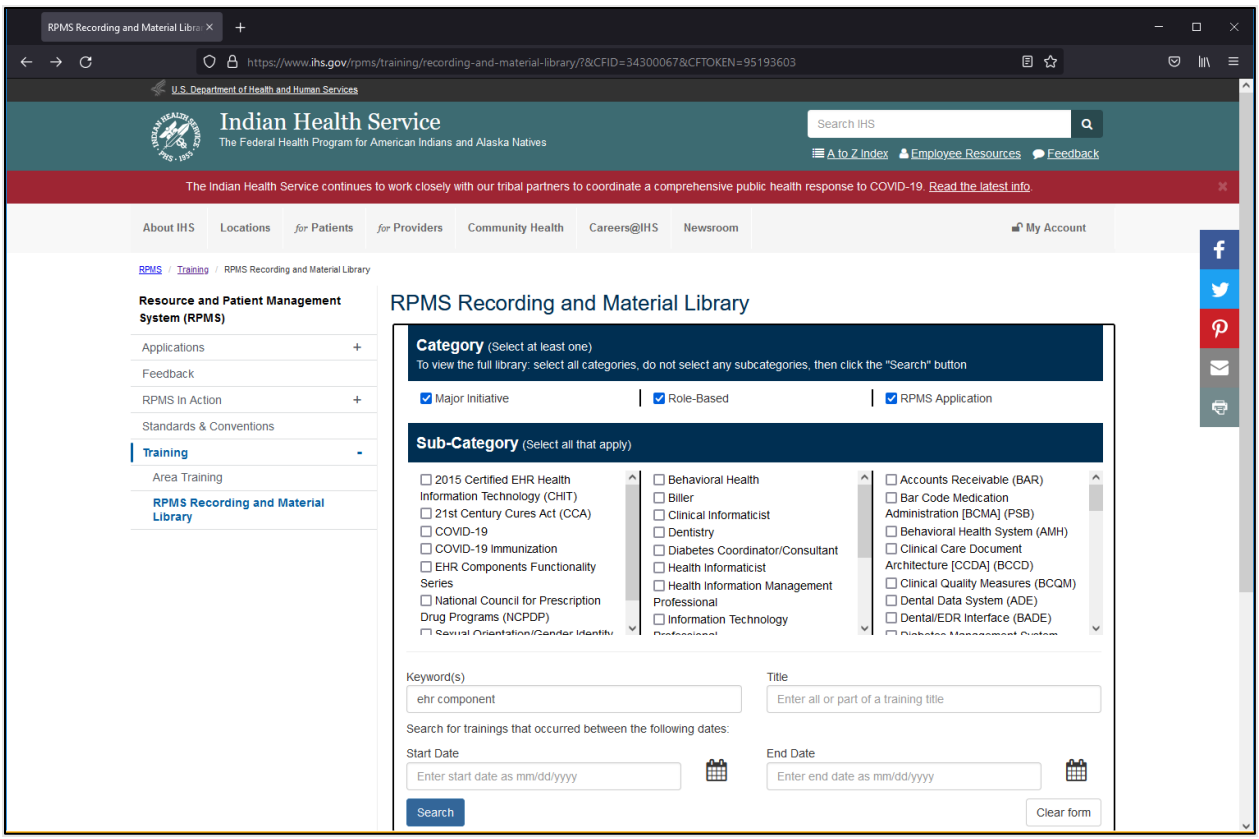

Figure 34-2: RPMS Recording and Material Library, Categories and Sub-Categories

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 with IHS policy.

- For a listing of general ROB for all users, see the most recent edition of *IHS Standard Operating Procedure 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/oittfs/standard-operating-procedures-sop/

> **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). For the purposes of the below ROB, RPMS is defined as use of RPMS, EHR, Practice Management, VistA Imaging, and any other connected information system.

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 their 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 training.
- 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.

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