RESOURCE AND PATIENT MANAGEMENT SYSTEM

AG IHS Eligibility Letter

(ZAG)

Installation, Setup, and User Guide

Version 7.1
October 2013

Office of Information Technology
Division of Information Resource Management
Albuquerque, New Mexico

Table of Contents

Preface

This document describes the installation, setup and use of the AG IHS Eligibility Letter update distributed in the local namespace (ZAG). This will later be incorporated into the national distribution as part of the RPMS Patient Registration (AG) package.

1.0 Introduction

In March 2010, President Obama signed comprehensive health reform, the Patient Protection and Affordable Care Act (ACA), into law. The law makes health care more accessible and affordable for many Americans. The ACA also requires that all non-exempt individuals must enroll in minimum essential (health benefits) coverage or pay the individual shared responsibility payment. However, patients who are members of federally recognized tribes are exempt from the payment, provided they file for an exemption with either the Marketplace or with the Internal Revenue Service (IRS).

In addition, individuals who are not members of a federally recognized Indian tribe, but who are eligible for services through an Indian health care provider, as defined in 42 CFR 447.50, or are eligible for services through the Indian Health Service in accordance with 25 U.S.C. 1680c(a), (b), or (d)(3), qualify for a hardship exemption. See 45 CFR 155.605(g)(6). These patients must apply for a hardship exemption and present documentation demonstrating such eligibility.

The IHS will assist patients in obtaining the hardship exemption by providing our patients with a letter acknowledging their eligibility for IHS services. The AG IHS Eligibility Letter update distributed in the local namespace (ZAG) is used to confirm a patient's eligibility for IHS services, print the letter proving eligibility, and later verify the legitimacy of the letter.

2.0 Installation

2.1 General Information

Before installing the AG IHS Eligibility Letter update, it is recommended that you print all Notes and Readme files associated with the patch. It is also recommended that you capture the terminal output during the installation using an auxport printer attached to the terminal at which you are performing the software installation. This will ensure a printed audit trail if any problems should arise.

The AG IHS Eligibility Letter update is distributed in the local namespace (ZAG). This is considered as a local enhancement/modification to the RPMS Patient Registration (AG) package. The enhancements in this update will be integrated into the national patch stream at a later date.

This patch adds the following functionality:

- Print IHS Eligibility Letter [AGACA PRINT]. This menu option allows printing of an Affordable Healthcare Act (ACA) Eligibility Letter to be used by patients seeking to document eligibility for IHS services.

  This menu option is locked with the security key: AGZACA PRINT

- Verify IHS Eligibility Letter [AGACA VERIFY]. This menu option allows the verification of the 21 digit (or longer) unique identifier printed at the bottom of each letter. The user will input the code provided by an entity seeking verification of the letter, and thereby determine the authenticity of the letter.

  This menu option is locked with the security key: AGZACA VERIFY

- The following security key has been added: AGZACA SIGN. This key needs to be assigned to one and only one user, typically the Service Unit Director (SUD) or Chief Executive Officer (CEO) of the facility, whose name will appear as the author of the printed AG IHS Eligibility Letters.

- Incoming file: AG ACA LOG FILE (#9009063.5)

  The AG ACA LOG file will be used to track/audit/verify all AG IHS Eligibility Letters printed by the site. This file will be view-only, preventing additions, modifications or deletions by the user.

2.2 Contents of Distribution

File	Description
zag_0710.11k	KIDS build
zag_0710.11n	Notes file
zag_0710.11o.pdf	Installation, Setup and User Guide

2.3 Requirements

The following KIDS must be installed:

- Kernel v8.0
- FM v22.0
- AG v7.1
- AVA v93.2
- AUPN v99.1

2.4 Installation Instructions

Follow these steps to install the AG IHS Eligibility Letter update:

1. Load the distribution into KIDS using option 1 on the Installation menu. The distribution was released in a file named **zag_0710.11k**.
2. Verify the load using option **2** on the Installation menu.
3. Consider using options **3** and **4** to print and compare the Transport.
4. Install the distribution using option **6** on the Installation menu.
5. For results, use the KIDS **Install File Print** option to view/print the "ZAG*7.1*11" entry.

2.5 After the Installation

After installing the KIDS build, perform the actions in the following sections to set up the AG IHS Eligibility Letter update for use.

2.5.1 Assign Print Menu Option and Security Key

Because this update is distributed in a local namespace, the menu options will need to be manually added to the users as secondary menu options.

1. Assign the AGACA PRINT secondary menu option and a synonym:

```
SECONDARY MENU OPTIONS: AGACA PRINT
               SYNONYM: ACA
```

2. Allocate the AGZACA PRINT security key:

```
Select Key Management Option: AKEY  Allocation of Security Keys

Allocate key: AGZACA PRINT
```

2.5.2 Assign Verify Menu Option and Security Key

Because this update is distributed in a local namespace, manually add the menu options to the users as secondary menu options.

1. Assign the AGACA VERIFY secondary menu option and a synonym:

```
SECONDARY MENU OPTIONS: AGACA VERIFY
               SYNONYM: ACAV
```

2. Allocate the AGZACA VERIFY security key:

```
Select Key Management Option: AKEY  Allocation of Security Keys

Allocate key: AGZACA VERIFY
```

2.5.3 Assign the Signature Security Key

The AGZACA SIGN security key is assigned to the authoritative person whose name will appear as the author of the AG IHS Eligibility Letter. Usually this will be the facility CEO or SUD. This key should be assigned to one user, and one user only. (If necessary, create a user for this.) The name of this user will be printed below the signature line as an additional level of verification.

The title field for the chosen user should be populated. This title will appear alongside the name of the user on all AG IHS Eligibility Letters generated by this update.

```
Select IHS Kernel Option: USER Management
Select User Management Option: EDIT an Existing User
Select NEW PERSON NAME:    ADMIN,SYSTEM                    CEO
                             Edit an Existing User
NAME: ADMIN,SYSTEM                                          Page 1 of 5
_____________________________________________________________________________
   NAME... ADMIN,SYSTEM                                  INITIAL:
    TITLE: CEO                                         NICK NAME:
```

1. Verify that no other users have been assigned the AGZACA SIGN key:

```
Select Key Management Option: LIST users holding a certain key

   Which key? AGZACA SIGN
```

```
There are no holders of this key.

Press RETURN to continue...
```

2. Assign the AGZACA SIGN key to the user whose name will appear on the AG IHS Eligibility Letters:

```
Select Key Management Option: AKEY  Allocation of Security Keys

Allocate key: AGZACA SIGN

Another key:

Holder of key: ADMIN,SYSTEM                    CEO

Another holder:

You've selected the following keys:

AGZACA SIGN

You've selected the following holders:

ADMIN,SYSTEM

You are allocating keys.  Do you wish to proceed? YES//

AGZACA SIGN being assigned to:
     ADMIN,SYSTEM
```

2.5.4 Populate the Phone Number Field in the Location File

The contact number printed in the AG IHS Eligibility Letter will be used to verify the authenticity of each letter printed by the Facility. For this reason, it is necessary to ensure the phone number associated with your Location is correct and included in the Location file:

```
Select VA FileMan Option: ENTER or Edit File Entries

INPUT TO WHAT FILE: LOCATION//
EDIT WHICH FIELD: ALL// PHONE
THEN EDIT FIELD:

Select LOCATION NAME: DEMO HOSPITAL       DEMO AREA       DEMO SU       01
                              NM  HOSPITAL  9999
         ...OK? Yes//   (Yes)

PHONE: 555-123-4567//
```

2.5.5 Printer Set Up for IHS/Facility Letterhead

The AG IHS Eligibility Letter is to be printed on IHS letterhead, or the appropriate official letterhead for your facility. Ensure that such a printer is set up at your facility and clearly identified to the users.

3.0 Operation

3.1 Introduction

The AG IHS Eligibility Letter may be printed for any person who seeks to document their eligibility for IHS services in order to support their application for a hardship exemption or related purpose as described in Section 1.0 above. Only patients who have been determined to be eligible for services from an Indian health care provider should receive the letter.

Due to the importance of this document, several mechanisms have been put in place to prevent forgeries and verify the authenticity of each letter. These range from automated patient eligibility checks to encrypted unique identifiers. Additionally, a log will be kept of each AG IHS Eligibility Letter printed along with key identifying information. The content of the AG IHS Eligibility Letters will be specific to a Facility, from the signing user to the generation of the encrypted identifiers.

> **Note:** There can only be one person per Facility designated as author of the AG IHS Eligibility Letter.

3.2 Printing an AG IHS Eligibility Letter

To print an AG IHS Eligibility Letter:

1. Log in to the correct division.
2. Enter the Print IHS Eligibility Letter [AGACA PRINT] secondary menu option:

```
You can also select a secondary option:

   ACA    Print IHS Eligibility Letter [AGACA PRINT]
             **> Locked with AGZACA PRINT

Select IHS Core Option: ACA  Print IHS Eligibility Letter
```

As mentioned earlier in this document, only one user can be assigned the AGZACA SIGN security key. The output displayed by the AGACA PRINT option will show whether a user has been correctly assigned.

- If a single user has been correctly assigned the appropriate key to author the letter, the following output will be displayed:

```
                            PATIENT REGISTRATION

                                DEMO HOSPITAL

                          Print IHS Eligibility Letter

   *** NOTE:  IF YOU EDIT A PATIENT AND SEE THEIR NAME IN REVERSE VIDEO ***
    *** WITH '(RHI)' BLINKING NEXT TO IT, IT MEANS THEY HAVE RESTRICTED ***
                           *** HEALTH INFORMATION ***

Printing of this letter is restricted to Individuals who are eligible for
services through an Indian health care provider as defined in 42 CFR 447.50
or is eligible for services through the Indian Health Service in accordance
with 25 USC 1680c(a), (b), or (d)(3).

Select PATIENT NAME:
```

- If no users have been assigned the appropriate key, this will display:

```
                            PATIENT REGISTRATION

                                DEMO HOSPITAL

                          Print IHS Eligibility Letter

   *** NOTE:  IF YOU EDIT A PATIENT AND SEE THEIR NAME IN REVERSE VIDEO ***
    *** WITH '(RHI)' BLINKING NEXT TO IT, IT MEANS THEY HAVE RESTRICTED ***
                           *** HEALTH INFORMATION ***

Printing of this letter is restricted to Individuals who are eligible for
services through an Indian health care provider as defined in 42 CFR 447.50
or is eligible for services through the Indian Health Service in accordance
with 25 USC 1680c(a), (b), or (d)(3).

<AG SIGN SECURITY KEY NOT ASSIGNED>
Press Enter to continue.:
```

- If more than one user has been assigned the appropriate key, this will display:

```
                            PATIENT REGISTRATION

                                DEMO HOSPITAL

                          Print IHS Eligibility Letter

   *** NOTE:  IF YOU EDIT A PATIENT AND SEE THEIR NAME IN REVERSE VIDEO ***
    *** WITH '(RHI)' BLINKING NEXT TO IT, IT MEANS THEY HAVE RESTRICTED ***
                           *** HEALTH INFORMATION ***

Printing of this letter is restricted to Individuals who are eligible for
services through an Indian health care provider as defined in 42 CFR 447.50
or is eligible for services through the Indian Health Service in accordance
with 25 USC 1680c(a), (b), or (d)(3).

<AG SIGN SECURITY KEY ASSIGNED TO MORE THAN ONE USER>
Press Enter to continue.:
```

3. After verifying a user has been assigned the AGZACA SIGN security key, enter and select the patient's name at the "Select PATIENT NAME" prompt.

```
Select PATIENT NAME: DEMO,PATIENT ONE
                                        M 01-01-1980 XXX-XX-9991    DH 9991
```

The output displayed will indicate whether the patient is eligible to receive the AG IHS Eligibility Letter:

- If the patient is an Indian/Alaska Native and receives Direct Only/CHS or Direct Only benefits, the following output will display:

```
Select PATIENT NAME: DEMO,PATIENT ONE
                                        M 01-01-1980 XXX-XX-9991    DH 9991
Press Enter to continue.:
```

- If the patient is not an Indian/Alaska Native, but still receives Direct Only/CHS or Direct Only benefits (such as Pregnant with Native American Child, or Adoptee), the following output will display:

```
Select PATIENT NAME: DEMO,PATIENT TWO
                                        F 01-01-1980 XXX-XX-9992    DH 9992

>>> Warning the patient you have selected is a NON-INDIAN BENEFICIARY,
>>> but listed as eligible for services.
>>> Are you sure you want to continue to print?
PROCEED TO PRINT LETTER ANYWAY (Y/N)? NO//
Press Enter to continue.:
```

- If the patient is not an Indian/Alaska Native, and Ineligible/Pending benefits, the following output will display:

```
Select PATIENT NAME: DEMO,PATIENT THREE
                                        M 01-01-1980 XXX-XX-9993    DH 9993

>>> Warning the patient you have selected is not eligible based on the
following information:
  CLASSIFICATION/BENEFICIARY : NON-INDIAN (FEE CHARGED)
          ELIGIBILITY STATUS : INELIGIBLE

Press Enter to continue.:
```

4. Print to the designated printer.

> **Note**: Be sure to select the printer designated for printing on IHS /Facility letterhead. Additionally, do not print the letter to your Home Device (computer screen), as this will be logged as a printed letter.

The following example shows the typical output sent to the designated printer:

```
Select PATIENT NAME: DEMO,PATIENT ONE
                                        M 01-01-1980 XXX-XX-9991    DH 9991
Press Enter to continue.:
```

```
DEVICE: HOME//   VT    Right Margin: 80//




<Date>

RE:       <First Middle Last Name>
          <Address line 1>
          <City, State  Zip>

Dear Federal or State Marketplace,

We have received a request to verify eligibility for Indian
Health Service (IHS) coverage for <First Middle Last Name>.

Upon review of our local facility data, we confirm that this
individual is an Indian eligible for services through an
Indian health care provider as defined by 42 CFR 447.50 or is
eligible for services through the Indian Health Service in
accordance with 25 USC 1680c(a), (b), or (d)(3). Eligibility
for such services under 42 CFR Part 136 has been verified at
the <Facility Name>
within the Indian Health Service <Area Prefix/Region> Area.

If you have any questions, please contact us at: <Facility Phone Number>

Sincerely,



<Signing User, Title>
<Facility Name>
<Area Prefix/Region> Area



UNIQUE IDENTIFIERS:
DOB: <Date of Birth>
SSN: <Last 4 of SSN>
<Unique Identifier>
```

3.3 Verifying an AG IHS Eligibility Letter

After the patient has delivered the AG IHS Eligibility Letter to the appropriate Federal or State Marketplace, you may be contacted to verify the authenticity of the letter. This is done with the AGACA VERIFY menu option.

To verify an AG IHS Eligibility Letter:

1. Log in to the correct division.
2. Enter the Verify IHS Eligibility Letter [AGACA VERIFY] secondary menu option:

```
You can also select a secondary option:
```

```
ACAV   Verify IHS Eligibility Letter [AGACA VERIFY]
            **> Locked with AGZACA VERIFY

Select IHS Core Option: ACAV  Verify IHS Eligibility Letter
```

3. Enter the unique identifier code given to you by the representative of the entity requesting verification:

```
                              PATIENT REGISTRATION

                                  DEMO HOSPITAL

                           Verify IHS Eligibility Letter


Verify the authenticity of a printed IHS Eligibility Letter by entering the
unique identifier code given to you by the representative of the entity
requesting verification.

** NOTE: The codes printed on the IHS Eligibility Letters are unique to **
** a facility and can only be verified at the site it was printed from. **

ENTER THE UNIQUE IDENTIFIER CODE (MINIMUM 21 DIGITS):
```

4. After entering the unique identifier code at the prompt, the results of the verification are displayed in three columns:

```
ENTER THE UNIQUE IDENTIFIER CODE (MINIMUM 21 DIGITS):
9UG089QXK2TW2772QJX387

                LETTER             RPMS                       RESULTS
                ------------       ------------               ------------
RECORD NUMBER:  22             ...  22                         PASSED
USER:           ADM,S          ...  ADMIN,SYSTEM              PASSED
DATE/TIME:      Sep 24, 2013   ...  Sep 24, 2013@09:34:11      PASSED
PT NAME:        DEM,P          ...  DEMO,PATIENT ONE           PASSED
PT DOB:         Jan 01, 1980   ...  Jan 01, 1980               PASSED
PT SSN:         XXX-XX-9991    ...  XXX-XX-9991                PASSED
Press Enter to continue.:
```

The three columns show the following information:

- LETTER – This column shows the information extracted from the AG IHS Eligibility Letter and used to create the unique identifier code.
- RPMS – This column shows the corresponding RPMS data used to compare with the information from the letter.
- RESULTS – This column shows whether the verification of that field passed or failed.

Any fields marked as FAILED will require manual verification.

- This example shows a case where the user at the facility has had a name change since the AG IHS Eligibility Letter was printed:

```
ENTER THE UNIQUE IDENTIFIER CODE (MINIMUM 21 DIGITS):
9UG089QXK2TW2772QJX387

                LETTER             RPMS                      RESULTS
                ------------       ------------              ------------
RECORD NUMBER:  22             ...  22                        PASSED
USER:           ADM,S          ...  ADMIN,LOCAL               FAILED ***
DATE/TIME:      Sep 24, 2013   ...  Sep 24, 2013@09:34:11     PASSED
PT NAME:        DEM,P          ...  DEMO,PATIENT ONE          PASSED
PT DOB:         Jan 01, 1980   ...  Jan 01, 1980              PASSED
PT SSN:         XXX-XX-9991    ...  XXX-XX-9991               PASSED
Press Enter to continue.:
```

- This example shows a case where the patient information on the letter does not match that stored in RPMS:

```
ENTER THE UNIQUE IDENTIFIER CODE (MINIMUM 21 DIGITS):
9UG089QXK2U1W332QJXX83

                LETTER             RPMS                      RESULTS
                ------------       ------------              ------------
RECORD NUMBER:  22             ...  22                        PASSED
USER:           ADM,S          ...  ADMIN,SYSTEM              PASSED
DATE/TIME:      Sep 24, 2013   ...  Sep 24, 2013@09:34:11     PASSED
PT NAME:        DEM,A          ...  DEMO,PATIENT ONE          FAILED ***
PT DOB:         Nov 30, 1950   ...  Jan 01, 1980              FAILED ***
PT SSN:         XXX-XX-0001    ...  XXX-XX-9991               FAILED ***
Press Enter to continue.:
```

- This example shows a case where the record number on the letter does not match a letter printed at this facility:

```
ENTER THE UNIQUE IDENTIFIER CODE (MINIMUM 21 DIGITS):
7UG086QXK26TW2772QJX387

                LETTER             RPMS                      RESULTS
                ------------       ------------              ------------
RECORD NUMBER:  100            ...  0                         FAILED ***
Press Enter to continue.:
```

Appendix A: Configuring Printer Settings for IHS Letterhead

The following is an example of the printer settings used for printing the AG IHS Eligibility Letter on IHS Letterhead. This is for use with a printer device defined in the RPMS device file.

A.1 Terminal Type Setup

Create a new terminal type entry or use an existing terminal type with changes to the following fields. The terminal type will be used in the SUBTYPE field in the DEVICE file.

In the following example a new terminal type was created called "P-IHSLTRHD".

```
Select TERMINAL TYPE NAME:    P-IHSLTRHD    LASER PRINTER IHS LETTERHEAD

NUMBER: 164                                 NAME: P-IHSLTRHD
  RIGHT MARGIN: 80                          FORM FEED: $C(12,13)
  PAGE LENGTH: 60                           BACK SPACE: $C(8)
  OPEN EXECUTE: H 1 W *27,"&l10E",*27,"&a10L",*27
  CLOSE EXECUTE: W *27,"E"
  DESCRIPTION: LASER PRINTER IHS LETTERHEAD
```

Note: The OPEN EXECUTE field defines how text is printed using PCL commands. The commands for your specific printer may vary.

A.1.1 Top Margin

The top margin setting designates number of lines between the top of the logical page and the top of text area.

```
? & l # E
```

= Number of lines

This command defines a top margin of 10 lines:

```
OPEN EXECUTE: H 1 W *27,"&l10E",*27,"&a10L",*27
```

A.1.2 Left Margin

This command sets the left margin to the left edge of the specified column:

```
? & a # L
```

= Column number

This command defines a left margin of 10 columns:

```
OPEN EXECUTE: H 1 W *27,"&l10E",*27,"&a10L",*27
```

A.2 Device File Examples

The following examples show a typical device setup for both Windows and AIX systems.

A.2.1 Windows Systems

```
NUMBER: 430                              NAME: OITPTR
  $I: |PRN|OITPTR                        ASK DEVICE: YES
  ASK PARAMETERS: YES                    VOLUME SET(CPU): OIT
  SIGN-ON/SYSTEM DEVICE: NO              LOCATION OF TERMINAL: OITHQ
  SUPPRESS FORM FEED AT CLOSE: YES       OPEN COUNT: 30
  SUBTYPE: P-IHSLTRHD                    TYPE: TERMINAL
```

A.2.2 AIX Systems

```
NUMBER: 436                              NAME: OITPTR
  $I: lp -doitptr                        ASK DEVICE: YES
  ASK PARAMETERS: NO                     VOLUME SET(CPU): EBCI
  LOCATION OF TERMINAL: OITHQ            SUPPRESS FORM FEED AT CLOSE: YES
  OPEN COUNT: 25                         OPEN PARAMETERS: "QW"
  SUBTYPE: P-IHSLTRHD                    TYPE: TERMINAL
```

Appendix B: 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: http://security.ihs.gov/.

The ROB listed in the following sections are specific to RPMS.

B.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).

B.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.

B.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.

B.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.

B.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.

B.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.

B.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).

B.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.

B.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.

B.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.

B.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.

B.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.

B.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.

B.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.

B.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.

B.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

ACA	Affordable Care Act
IHS	Indian Health Service
CEO	Chief Executive Officer
RPMS	Resource and Patient Management System
SUD	Service Unit Director

Contact Information

If you have any questions or comments regarding this distribution, please contact the OIT Help Desk (IHS).

Phone: (505) 248-4371 or (888) 830-7280 (toll free)

Fax: (505) 248-4363

Web: http://www.ihs.gov/GeneralWeb/HelpCenter/Helpdesk/index.cfm

Email: support@ihs.gov