RESOURCE AND PATIENT MANAGEMENT SYSTEM

IHS Personal Health Record

(BPHR)

Addendum to User Manual

Version 2.1 Patch 2
March 2018

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

Table of Contents

Preface

The purpose of this manual is to provide technical information about the IHS Personal Health Record (BPHR) package. The BPHR package contains an Application Programming Interface (API) call used by a Meaningful Use Performance Measure report and is also used to identify a selected patient’s DIRECT email address. The Web Service connections to the Personal Health Record (PHR) server are maintained in RPMS.

1.0 Introduction

The BPHR package creates classes used to communicate between RPMS and the PHR server. The BPHR package in RPMS sets up the communication information for two PHR web servers: a Training server and a Production server.

1.1 System Navigation

The BPHR package has one RPMS menu used by site managers: IHS Personal Health Record Management [BPHRMENU]. The menu contains the following options:

- **WEB** Edit PHR Web Service [BPHR EDIT WEB SERVICE]
- **CHK** Check the PHR connection [BPHR CHECK CONNECTION]
- **DIR** Check Patient for DIRECT Message [BPHR MU DIRECT CHECK]

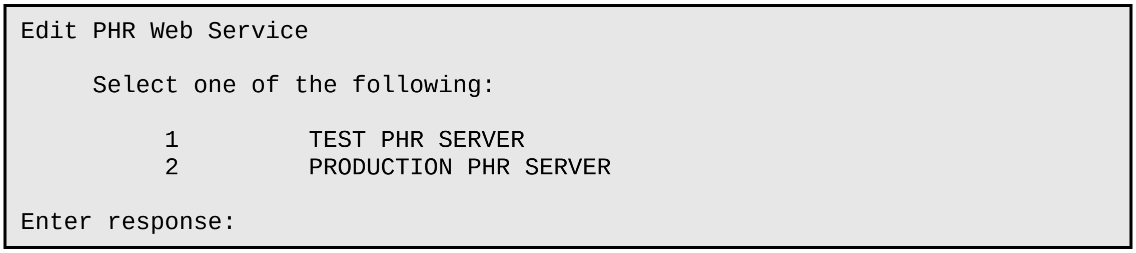
Site managers are responsible for updating the Web Service information as directed by the Office of Information Technology (OIT).

2.0 Package Management

2.1 Edit PHR Web Service

The RPMS option Edit PHR Web Service [BPHR EDIT WEB SERVICE] allows site managers to modify BPHR parameters if so directed by the PHR team. BPHR parameters will be released in the KIDS build but could need to be changed if the PHR team directs you. Note that this menu option is locked by security key BPHRZMENU.

There are two PHR server connections now.



```
Edit PHR Web Service

     Select one of the following:

          1          TEST PHR SERVER
          2          PRODUCTION PHR SERVER

Enter response:
```

Figure 2-1: PHR server connection options

The following ten parameters can be edited using this option:

1. URL ROOT
2. PORT NUMBER
3. TIMEOUT OVERRIDE
4. USERNAME
5. PASSWORD
6. SERVICE PATH
7. SSL/TLS CONFIGURATION
8. CONNECTION TIMEOUT OVERRIDE
9. RETRIES ON FAILURE
10. MAXIMUM FAILURES

Again, these values should not be changed unless directed by the Office of Information Technology (OIT) or the PHR team.

“URL ROOT” is the first prompt and the DNS identifier for the PHR web server endpoint. Use name instead of IP address.

The second prompt is “PORT NUMBER” and is the port number used to connect to the PHR server.

“TIMEOUT OVERRIDE” is the number of seconds for timing out of the connection if no response is received.

“USERNAME” and “PASSWORD” are the PHR system-specific username and password needed to connect to the PHR server.

The “SERVICE PATH” is part of the URL that forms the rest of the address for reaching the PHR web service.

The “SSL/TLS CONFIGURATION” contains the cryptographic settings (the Protocols and Enabled cipher suites) that are used when making a secure connection to the MU2 PHR Performance Portal to retrieve report data.

The **CONNECTION TIMEOUT OVERRIDE**, the **RETRIES ON FAILURE**, and the **MAXIMUM FAILURES** fields enable the API to retry if the network connection is slow, instead of failing outright.

2.2 Check the PHR Connection

The RPMS option Check the PHR connection [BPHR CHECK CONNECTION] allows site managers to check if the PHR connection is working.

The first thing the prompt will inform is if the current RPMS database is defined as a TEST or a PRODUCTION system. It is important to correctly identify the database so that it is known if the connection is to the PHR test server or the PHR live server.

```
Select IHS Personal Health Record Management <TEST ACCOUNT> Option: CHK  Check the
PHR connection
This system has been designated as a TEST system. Is this correct? YES
```

Figure 2-2: Check the PHR connection

If the RPMS database is not correctly identified, please contact the IHS Help Desk and request a HEAT ticket to be created so this can be corrected.

```
This system has been designated as a TEST system. Is this correct? NO
Please contact the IHS HELP desk for this issue.
```

Figure 2-3: Contact the Help Desk if the database is not correctly designated

If this RPMS database is a multi-divisional database, each pertinent location must have a DIRECT email address defined. If the location currently signed on for does not have a DIRECT email address, a message will display.

```
Location 2016 DEMO HOSPITAL does not have DIRECT email address.
```

Figure 2-4: Message if location does not have DIRECT email account

The next prompt will be for a patient name. If the patient does not have a unique Master Patient Index (MPI) identification (EUID), please select another patient for testing the connection.

```
This system has been designated as a TEST system. Is this correct? YES
Select PATIENT NAME: DEMO,AMY
                                        F 11-27-2015 XXX-XX-6666    DB 123
Patient does not have an MPI EUID
```

Figure 2-5: Patient does not have an MPI EUID

An error message should display if the connection is unable to be established.

```
This system has been designated as a TEST system. Is this correct? YES
Select PATIENT NAME:  PATIENT,CHRISTINA             F 02-28-1959 XXX-XX-5763    DB
100018
ERROR #6059: Unable to open TCP/IP socket to server hqabqdittphrw01.d1.na.ihs.gov
```

Figure 2-6: Unable to connect error message

2.3 Check Patient for DIRECT Message

To check a patient for DIRECT messages, many of the same prompts and responses in Section 2.2 also apply. Before the prompt for PATIENT NAME, the specific additional prompts for this option are for PROVIDER and the report date range.

The Beginning Date and Ending Date are for the report period. The API checks for the calendar year of the report period. It will list the Messaging Agents for the Calendar Year.

Figure 2-7 shows an example of a patient who received a DIRECT message during the Calendar Year.

```
Enter the name of the provider.
Enter PROVIDER NAME:    DOCTOR,DUANE MD     DR          PHYSICIAN

Enter Beginning Date:  1/1/2017  (JAN 01, 2017)
Enter Ending Date:  3/1/2017  (MAR 01, 2017)
     Report Calendar Year is Jan 01, 2017-Dec 31, 2017

Select PATIENT NAME: DEMO,DUGAN <A>   M 07-21-1965 XXX-XX-2845   TST 107889

     Patient last accessed PHR during Calendar Year Nov 27, 2017@08:40:10

     Patient has a DIRECT email address
     Patient's last DIRECT message during Calendar Year was Jan 04, 2017@08:27:21

     Patient's Message Agents for Calendar Year Jan 01, 2017-Dec 31, 2017 are:
       lisa.demo@direct.ihs.gov Jul 21, 2016 - Nov 02, 2017
       linda.demo@direct.ihs.gov Nov 02, 2017 - Dec 08, 2017
       lisa.demo@direct.ihs.gov Dec 08, 2017 - Mar 12, 2018
```

Figure 2-7: Patient who received DIRECT message during calendar year.

Figure 2-8 and Figure 2-9 show examples in the case the patient did not receive a DIRECT message for the Calendar Year.

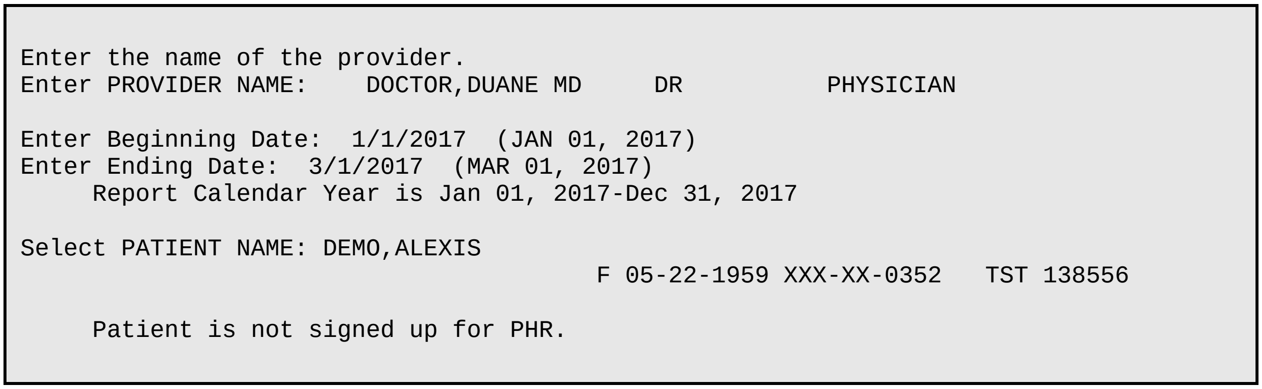
```
Enter the name of the provider.
Enter PROVIDER NAME:    DOCTOR,DUANE MD     DR         PHYSICIAN

Enter Beginning Date:  1/1/2018  (JAN 01, 2018)
Enter Ending Date:  3/1/2018  (MAR 01, 2018)
     Report Calendar Year is Jan 01, 2018-Dec 31, 2018

Select PATIENT NAME: DEMO,DUGAN <A>   M 07-21-1965 XXX-XX-2845   TST 107889

     Patient last accessed PHR during Calendar Year Feb 23, 2018@01:26:22

     Patient has a DIRECT email address

     Patient does not have a record of a DIRECT message.

     Patient's Message Agents for Calendar Year Jan 01, 2018-Dec 31, 2018 are:
       lisa.demo@direct.ihs.gov Dec 08, 2017 - Mar 12, 2018
```

Figure 2-8: Patient does not have record of DIRECT message

```
Enter the name of the provider.
Enter PROVIDER NAME:    DOCTOR,DUANE MD     DR         PHYSICIAN

Enter Beginning Date:  1/1/2016  (JAN 01, 2016)
Enter Ending Date:  3/1/2016  (MAR 01, 2016)
     Report Calendar Year is Jan 01, 2016-Dec 31, 2016

Select PATIENT NAME: DEMO,DUGAN    <A>   M 07-21-1965 XXX-XX-2845   TST 107889

     Patient last accessed PHR during Calendar Year Dec 15, 2016@08:01:17

     Patient has a DIRECT email address

     Patient's last DIRECT message during Calendar Year was Dec 12, 2016@14:30:38

     Patient's Message Agents for Calendar Year Jan 01, 2016-Dec 31, 2016 are:
       meghna.demo@direct.ihs.gov Apr 19, 2016 - Jul 21, 2016
       lisa.demo@direct.ihs.gov Jul 21, 2016 - Nov 02, 2017
```

Figure 2-9: Patient does not have record of DIRECT message for Calendar Year

Figure 2-10 shows an example of a patient who is not signed up.

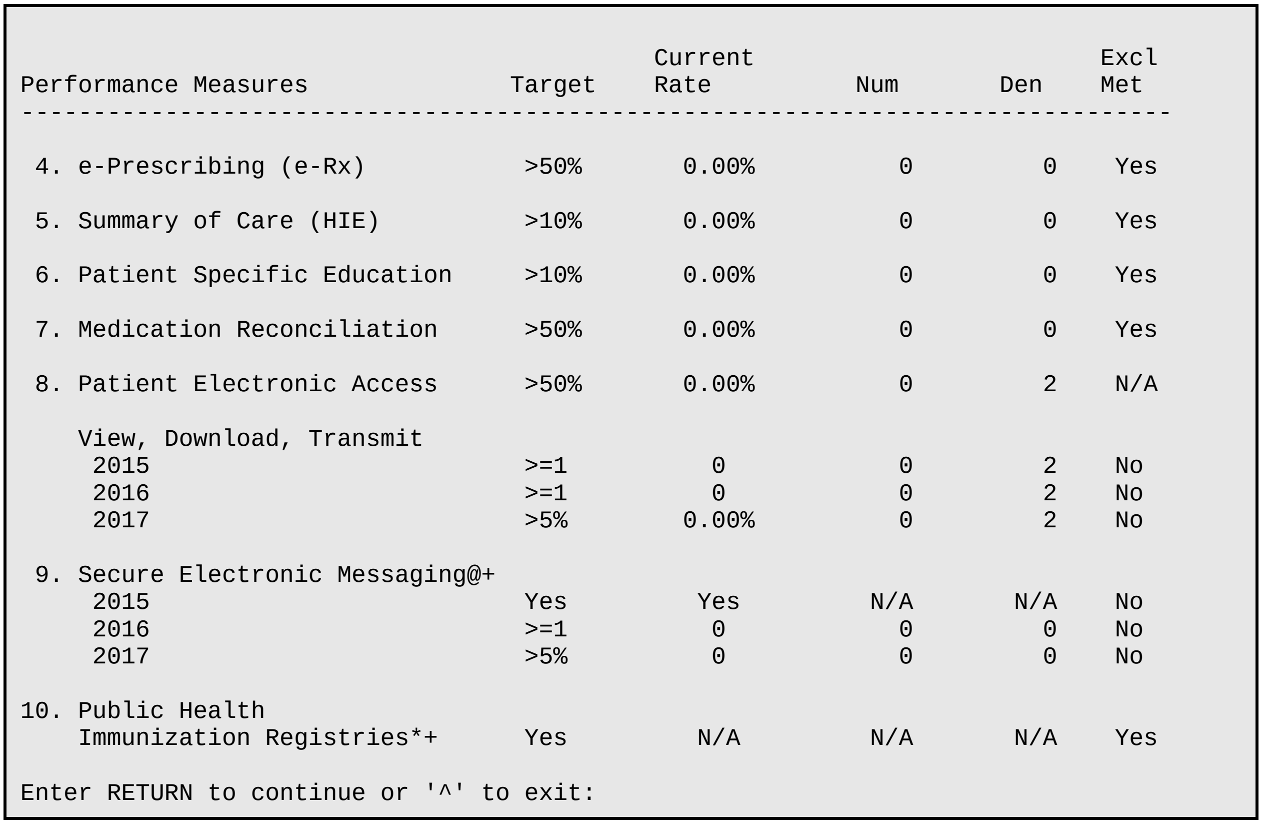


```
Enter the name of the provider.
Enter PROVIDER NAME:    DOCTOR,DUANE MD     DR          PHYSICIAN

Enter Beginning Date:  1/1/2017  (JAN 01, 2017)
Enter Ending Date:  3/1/2017  (MAR 01, 2017)
     Report Calendar Year is Jan 01, 2017-Dec 31, 2017

Select PATIENT NAME: DEMO,ALEXIS
                                        F 05-22-1959 XXX-XX-0352   TST 138556

     Patient is not signed up for PHR.
```

Figure 2-10: Example of patient who is not signed up for PHR

3.0 Package Operation

Currently BPHR is used to communicate to the PHR server to obtain information about PHR usage for Performance Measure — Patient Electronic Access.



```
                                          Current                       Excl
Performance Measures              Target    Rate          Num       Den    Met
-------------------------------------------------------------------------------

 4. e-Prescribing (e-Rx)           >50%       0.00%         0         0    Yes

 5. Summary of Care (HIE)          >10%       0.00%         0         0    Yes

 6. Patient Specific Education     >10%       0.00%         0         0    Yes

 7. Medication Reconciliation      >50%       0.00%         0         0    Yes

 8. Patient Electronic Access      >50%       0.00%         0         2    N/A

    View, Download, Transmit
     2015                          >=1          0           0         2    No
     2016                          >=1          0           0         2    No
     2017                          >5%        0.00%         0         2    No

 9. Secure Electronic Messaging@+
     2015                          Yes         Yes         N/A       N/A   No
     2016                          >=1          0           0         0    No
     2017                          >5%          0           0         0    No

10. Public Health
    Immunization Registries*+      Yes         N/A         N/A       N/A   Yes

Enter RETURN to continue or '^' to exit:
```

Figure 3-1: Performance Measures

The Performance Measure code calls an API in BPHR to return information for the two measures in the report: Patient Electronic Access and Secure Electronic Messaging.

The **DIRECT Mail** button in EHR also calls the API to obtain the selected patient’s DIRECT email address if they have enrolled in PHR.

An RPMS patient must have an Unique ID (UID) assigned by the Master Patient Index (MPI) and have signed up to use PHR in order for any results to be returned to the report.

The information returned by the API is as follows:

- Patient signed up for PHR (0 = No; 1 = Yes)
- The date the patient signed up for PHR
- Patient accessed PHR (0 = No; 1 = Yes)

- The last date the patient accessed PHR
- Patient used secure messaging (0 = No; 1 = Yes)
- The last date the patient used secure messaging
- The patient’s DIRECT email address

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.

In accordance IHS policy 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.

- 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 the *IHS General User Security Handbook* and *IHS Technical and Managerial Handbook* are available at this IHS Web site: http://security.ihs.gov/.

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

A.1 All RPMS Users

In addition to these rules, each application may include additional ROBs that may be defined within the documentation of that application (e.g., Dental, Pharmacy).

A.1.1 Access

RPMS users shall:

- Only use data for which the users 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 a user’s 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.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 the users created and those other documents to which the users have a valid need to know and to which the users 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 PCs.
- Be alert to threats and vulnerabilities in the security of the system.
- Report all security incidents to the user’s 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 the users as part of the users’ government employment.

- Abide by all DHHS and IHS 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 hardcopy 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 encryption.

A.1.5 Integrity

RPMS users shall:

- Protect users’ 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 the user’s manager’s written permission and without first scanning it for viruses.

A.1.6 System Logon

RPMS users shall:

- Have a unique User Identification/Account name and password.
- Be granted access based on authenticating the account name and password entered.
- Be locked out of an account after five successive failed login attempts within a specified time period (e.g., one hour).

A.1.7 Passwords

RPMS users shall:

- Change passwords a minimum of every 90 days.
- Create passwords with a minimum of eight characters.
- If the system allows, use a combination of alpha-numeric characters for passwords, with at least one uppercase letter, one lower case letter, and one number. It is recommended, if possible, that a special character also be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or storing 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 the users' 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 the users’ ISSO of 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 five minutes of inactivity.

RPMS users shall:

- Utilize a screen saver with password protection set to suspend operations at no greater than ten minutes of inactivity—which will prevent inappropriate access and viewing of any material displayed on the screen after some period of inactivity.

A.1.11 Hardware

RPMS users shall:

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).
- Keep an inventory of all system equipment.

- Keep records of maintenance/repairs performed on system equipment.

RPMS users shall not

- Eat or drink near system equipment.

A.1.12 Awareness

RPMS users shall:

- Participate in organization-wide security training as required.
- Read and adhere to security information pertaining to system hardware and software.
- Take the annual information security awareness.
- Read all applicable RPMS manuals for the applications used in the users' 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 non-recovery 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.
- Justify and approve in writing the use of direct dial in access 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 the developers have been assigned as part of the developers' duties.
- Remember that all RPMS code is the property of the U.S. Government, not the developers'.
- 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, including the programmer's initials, date of change, and reason for the change.
- Use checksums or other integrity mechanism when releasing certified applications to assure the integrity of the routines within their RPMS applications.
- Follow industry best standards for assigned systems to develop or maintain.
- 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, super user, or system administrator passwords.
- Avoid instances where the same individual has responsibility for several functions (e.g., 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--either in person or have the user answer a question that can be compared to one in the administrator’s database.
- Follow industry best standards for assigned systems 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 privileged RPMS users’ duties
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

Glossary

Web Service

An application programming interface (API) that allows communication with an application via SOAP messages over HTTP.

Acronym List

Acronym	Term Meaning
API	Application Programmer Interface
HHS	Health and Human Services
IHS	Indian Health Service
ISSO	Information System Security Officer
IT	Information Technology
KIDS	Kernel Installation and Distribution
MPI	Master Patient Index
OIT	Office of Information Technology
PC	Personal Computer
PHR	Personal Health Record
ROB	Rules of Behavior
RPMS	Resource and Patient Management System
UID	Unique ID

Contact Information

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

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

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

Email: support@ihs.gov