RESOURCE AND PATIENT MANAGEMENT SYSTEM

IHS Clinical Quality Mapping

(BCQM)

User Manual

Version 1.0 Patch 12
January 2025

Office of Information Technology
Division of Information Resource Management

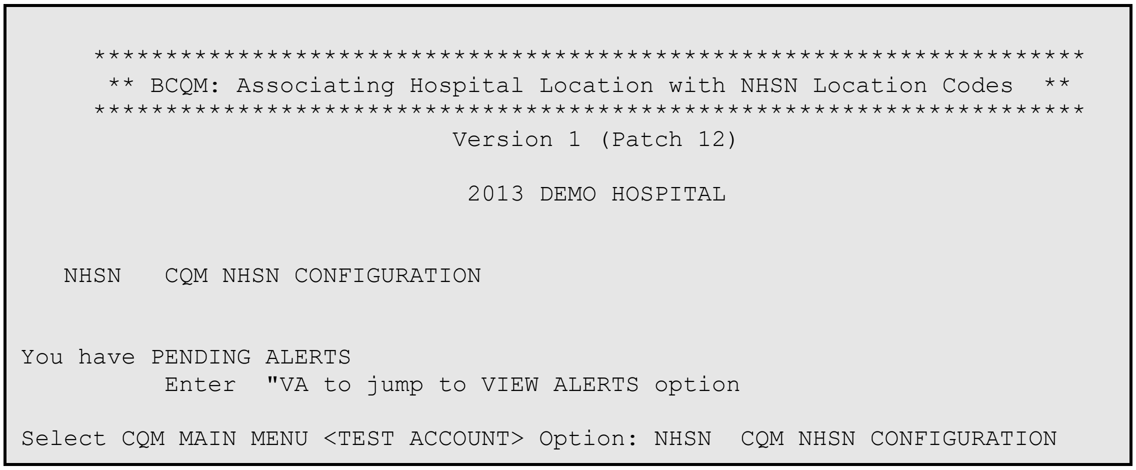
Table of Contents

1.0 Introduction

The BCQM v1.0 p12 release delivers updated work needed to prepare the electronic Clinical Quality Measures (eCQMs) for the 2024 CMS Reporting Period. eCQMs are tools that help measure and track the quality of healthcare services that eligible clinicians (EC), eligible hospitals (EH), and critical access hospitals (CAH) provide. Measuring and reporting eCQMs helps to ensure that our healthcare system is delivering effective, safe, efficient, patient-centered, equitable, and timely care. This BCQM patch release will also support local quality improvement activities by updating the product to 2024 version and maintaining the Office of the National Coordinator for Health Information Technology (ONC) Certification Criteria for Health IT necessary for participating in various Centers for Medicare and Medicaid Services (CMS) Programs. This criterion includes: IHS Code Mapping, local installation used by inpatient and outpatient facilities, used during data entry to translate the value sets used by RPMS to value sets recognized by CQM. Maps ICD-10, CPT, and HCPCS codes on SNOMED and LOINC codes recognized by the measure.

2.0 CQM Main Menu Option

The clinical quality measure (CQM) is security key restricted. The options from the main menu are shown on the following page. A brief description of each option follows.



```
     *********************************************************************
      ** BCQM: Associating Hospital Location with NHSN Location Codes  **
     *********************************************************************
                              Version 1 (Patch 12)

                               2013 DEMO HOSPITAL


   NHSN   CQM NHSN CONFIGURATION


You have PENDING ALERTS
          Enter  "VA to jump to VIEW ALERTS option

Select CQM MAIN MENU <TEST ACCOUNT> Option: NHSN  CQM NHSN CONFIGURATION
```

Figure 2-1: Main menu for Clinical Quality Measure (CQM)

2.1 NHSN–National Health Safety Network

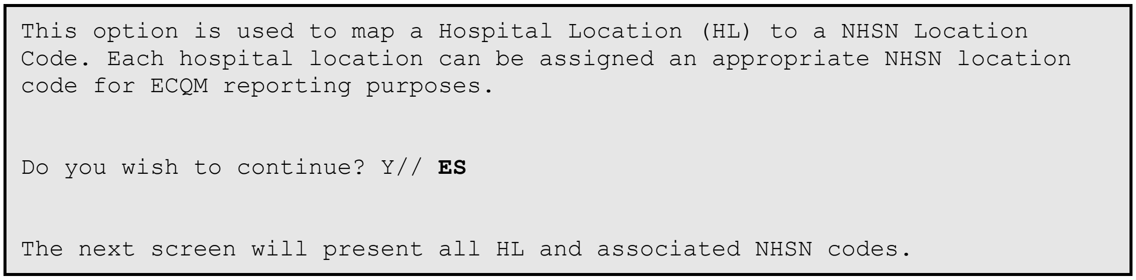
The **NHSN** option is used to map a Hospital Location (HL) to a NHSN Location Code. Each hospital location can be assigned an appropriate NHSN location code for ECQM measure reporting purposes.

NHSN Resources for users, if needed:

NHSN Chapter 15 CDC Location Labels and Location Descriptions:

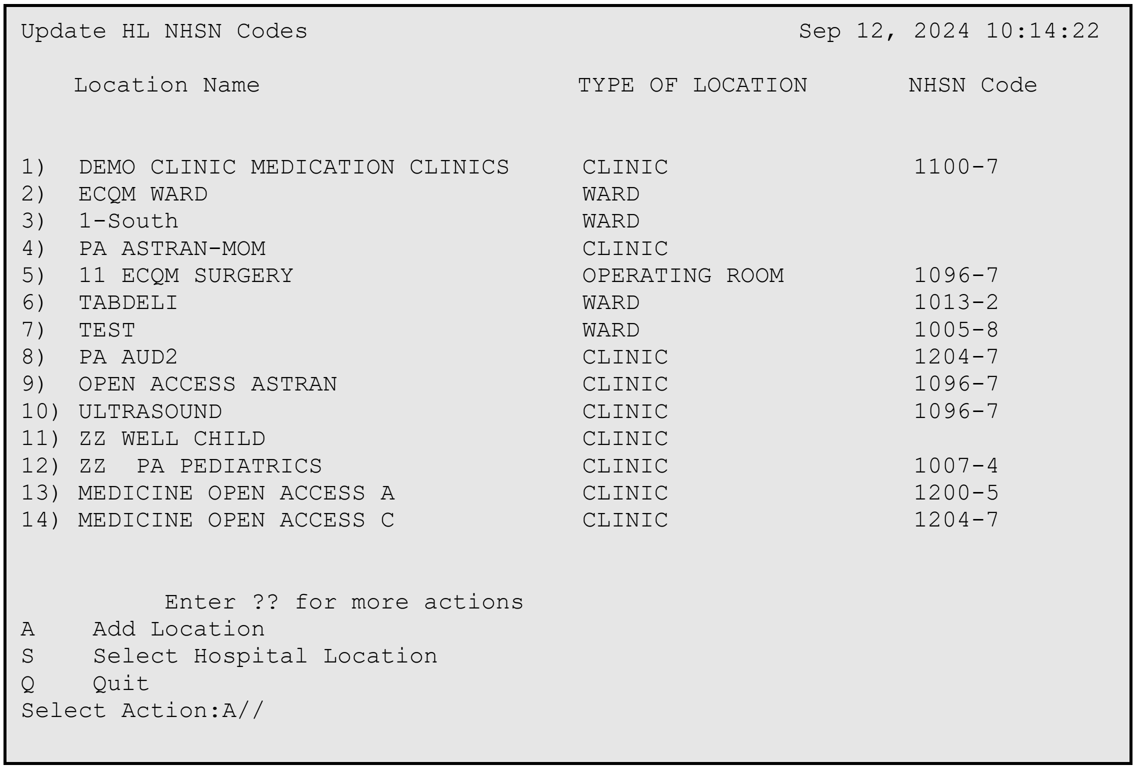
https://www.cdc.gov/nhsn/pdfs/pscmanual/15locationsdescriptions_current.pdf
NHSN CDA Submission Portal–Code System: HSLOC

https://www.cdc.gov/nhsn/cdaportal/terminology/codesystem/hsloc.html



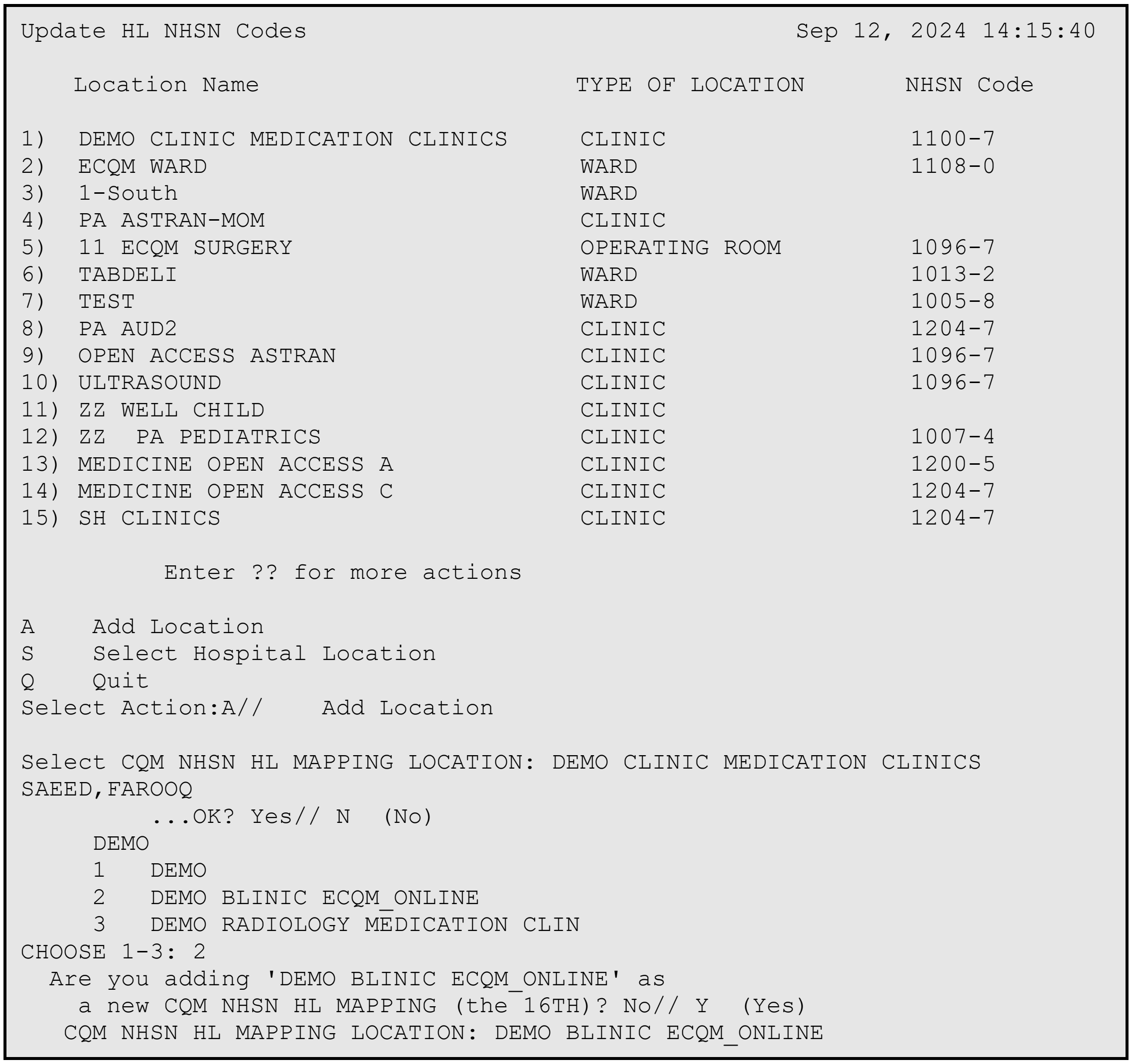
```
This option is used to map a Hospital Location (HL) to a NHSN Location
Code. Each hospital location can be assigned an appropriate NHSN location
code for ECQM reporting purposes.


Do you wish to continue? Y// ES


The next screen will present all HL and associated NHSN codes.
```

Figure 2-2: Sample Interaction to Update to map a HL to a NHSN Location Code



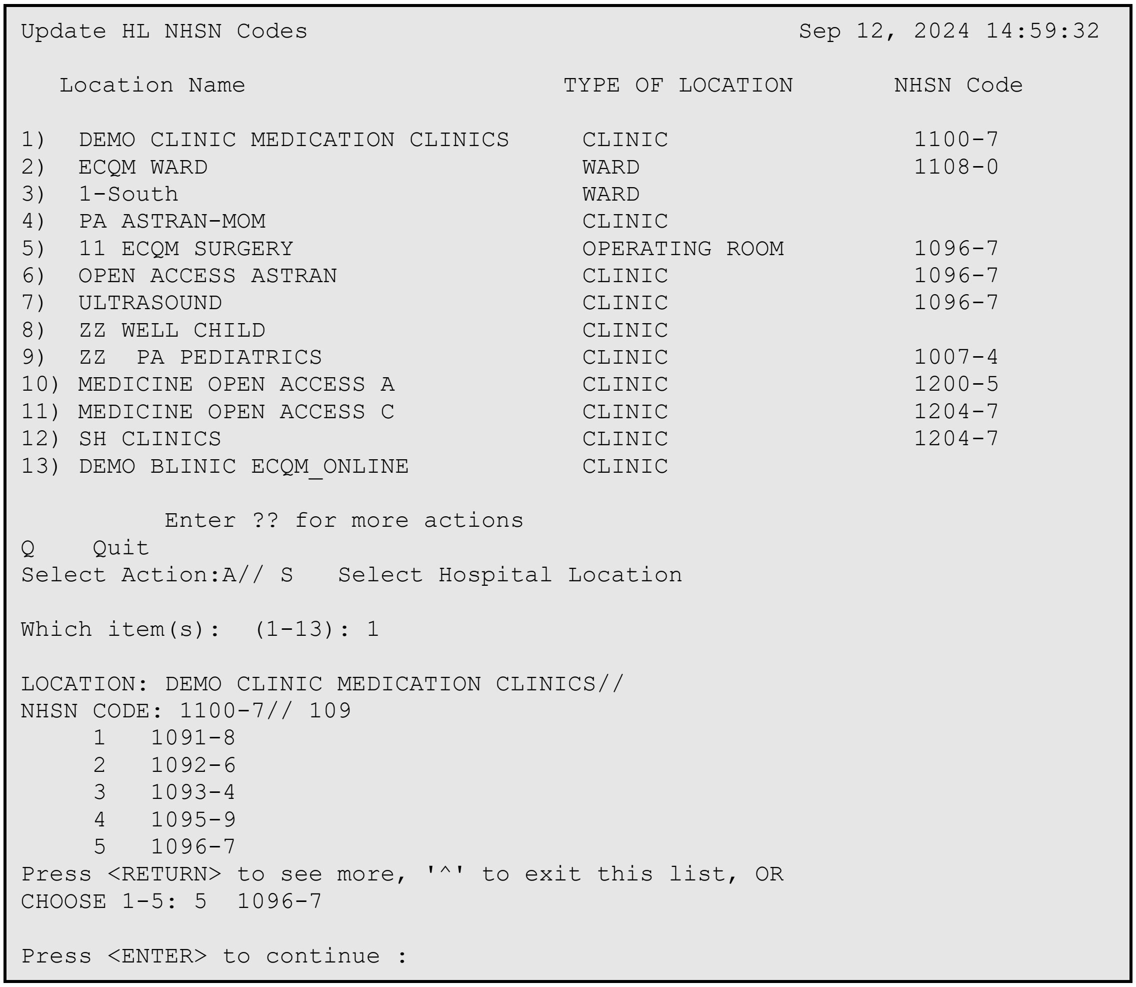
```
Update HL NHSN Codes                                    Sep 12, 2024 10:14:22

   Location Name                      TYPE OF LOCATION       NHSN Code


1)  DEMO CLINIC MEDICATION CLINICS     CLINIC                 1100-7
2)  ECQM WARD                          WARD
3)  1-South                            WARD
4)  PA ASTRAN-MOM                      CLINIC
5)  11 ECQM SURGERY                    OPERATING ROOM         1096-7
6)  TABDELI                            WARD                   1013-2
7)  TEST                               WARD                   1005-8
8)  PA AUD2                            CLINIC                 1204-7
9)  OPEN ACCESS ASTRAN                 CLINIC                 1096-7
10) ULTRASOUND                         CLINIC                 1096-7
11) ZZ WELL CHILD                      CLINIC
12) ZZ  PA PEDIATRICS                  CLINIC                 1007-4
13) MEDICINE OPEN ACCESS A             CLINIC                 1200-5
14) MEDICINE OPEN ACCESS C             CLINIC                 1204-7


          Enter ?? for more actions
A    Add Location
S    Select Hospital Location
Q    Quit
Select Action:A//
```

Figure 2-3: Listing of Hospital Locations Mapped to NHSN Location Codes



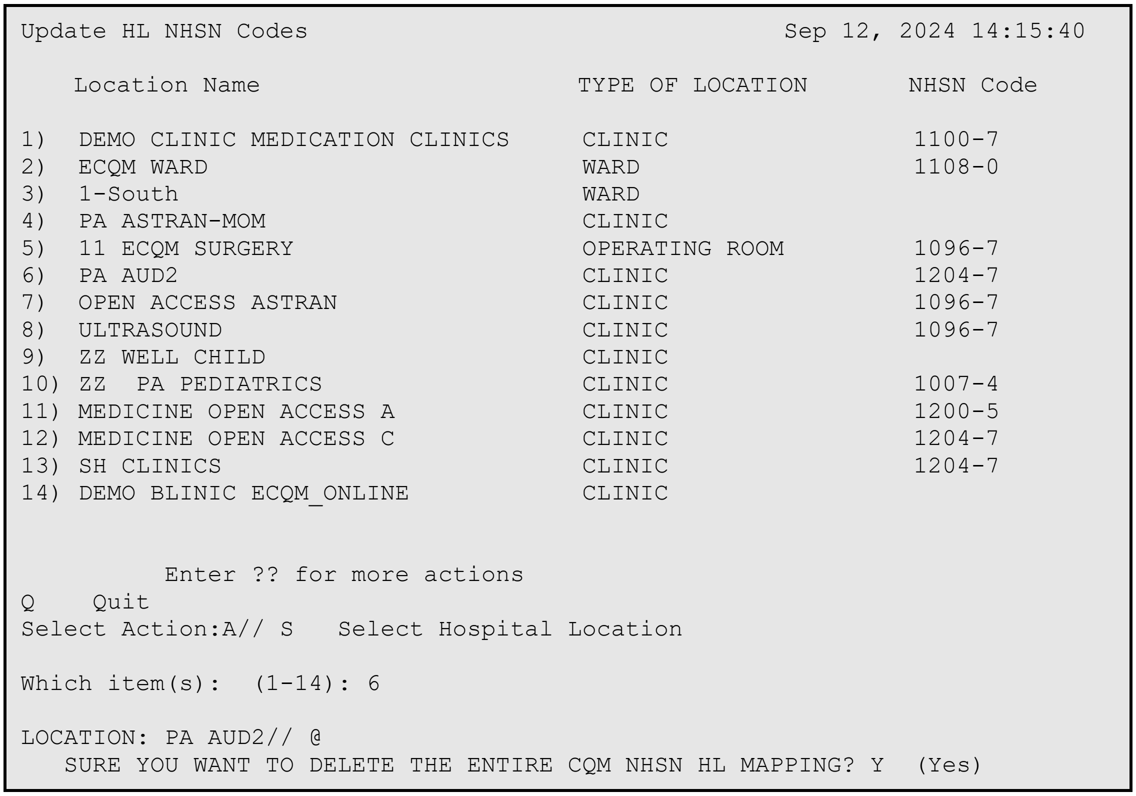
```
Update HL NHSN Codes                                    Sep 12, 2024 14:15:40

    Location Name                          TYPE OF LOCATION       NHSN Code

1)  DEMO CLINIC MEDICATION CLINICS         CLINIC                 1100-7
2)  ECQM WARD                              WARD                   1108-0
3)  1-South                                WARD
4)  PA ASTRAN-MOM                          CLINIC
5)  11 ECQM SURGERY                        OPERATING ROOM         1096-7
6)  TABDELI                                WARD                   1013-2
7)  TEST                                   WARD                   1005-8
8)  PA AUD2                                CLINIC                 1204-7
9)  OPEN ACCESS ASTRAN                     CLINIC                 1096-7
10) ULTRASOUND                             CLINIC                 1096-7
11) ZZ WELL CHILD                          CLINIC
12) ZZ  PA PEDIATRICS                      CLINIC                 1007-4
13) MEDICINE OPEN ACCESS A                 CLINIC                 1200-5
14) MEDICINE OPEN ACCESS C                 CLINIC                 1204-7
15) SH CLINICS                             CLINIC                 1204-7

          Enter ?? for more actions

A    Add Location
S    Select Hospital Location
Q    Quit
Select Action:A//    Add Location

Select CQM NHSN HL MAPPING LOCATION: DEMO CLINIC MEDICATION CLINICS
SAEED,FAROOQ
         ...OK? Yes// N  (No)
     DEMO
     1   DEMO
     2   DEMO BLINIC ECQM_ONLINE
     3   DEMO RADIOLOGY MEDICATION CLIN
CHOOSE 1-3: 2
  Are you adding 'DEMO BLINIC ECQM_ONLINE' as
    a new CQM NHSN HL MAPPING (the 16TH)? No// Y  (Yes)
   CQM NHSN HL MAPPING LOCATION: DEMO BLINIC ECQM_ONLINE
```

Figure 2-4: Add Hospital Location for NHSN Location Code Assignment



```
Update HL NHSN Codes                                       Sep 12, 2024 14:59:32

   Location Name                           TYPE OF LOCATION       NHSN Code

1)  DEMO CLINIC MEDICATION CLINICS     CLINIC                   1100-7
2)  ECQM WARD                          WARD                     1108-0
3)  1-South                            WARD
4)  PA ASTRAN-MOM                      CLINIC
5)  11 ECQM SURGERY                    OPERATING ROOM           1096-7
6)  OPEN ACCESS ASTRAN                 CLINIC                   1096-7
7)  ULTRASOUND                         CLINIC                   1096-7
8)  ZZ WELL CHILD                      CLINIC
9)  ZZ  PA PEDIATRICS                  CLINIC                   1007-4
10) MEDICINE OPEN ACCESS A             CLINIC                   1200-5
11) MEDICINE OPEN ACCESS C             CLINIC                   1204-7
12) SH CLINICS                         CLINIC                   1204-7
13) DEMO BLINIC ECQM_ONLINE            CLINIC

          Enter ?? for more actions
Q    Quit
Select Action:A// S   Select Hospital Location

Which item(s):  (1-13): 1

LOCATION: DEMO CLINIC MEDICATION CLINICS//
NHSN CODE: 1100-7// 109
     1   1091-8
     2   1092-6
     3   1093-4
     4   1095-9
     5   1096-7
Press <RETURN> to see more, '^' to exit this list, OR
CHOOSE 1-5: 5  1096-7

Press <ENTER> to continue :
```

Figure 2-5: NHSN Location Code Assignment



```
Update HL NHSN Codes                                     Sep 12, 2024 14:15:40

   Location Name                           TYPE OF LOCATION       NHSN Code

1)  DEMO CLINIC MEDICATION CLINICS         CLINIC                 1100-7
2)  ECQM WARD                              WARD                   1108-0
3)  1-South                                WARD
4)  PA ASTRAN-MOM                          CLINIC
5)  11 ECQM SURGERY                        OPERATING ROOM         1096-7
6)  PA AUD2                                CLINIC                 1204-7
7)  OPEN ACCESS ASTRAN                     CLINIC                 1096-7
8)  ULTRASOUND                             CLINIC                 1096-7
9)  ZZ WELL CHILD                          CLINIC
10) ZZ  PA PEDIATRICS                      CLINIC                 1007-4
11) MEDICINE OPEN ACCESS A                 CLINIC                 1200-5
12) MEDICINE OPEN ACCESS C                 CLINIC                 1204-7
13) SH CLINICS                             CLINIC                 1204-7
14) DEMO BLINIC ECQM_ONLINE                CLINIC


          Enter ?? for more actions
Q    Quit
Select Action:A// S   Select Hospital Location

Which item(s):  (1-14): 6

LOCATION: PA AUD2// @
   SURE YOU WANT TO DELETE THE ENTIRE CQM NHSN HL MAPPING? Y  (Yes)
```

Figure 2-6: Delete Hospital Location for NHSN Location Code Assignment

Appendix A Rules of Behavior

The Resource and Patient Management (RPMS) system is an information system operated by the United States Department of Health and Human Services (HHS) and the Indian Health Service (IHS) that is FOR OFFICIAL USE ONLY. The RPMS system is monitored; therefore, no expectation of privacy shall be assumed. Individuals found performing unauthorized activities are subject to disciplinary action, including criminal prosecution.

In accordance with IHS policy, all RPMS users (Contractors and IHS Employees) will be provided a copy of the Rules of Behavior (ROB) and must acknowledge that they have received and read them before being granted access to an RPMS system.

- For a listing of general ROB for all users, see the most recent edition of the 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 on this IHS Website: https://home.ihs.gov/security/index.cfm.

> **Note**: Users must be logged on to the IHS D1 Intranet to access these documents.

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

A.1 All RPMS Users

In addition to these rules, each application may include additional ROBs that may be defined within that application's documentation (e.g., dental, pharmacy).

A.1.1 Access

RPMS users shall:

- Only use data for which you have been granted authorization.
- Only give information to personnel who have access authority and have a need to know.
- Always verify a caller’s identification and job purpose with your supervisor or the entity provided as an employer before providing any information system access, sensitive or nonpublic agency information.

- Be aware that personal use of information resources is authorized on a limited basis within the provisions of 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 the 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, 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 their functions, such as system administrator or application administrator.
- Acquire a written preauthorization in accordance with IHS policies and procedures before interconnection to or transferring data from RPMS.

A.1.3 Accountability

RPMS users shall:

- Behave ethically, technically proficient, informed, and trustworthy.
- 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 person has sole access to or control of important resources.
- Protect all sensitive data entrusted to them as part of their government employment.
- Abide by all Department and Agency policies, 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 before 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 not authorized to access that data is nearby.
- 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.

- Users may not use freeware, shareware, or public domain software on/with the system without their 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 lowercase letter, and one number. If possible, it is recommended that a special character be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or storing them safely (do not store passwords in login scripts or batch files).
- Change passwords immediately if the 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 using 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.2 Session Timeouts

The RPMS system implements system-based timeouts, which allow users to exit a prompt after 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.2.1 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.2.2 Awareness

RPMS users shall:

- Participate in organization-wide security training as required.
- Read and adhere to security information pertaining to system hardware and software.
- Take the annual information security awareness.
- Read all applicable RPMS manuals for the applications used in their jobs.

A.2.3 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 remote user authentication through ID and password or other acceptable technical means.
- Outline the work requirements, security safeguards, and procedures the employee must 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. 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.2.4 RPMS Developers

RPMS developers shall:

- When writing or revising code, always remember to protect the confidentiality, availability, and integrity of RPMS.
- Always follow the IHS RPMS Programming Standards and Conventions (SAC) when developing RPMS.
- Only access information or code within the namespaces 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 the separation of duties, policies, and procedures to the fullest extent possible.
- Document or comment on all changes to any RPMS software when the change or update is made. Documentation shall include the programmer’s initials, change date, and reason for the change.
- Checksums or other integrity mechanisms should be used when releasing their certified applications to ensure the integrity of the routines within their RPMS applications.
- Follow industry best standards for systems assigned to develop, 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.2.5 Privileged Users

Personnel with significant access to processes and data in RPMS, such as system security administrators, systems administrators, and database administrators, have added responsibilities to ensure its secure operation.

Privileged RPMS users shall:

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government 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 is responsible 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 system's accountability, integrity, confidentiality, and availability.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible after the user is no longer authorized to use the 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 the authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel login IDs and passwords and delete or reassign related active and backup files.
- If the system is left on and unattended, use a suspended program to prevent an unauthorized user from logging on with the current user's ID.
- Verify the user's identity when resetting passwords. This can be done in person or by 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.

Glossary

Hospital Location

Locations at an RPMS site where patient care is provided.

Acronym List

Acronym	Meaning
eCQM	Electronic Clinical Quality Measures
IHS	Indian Health Service
NHSN	National Health Safety Network
RPMS	Resource and Patient Management System

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