RESOURCE AND PATIENT MANAGEMENT SYSTEM

Practice Management Application Suite

(BMW)

Application Overview User Manual

Version 2.0
February 2014

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

Table of Contents

Preface

The Practice Management Application Suite (BMW) is a browser-enabled graphical user interface (GUI) for the Indian Health Service (IHS) Resource and Patient Management System (RPMS) applications.

BMW provides for the entry of new patients and editing the records of those already registered at a medical facility. The patient data managed with BMW is crucial to the third-party billing and follow up patient care. Appropriate caution and checking should be employed to ensure that accurate data is entered into the patient registration system and, subsequently, transmitted to the National Patient Information Resource System and used by providers and staff.

1.0   Introduction

BMW represents a forward step in the streamlining of IHS record and patient management. Through the use of a consistent GUI and module-based architecture, it not only simplifies record and patient management, but also allows for future expansion of the scope and capabilities of the system.

This User Manual provides an overview of the BMW suite. Individual User Manuals are available for each major module of the suite.

1.1   Opening the BMW Application

Follow these steps to open BMW:

1. Open Internet Explorer.

2. In the Address bar, enter the IP address of your Windows application server using this form:

    http://*nnn.nnn.nnn.nnn*

    > **Note:** The IP address of your Windows application server is available from your System Manager.

3. If Microsoft Silverlight is not already installed on the computer, a message will be displayed offering to download and install it. Follow the prompts to install Silverlight on the computer.

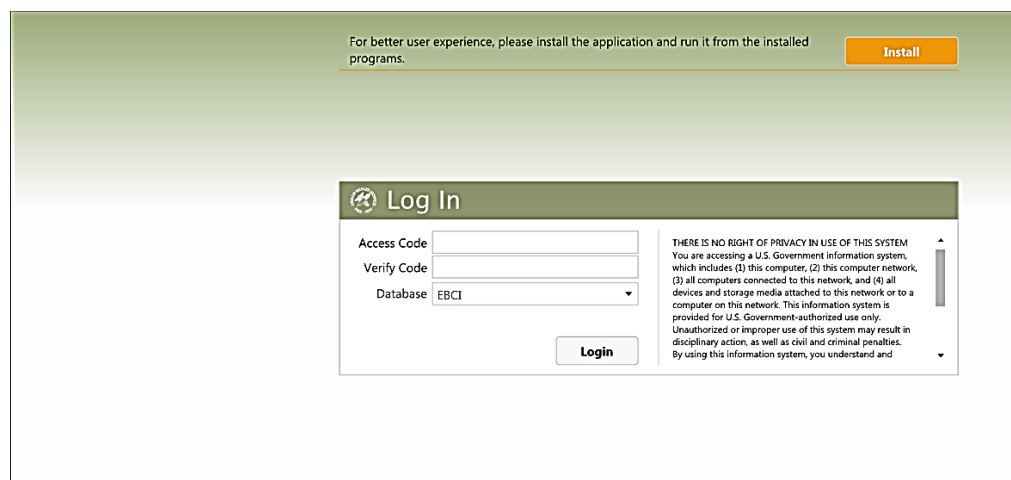4. Once Silverlight is installed, the BMW **Log In** screen (Figure 1-1) is displayed.

Figure 1-1: BMW **Log In** screen

5. Type your RPMS Access Code (user name) in the **Access Code** field

6. Type your RPMS Verify Code (password) in the **Verify Code** field.

7. Select your RPMS database from the **Database** list box.

> **Note:** Users must have an RPMS division assigned to them before
> they can log into the RPMS database selected in this step.

8. Click **Login**. A screen similar to that shown in Figure 1-2 will be displayed.
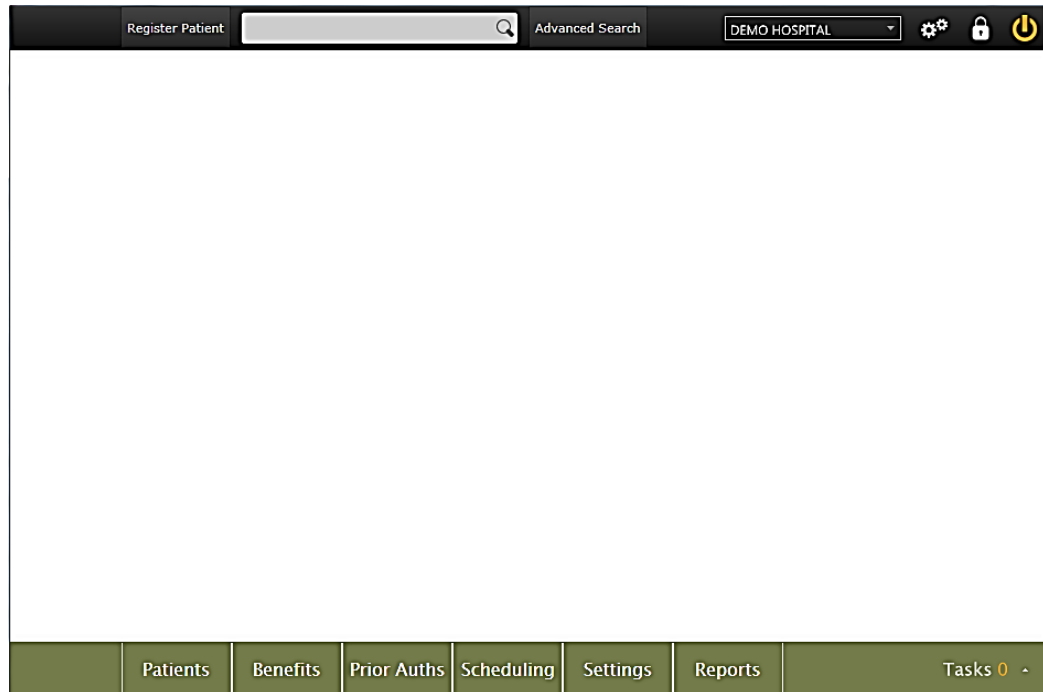

Figure 1-2: BMW Opening Screen

Refer to the separate BMW User Manuals for additional information about using the modules that make up the application suite.

2.0   System Navigation

BMW provides access to a vast array of RPMS information. Entering and accessing that information is done through a consistent interface, primarily the Application Toolbar, the Taskbar, and the Workspace. Each of these components are described briefly in this section, and discussed in further detail later in this manual.

2.1   Application Toolbar

The Application Toolbar (Figure 2-1) at the top of the BMW page provides a simplified method and location for registering new patients, finding the records for existing patients, and selecting the applicable health facility. The Application Toolbar is displayed at all times, regardless of the RPMS module being used. Sections 2.1.1 through 2.1.6 briefly describe the options available from the Application Toolbar.

Figure 2-1: Application Toolbar

2.1.1   Register Patient

Click **Register Patient** (Figure 2-2) in the Application Toolbar to register a new patient and enter the patient's information into the RPMS system. See the *BMW Patient Registration User Manual* for a detailed explanation of the options available when registering a new patient.
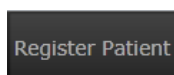

Figure 2-2: **Register Patient** Button

2.1.2   Search Box

Use the Search box (Figure 2-3) in the Application Toolbar to find the records for an existing patient. You can search for a patient based on their name (LAST NAME,FIRST NAME,MIDDLE NAME), their exact Health Record Number (HRN), date of birth (in the form BMMDDYYYY or DD-MM-YYYY), or Social Security Number (SSN).

Figure 2-3: **Search** box

Typing any one (or combination) of these search criteria into the Search box causes a list of search results to be displayed. Select a patient from the list displayed to open that patient's record in the Patient workspace.

2.1.3   Advanced Search

The Advanced Search option provides additional fields to search for a patient record.

Click **Advanced Search** (Figure 2-4) in the Application Toolbar to open the **Advanced Patient Search** form.
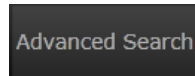

Figure 2-4: **Advanced Search** button

When you click **Advanced Search**, a form similar to that shown in Figure 2-5 is displayed. Type your search criteria in any of the fields provided and click **Search Patients**. (Click **Clear** in the upper right corner of the form to clear any previously-entered search criteria.)

Figure 2-5: **Advanced Patient Search** form

The search results will be displayed in the lower portion of the **Advanced Patient Search** form. If necessary, use the scroll bar on the right of the form to scroll through the page of search results. Use the left and right arrows in the lower left corner of the search listing to navigate through multiple search result pages.

Open a patient record by selecting the appropriate row and clicking **OK**, or by double-clicking the patient record.

2.1.4   Division Selection List

Use the Division Selection list button (Figure 2-6) on the Application Toolbar to select the medical facility for which you want to manage patient records.

Figure 2-6: Division Selection list button

2.1.5   Tools Button

Use the **Tools** button (Figure 2-7) on the Application Toolbar to access the options shown in Figure 2-8.

Figure 2-7: **Tools** button

After clicking the **Tools** button, the menu of options shown in Figure 2-8 is displayed.
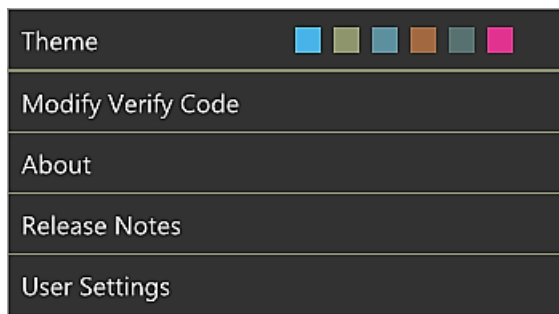
Figure 2-8: Tools Button options

Table 2-1 describes each of the options available:

Table 2-1: Tools Button Options

Option Name	Description
Theme	Select this option to change the color theme of the BMW interface.
Modify Verify Code	Select this option to modify a user's verify code.
About	Select this option to display a report showing information about the current user (including the roles assigned to them), as well as information about the BMW version being used. More information about user roles is available in the *Practice Management Application Suite (BMW) Technical Manual*. The information shown in this report is primarily for use by the IHS Help Desk.

Option Name	Description
Release Notes	Select this option to display the Release Notes for the currently-installed version of BMW.
User Settings	Select this option to enable or disable the option to force BMW to retrieve and update the scheduling data shown when users are also using legacy (roll and scroll) RPMS scheduling applications.

2.1.6   Lock Button

Use the Lock button (Figure 2-10) on the Application Toolbar to lock the current BMW session. After locking the session, you must enter your Access Code and Verify Code to return to BMW.

Figure 2-9: Lock button

2.1.7   Log Out Button

Use the Log Out button (Figure 2-10) on the Application Toolbar to log out from the BMW application and the RPMS database.

Figure 2-10: Log Out button

2.2   Workspace

The Workspace (Figure 2-11) makes up the majority of the BMW display. The information displayed within the Workspace varies, depending on the task being done. In most cases, the Workspace is used for both entering and displaying patient information.
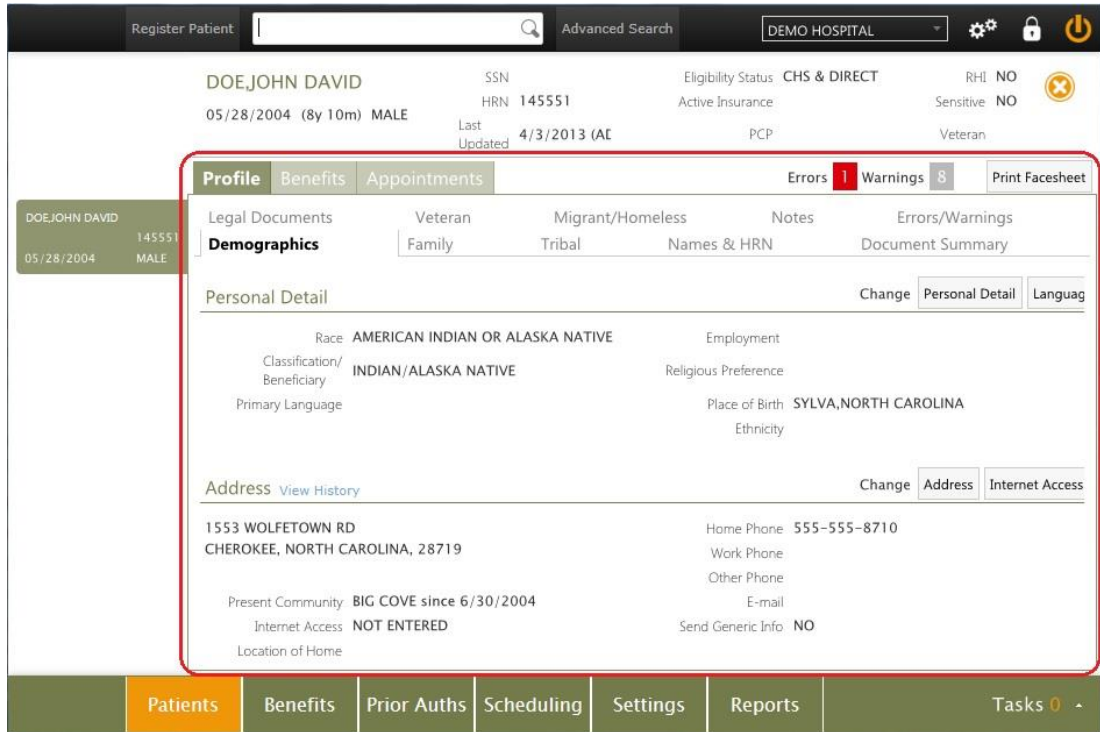
Figure 2-11: Workspace

2.3   Patient Record Pane

The Patient Record Pane (Figure 2-12) shows the currently open patient records. Up to six open patient records can be displayed in the Patient Record Pane. Click any of the records shown to navigate to that patient's record.

Figure 2-12: Patient Record pane

2.4   Taskbar

The BMW Taskbar (Figure 2-13) provides quick access to various Patient Registration and Scheduling modules. These modules are grouped into separate, but related tasks.

Figure 2-13: Sample Taskbar

Click any of the modules in the Taskbar to display and work on that task in the Workspace.

> **Note**: The modules you will see displayed may vary depending on which ones have been installed and which modules you have permissions to access.

2.4.1   Tasks Button

The Patient Management Application Suite gives you the ability to open and work on multiple patient records at the same time. For example, while updating the insurance information for Patient A, you can open the record for Patient B to add a new Emergency Contact phone number. When you do this, a message (Figure 2-14) is displayed giving you the following options:

- Exit from Patient A's record without saving any changes

- Continue working on Patient A's record

- Keep the changes to Patient A's record pending while opening Patient B's record
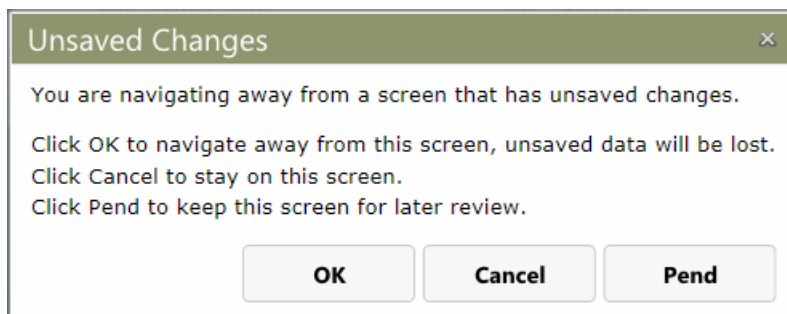
Figure 2-14: **Unsaved Changes** warning message

When you click **Pend**, the page you are working on is temporarily saved as a pending task, and the **Tasks** button in the lower left corner of the screen is incremented to show the number of pending tasks. In the example shown in Figure 2-15, there are three pending tasks.

Figure 2-15: **Tasks** button

Click the **Tasks** button to see a list of the pending tasks (Figure 2-16). Click any of the pending tasks to jump immediately to the page where that task is pending.
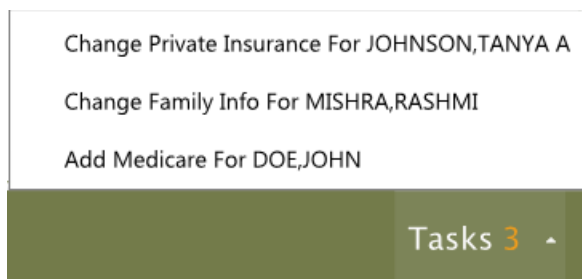
Figure 2-16: **Tasks** button with pending tasks

Using the Tasks button:

- You can have up to 10 pending tasks at one time.

- Due to the need to validate data entries, information you enter into a field on a form will not be saved with the pending task unless you click another field or press the <Tab> key to move to another field before opening another patient's record.

2.5   List Boxes

Throughout BMW are numerous instances of list boxes, also commonly referred to as a drop-down list. List boxes provide a convenient way to display and select from a list of options. As displayed within BMW, a list box is closed (Figure 2-17) and initially appears as an empty field within the form being viewed.

Employment Status

Figure 2-17: Closed List Box example

Click anywhere within the empty list box to expand it and display a list of choices applicable for that field within the form. Figure 2-18 shows an example of an expanded list.

Employment Status

ACTIVE MILITARY DUTY
FULL-TIME
PART-TIME
RETIRED
SELF EMPLOYED
UNEMPLOYED
UNKNOWN
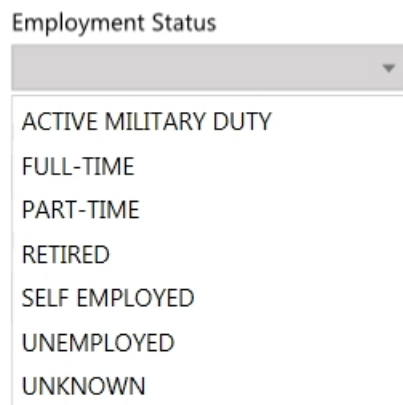
Figure 2-18: Expanded List Box example

After expanding the list box, click any of the choices shown to populate that field of the form.

2.6   Search-Based List Boxes

Some fields in forms throughout the Patient Management Application Suite use list boxes that initiate a search of the RPMS database to retrieve existing records. These list boxes are identified by the magnifying glass icon on the right side of the box, as shown in Figure 2-19.

Employer

Figure 2-19: Closed Search-Based List Box example

Enter information into a search-based list box using one of these methods:

- Type one or more letters in the name (or other part of the name) you want to enter into the list box. A list of entries containing the sequence of letters you typed is displayed. Figure 2-20 shows an example of an expanded search-based list box. Use the scroll bar on the right side of the listing to scroll through all of the entries. Click any of the choices shown to populate that field of the form.

Employer

AUTO

TAYLOR AUTO PARTS   SYLVA NC 2877⁹

B & AUTO GLASS AND PLATE   PO BOX 117
                            HARMONY NC

KING AUTO SUPPLY   MURPHY NC 2890⁰

ROCKDACE AUTO   2394 SIGMAN
                            INO CT

GREENS AUTO   OLD ASH.HWY,
                            SYLVA NC 2877⁹

SMOKEY MTN AUTOMOTIVE   BRYSON CITY N

BEM AUTO GLASS

GREENVILLE AUTO MALL   LAURENS RD

Figure 2-20: Expanded Search-Based List Box example

- Type two question marks (**??**) into the list box. A list of the first ten database entries pertaining to that field is displayed, in alphanumeric order. Use the right and left arrows at the bottom of the listing to navigate through additional pages of database entries. Click any of the choices shown to populate that field of the form.

- Type the full name you want to enter into the list box. Note that you must type the name exactly as it is stored in RPMS.

2.7   Entering Dates

A number of the fields within BMW require calendar dates. To simplify the entering of dates, BMW provides date entry boxes. Similar to a list box, a date entry box is closed (Figure 2-21) and initially appears as an empty field within the form being viewed.

Date of Entry

| Enter date | 🗓 |

Figure 2-21: Closed Date Entry Box example

Date entry boxes accept different types of input. You can type the date directly into the date entry box using any of these accepted formats:

- 5/25/2012

- 05252012

- 5-25-2012

- 5.25.2012

The date will automatically be formatted and stored as MM/DD/YYYY, regardless of how you type it.

Alternatively, you can click the calendar icon on the right side of the date entry box to display a calendar. The current date is selected by default, but you can click any of the other dates displayed to select it. You can also use the left and right arrows at the top of the calendar box to navigate to other months, and then select the specific date.

As in RPMS, you can type the letter **T** in any date entry box to enter today's date. Also, you can type **T-*n***, where *n* is the number of days before today's date that you want to enter. Conversely, typing **T+*n*** will enter a date *n* days from today's date. For example, typing **T+90** will enter a date 90 days into the future from the current date.

3.0   The Settings Module

Unlike the other modules in BMW, the **Settings** module does not directly control or modify patient records. Instead, it controls a variety of application settings for other modules, allowing you to change or add such things as available appointment types, employer names, insurers, and clinics. Although they are grouped in the **Settings** module, these settings affect other modules in the BMW suite. In most cases, once these settings have been established, they will rarely need to be changed.

> **Notes:** The options available in the **Settings** module may vary for different users, depending on the RPMS functionality enabled at your site and the access permissions granted to each user.
>
> You must log off and back in to the BMW application for any patient registration configuration changes to take effect.

Open the Settings module by clicking **Settings** in the Taskbar, as shown in Figure 3-1.

| Patients | Benefits | Prior Auths | Scheduling | Settings | Reports | | Tasks 0 ▲ |

Figure 3-1: Taskbar with **Settings** module highlighted

The selection pane on the left side of the Settings module displays a list of available options. The information displayed on the right side of the screen varies, depending on the option chosen.

3.1 Clinics Page

Click **Clinics** in the selection pane of the Settings Module to see the Clinics page of the Settings module. Figure 3-2 shows an example of the Settings module with the **Clinics** options displayed.

Figure 3-2: Settings Module - **Clinics** page

Refer to the *BMW Scheduling Module User Manual* for more information about using the Clinics page of the Settings Module.

3.2   Table Maintenance Page

Click **Table Maintenance** in the selection pane to see the main **Table Maintenance** page. Figure 3-3 shows an example of the Settings module with the **Table Maintenance** page displayed.
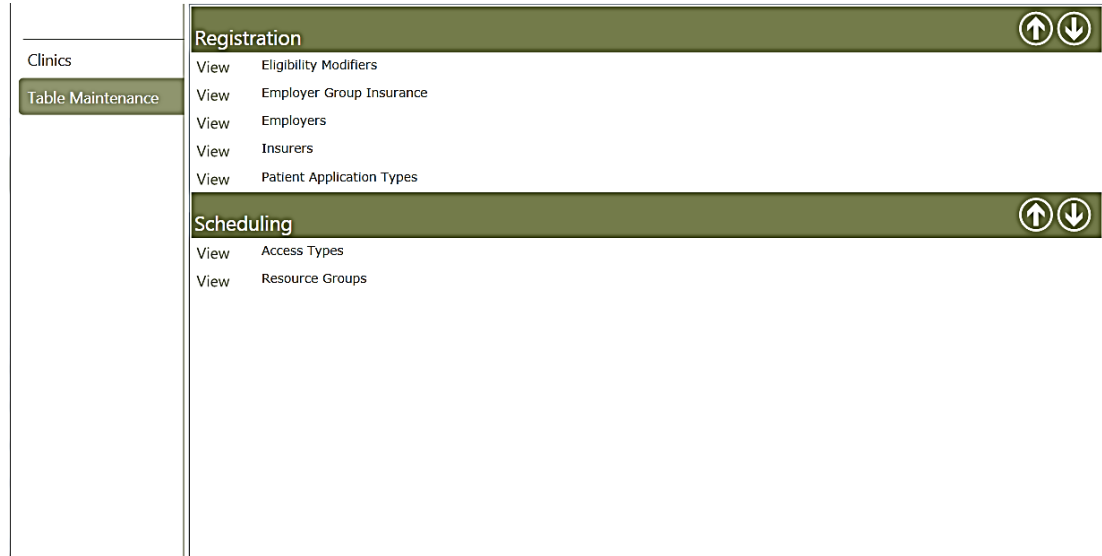
Figure 3-3: Settings Module - **Table Maintenance** page

The individual options from the **Table Maintenance** page are described in the User Manual for that particular module as shown in Table 3-1.

Table 3-1: Settings module – Table Maintenance options

Option	Described In
Eligibility Modifiers	*BMW Patient Registration User Manual*
Employer Group Insurance	*BMW Patient Registration User Manual*
Employers	*BMW Patient Registration User Manual*
Insurers	*BMW Patient Registration User Manual*
Patient Application Types	*BMW Patient Registration User Manual*
Access Types	*BMW Scheduling Module User Manual*
Resource Groups	*BMW Scheduling Module User Manual*

4.0   Browser Mode vs. Out of Browser Mode

The BMW application can be operated in two separate ways: "browser" mode and "out of browser" mode.

4.1   Using Browser Mode

Browser mode runs BMW within a web browser such as Microsoft Internet Explorer or Mozilla Firefox. (Google Chrome, however, is not supported at this time.) In browser mode, BMW is accessed by typing a specific URL (web address) into the address bar of the browser, or by clicking a bookmark or shortcut containing that address.

When running BMW in browser mode, use of the browser navigation buttons (such as Back and Refresh) is not recommended. A typical browser may have additional toolbars or other add-ons, and these can limit the screen space available for the display. For this reason, it is recommended that you use full screen mode when running BMW in browser mode. Use <F11> to access the full screen mode. Keyboard shortcuts are not available when running BMW in browser mode.

4.2   Using Out of Browser Mode

Out of browser mode runs BMW as an installed application, using a separate window that does not require a web browser. In out of browser mode, BMW is accessed through the Windows Program Files (or All Programs) listing, or by double-clicking the desktop shortcut that is installed with the application. Figure 4-1 shows an example of the desktop shortcut.

Figure 4-1: **IHS Practice Management** desktop icon

Running BMW in "out of browser" mode ensures the maximum screen space will be available for the application display. Out of browser mode also provides improved performance, especially when working within the Scheduling module. Keyboard shortcuts are only available when running BMW in "out of browser" mode. See Appendix A for information about using keyboard shortcuts.

Application Overview User Manual   Browser Mode vs. Out of Browser Mode
February 2014

16

Appendix A: Keyboard Shortcuts

When running BMW in "out of browser" mode, many of the BMW features and functions can be accessed with keyboard shortcuts. This Appendix covers the keyboard shortcuts that apply to the Patient Search box at the top of the Application Toolbar described in Section 2.1. Table 4-1 shows the keyboard shortcuts for the Application Toolbar.

Table 4-1: Keyboard Shortcuts for the Application Toolbar

Keys	Available On	Action Performed
Ctrl-R	Application Toolbar	Open Register New Patient dialog
Ctrl-A	Application Toolbar	Open Advanced Search dialog
Ctrl-S	Application Toolbar	Move focus to Patient Search box

Keyboard shortcuts for the BMW Patient Registration module and the BMW Scheduling module are described in the respective User Manuals for those modules.

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.

Glossary

Employer

Company or person that has hired the patient, often offering private health insurance as part of the benefit package.

Health Record Number

A number assigned to each patient by the Medical Records Department (if possible).

Resource and Patient Management System

A suite of software programs maintained for IHS use.

Social Security Number

A nine-digit number assigned by the Social Security Administration for tracking and Social Security benefit purposes.

Acronym List

BMW	RPMS Namespace allocated to the Practice Management Application Suite
GUI	Graphical User Interface
HRN	Health Record Number
IHS	Indian Health Service
IP	Internet Protocol, the method by which information is sent between any two computers on the Internet or a browser-enabled network.
RPMS	Resource and Patient Management System
URL	Web address

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

Email: support@ihs.gov