RESOURCE AND PATIENT MANAGEMENT SYSTEM

Practice Management Application Suite

(BPRM)

Application Overview User Manual

Version 4.0 Patch 6
November 2025

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

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

BPRM provides for the entry of new patients and editing the records of those already registered at a medical facility. The patient data managed with BPRM 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

The Practice Management Application Suite (BPRM) version 4.0 represents a forward step in the streamlining of IHS record and patient management. By using the web browsers Microsoft Edge or Google Chrome, a consistent GUI and module-based architecture is provided. 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 BPRM suite.

Refer to the separate BPRM user manuals for additional information, including settings, about using the modules that make up the application suite:

- *BPRM Patient Registration Module User Manual*
- *BPRM Admission/Discharge/Transfer (ADT) Module User Manual*
- *BPRM Scheduling Module User Manual*

1.1 Opening the BPRM Application

Follow these steps to open BPRM:

1. Open Edge or Chrome web browser

   Note: Firefox is no longer supported by BPRM.

2. In the address bar, type 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.

   The **BPRM Log In** dialog (Figure 1-1) displays with the version of BPRM in the top right corner.

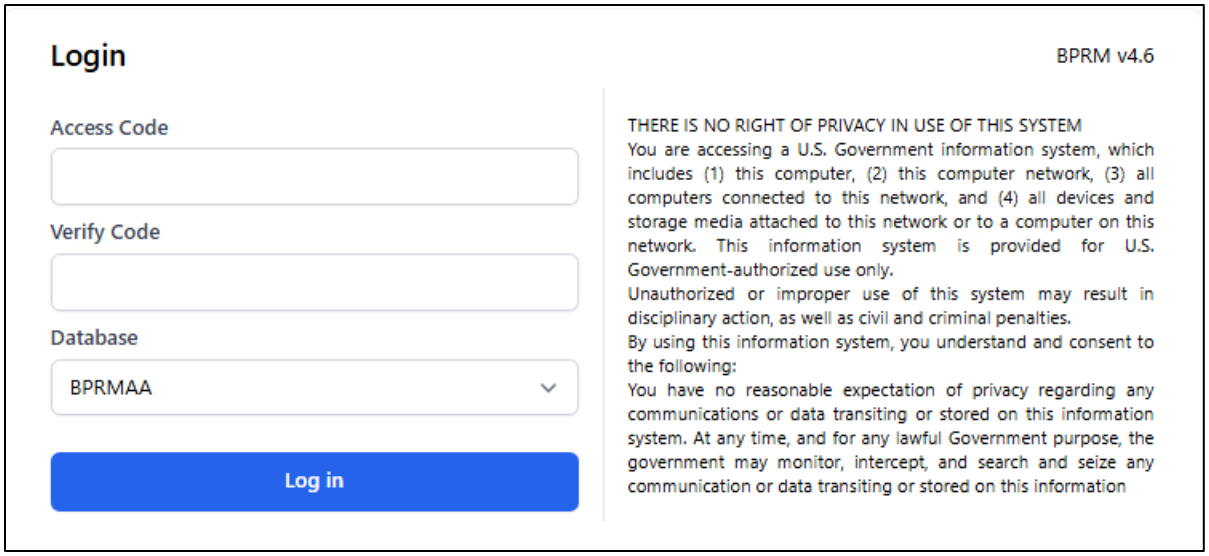

Figure 1-1: BPRM Login window

3. Type your RPMS access code (user name) in the **Access Code** field.
4. Type your RPMS verify code (password) in the **Verify Code** field.
5. Select your RPMS database from the **Database** list field.

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

6. Click **Log in**. The main **BPRM** window (Figure 1-2) displays. The options displayed and available to the user will depend on the user's access.

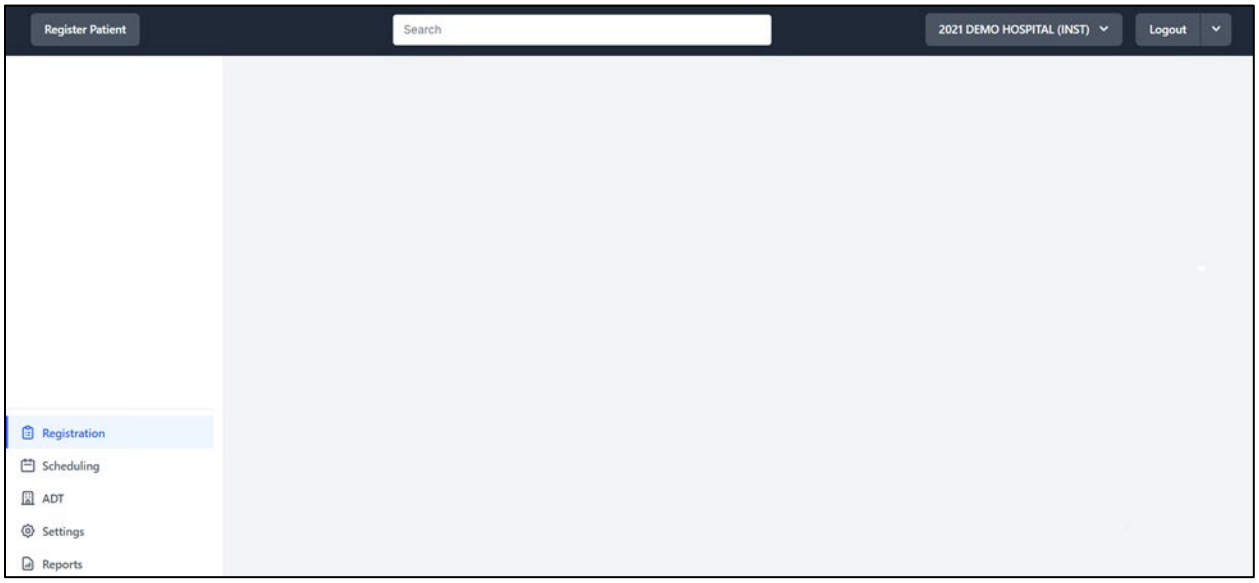

Figure 1-2: BPRM opening window

2.0 System Navigation

BPRM provides access to a vast array of RPMS information. Entering and accessing that information is done through a consistent interface, primarily the application toolbar, left-navigation pane, 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 BPRM page provides a simplified method and location for registering new patients, finding the records for existing patients, and selecting the applicable health facility. Sections 2.1.1 through 2.1.5 briefly describe the options available from the application toolbar. The **Register Patient** option is only available for users who have access to the **Registration** module. The **Patient Search** option is available for users who have access to the **Registration** or **Scheduling** module.

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 *BPRM Patient Registration User Manual* for a detailed explanation of the options available when registering a new patient.

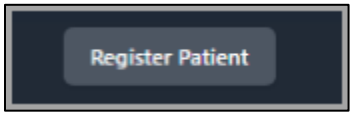

Figure 2-2: Register Patient button

2.1.2 Patient Search Field

Use the **Patient Search** field (Figure 2-3) in the application toolbar to find the records for an existing patient. You can search for a patient based on their legal name, preferred name, or other name (LAST NAME,FIRST NAME,MIDDLE NAME), their exact health record number (HRN), date of birth (in the form MMDDYYYY, DD/MM/YYYY, or DD-MM-YYYY), or phone number (in the form (xxx)xxx-xxxx, xxx-xxx-xxxx, or xxxxxxxxxx).

Figure 2-3: Patient Search field

Typing one of these search criteria into the **Search** field causes a list of search results to display. Select a patient from the list displayed to open that patient's record in the workspace.

2.1.3 Select Division

Use the **Division** drop-down selection (Figure 2-4) on the application toolbar to select the medical facility to manage patient records.

Figure 2-4: Select medical facility button

> **Note:** When a user logs into BPRM they will be taken to the last division they accessed instead of the default division.

2.1.4 Logout Button

The **Logout** button (Figure 2-5) ends the current BPRM session.

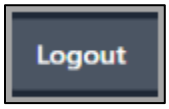

Figure 2-5: Logout button example

> **Note:** When a user closes the browser, the user is automatically logged out of BPRM and must log into BPRM again with credentials.

2.1.5 Timeout

The system uses the RPMS User timeout parameter called "Timed Read (# of Seconds)" in the NEW PERSON file to notify the user of the idle time lapse and that the logout will occur.

When there is only 60 seconds remaining before idle time lapse will occur, the system pops up the message: “Your session is about to expire due to inactivity. Do you want to extend the session?” If the user clicks "Stay Connected", the idle time lapse calculation will restart. If the user clicks "Log out" or the 60 seconds passes, the user will be logged out of BPRM.

> **Note:** If the user has multiple BPRM tabs open, the idle time is calculated for EACH tab because EACH tab uses the login and timeout parameter independently. This message displays on the tab that has TIMED OUT only. Other tabs are NOT affected.

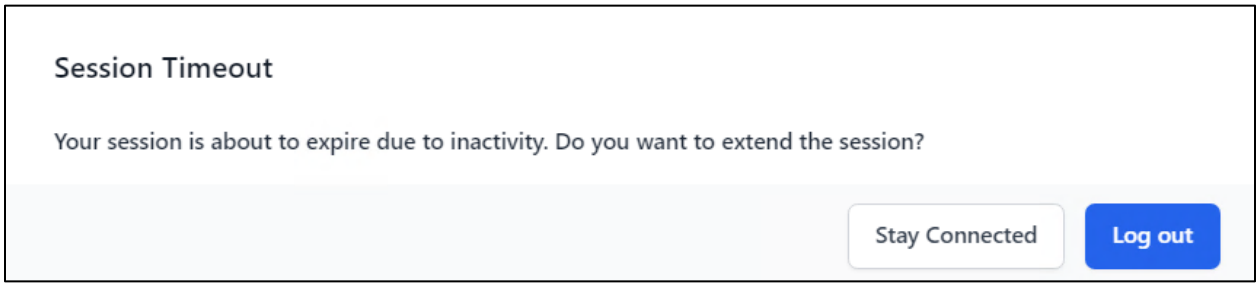

Figure 2-6: Session Timeout window

2.1.6 Drop-Down List Option

- Current user logged in—LastName,FirstName (Figure 2-7).

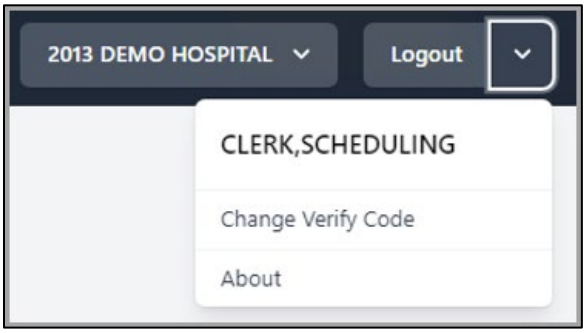

Figure 2-7: Current logged-in user example

- **Change Verify Code**—Enables the user to change their verify code (Figure 2-8).

> **Note:** **Current Access Code** and **Current Verify Code** must be entered prior to entering **New Verify Code** and confirming it.

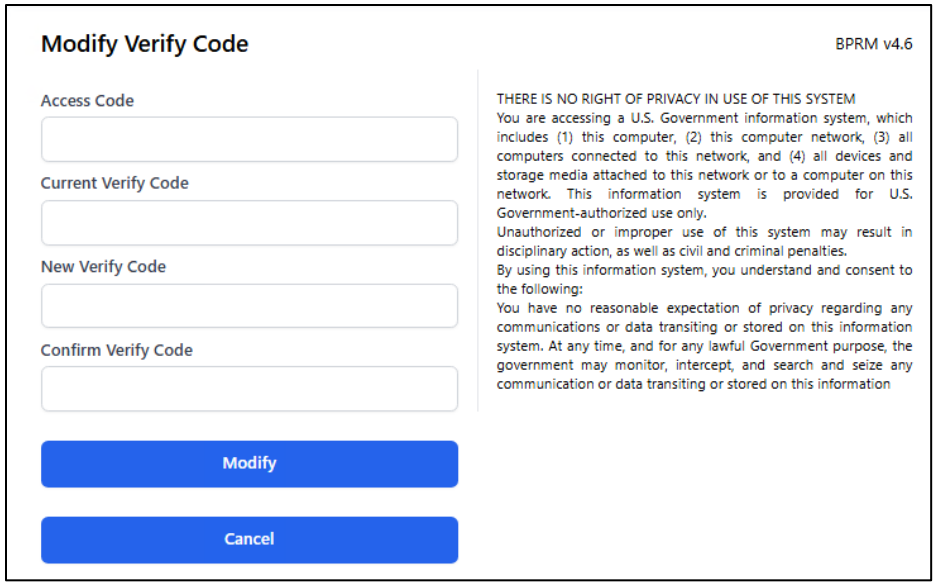

Figure 2-8: Modify Verify Code dialog example

- **About**—Displays information about the current user's security keys, menu options, divisions, and authorized modules. Server information includes Server Type, Application Server Date/Time, Database (RPMS) Server Application Date/Time, and Connection Info. Also included is the browser information (Figure 2-9).

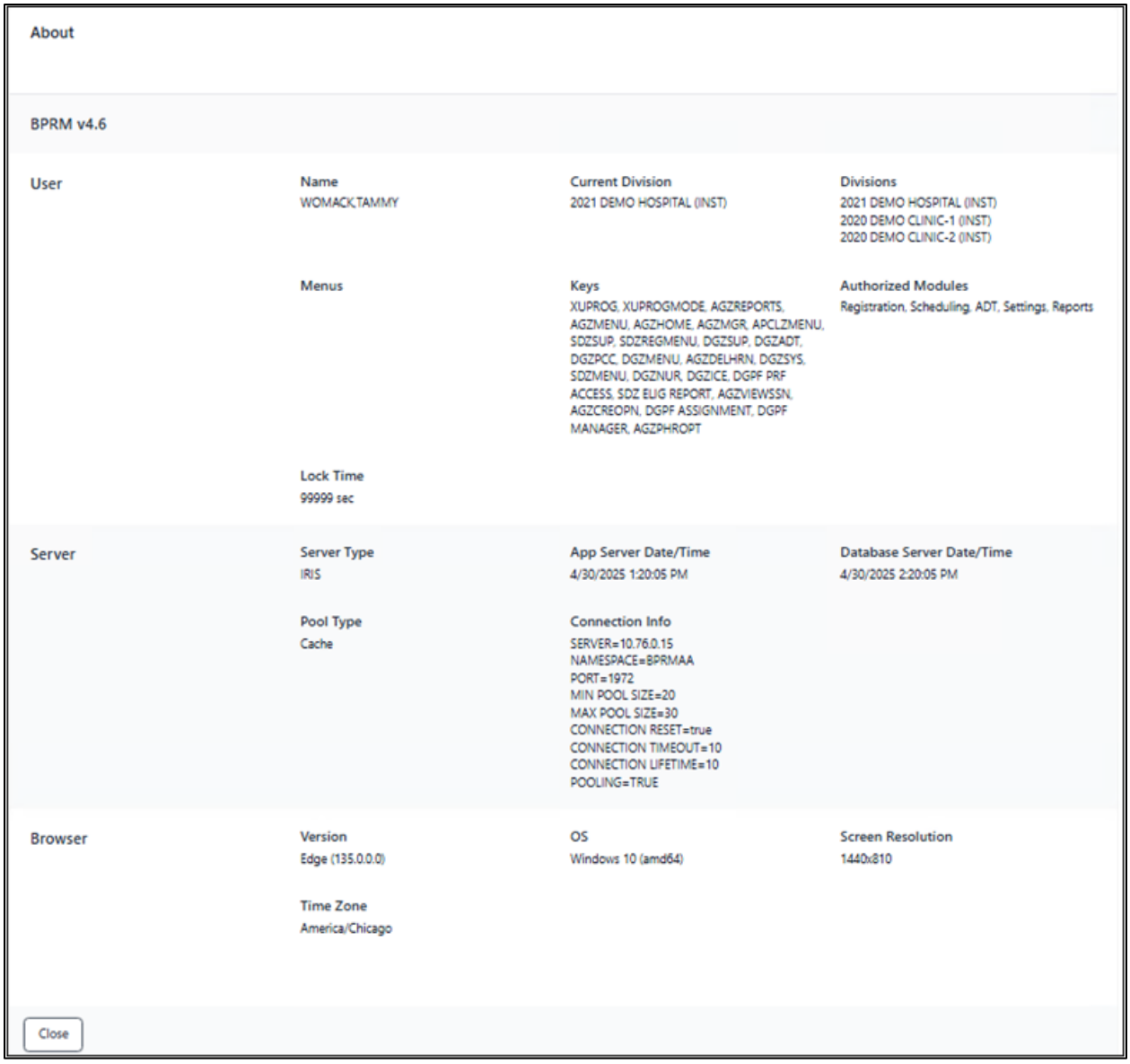

Figure 2-9: About information window example

2.2 Workspace

The workspace (Figure 2-10) makes up the majority of the BPRM 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. Depending on the module being accessed, the workspace can include tabs or a set of toolbars.

For example, in the Registration module, a patient record is comprised of several key components. These include the patient banner, as well as the Profile, Insurance, Prior Auth, Benefits Cases, and Appointments tabs. The tabs at the top of the workspace also contain additional windows of information, which provide access to information within the patient record. Refer to the *BPRM Patient Registration User Manual* for a detailed explanation of each of the available tabs.

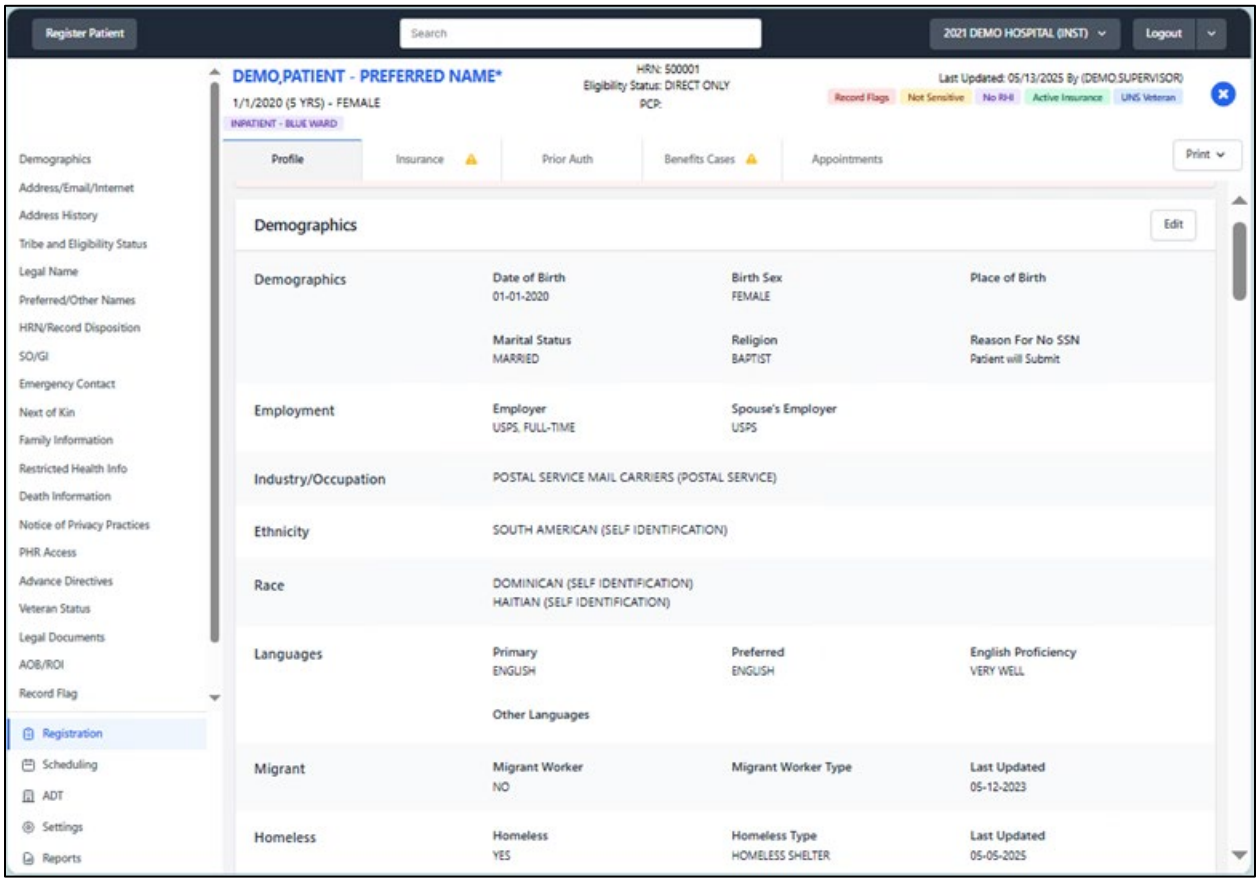

Figure 2-10: Registration Workspace example

For the **Scheduling** and **ADT** modules, there are no tabs; however, a toolbar is included to provide different views or to provide a different way to complete tasks. Figure 2-11 and Figure 2-12 are examples of the Scheduling toolbar and ADT toolbar. Refer to the *BPRM Scheduling Module User Manual* and the *Admission/Discharge/Transfer (ADT) Module User Manual* for a detailed explanation of each of the available options.

Figure 2-11: ADT Toolbar example

Figure 2-12: Scheduling Toolbar example

2.3 Left-Navigation Pane

To the left of the workspace is the navigation pane. A list of available modules displays at the bottom-left of the panel. The list may vary depending on which modules have been installed and which modules the current user has permission to access. Figure 2-13 shows an example of all modules.

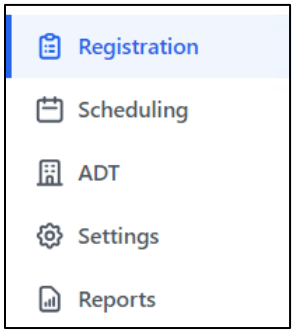

Figure 2-13: Left navigation pane modules

The top portion of the navigation panel lists options to access for the different sections or options related to the current task selected. Depending on the module, the panel may include filter options or sort-by options. Figure 2-14, Figure 2-15, and Figure 2-16 show some examples of what displays.

Figure 2-14: Registration Profile left-navigation pane example

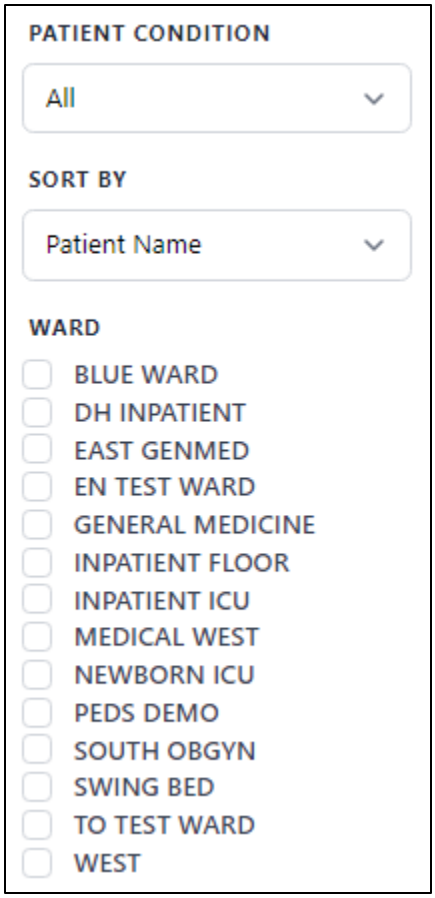

Figure 2-15: ADT list navigation panel example

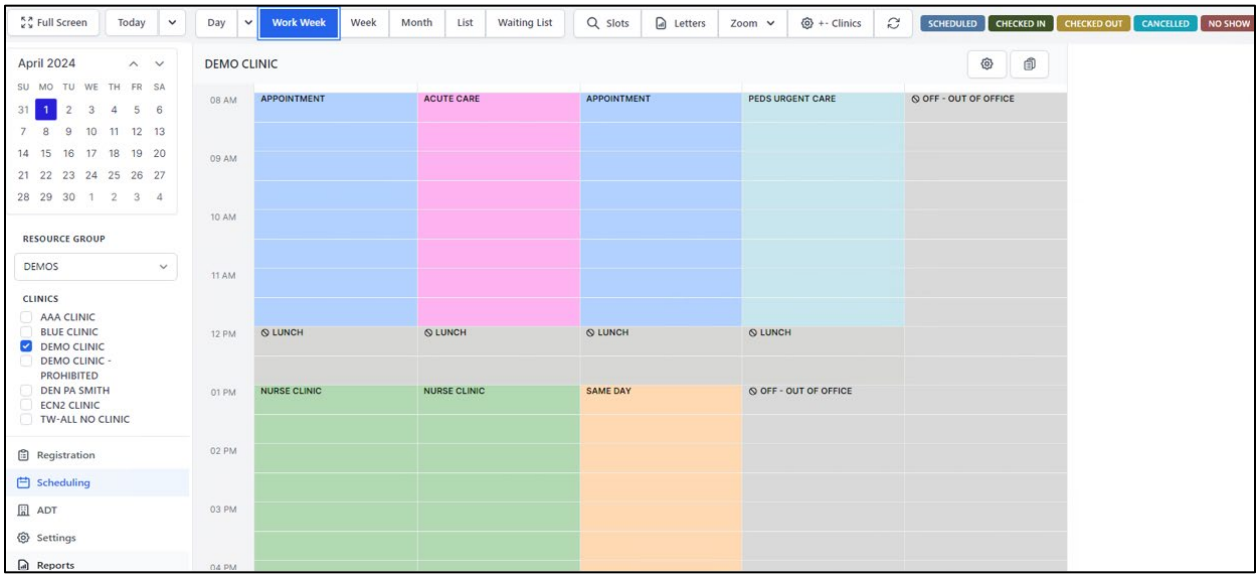

Figure 2-16: Scheduling Work Week view navigation panel example

2.4 Fields

2.4.1 Required Fields

Most fields containing required information are marked as such. These fields are highlighted with a red outline (Figure 2-17). If a required field is left incomplete or blank, the patient record information will not save until the field is completed.

Figure 2-17: Required field example

2.4.2 Note Fields

All note fields are word-processing fields that allow users to enter unlimited amounts of information. However, if the user attempts to enter a word that exceeds 74 characters, the following message (Figure 2-18) displays and the information cannot be saved: “An overlong word (more than 74 characters) was encountered.”

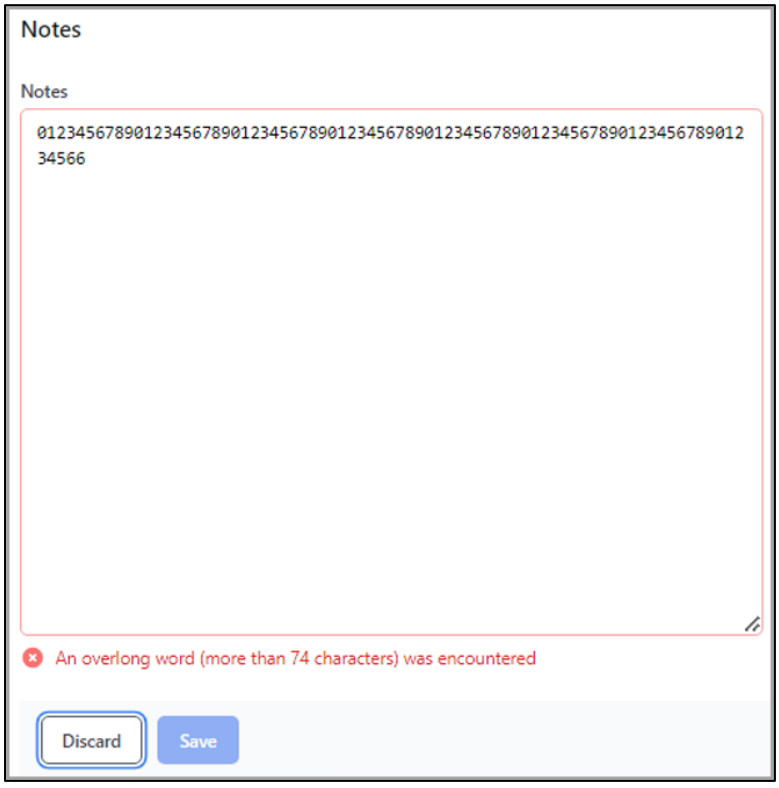

Figure 2-18: Overlong word warning message example

2.4.3 List Fields

Throughout BPRM there are numerous instances of list fields, also commonly referred to as drop-down lists (Figure 2-19). List fields, which initially appear as empty fields within the dialog being reviewed, provide a convenient way to display and select from a list of options.

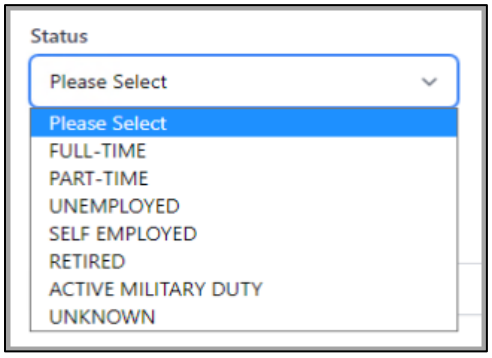

Figure 2-19: List field/drop-down list example

To select information from a drop-down list, click within the field to expand it and display the list of options. Users can also begin typing the option name and the field auto fills with the selection.

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

2.4.4 Search-Based List Fields

Some fields in forms throughout the Patient Management Application Suite use list fields that initiate a search of the RPMS database to retrieve existing records. Enter information into a search-based list field using one of these methods:

- Type one or more letters of the name (or other part of the name) into the list field. A list of entries containing the sequence of letters typed displays. Figure 2-20 shows an example of an expanded search-based list field. Select any of the options shown to populate that field of the form.

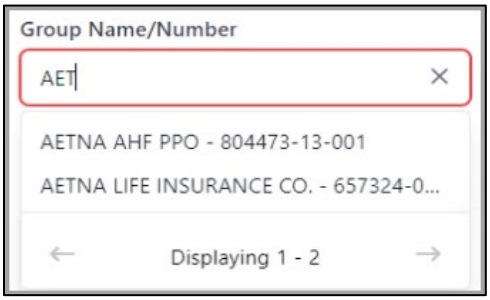

Figure 2-20: Expanded search using partial name example

- Type two question marks (**??**) into the list field (Figure 2-21). A list of the first 10 database entries pertaining to that field displays, in alphanumeric order. Use the right and left arrows at the bottom of the listing to navigate through additional pages of database entries. Select any of the options shown to populate that field of the form.

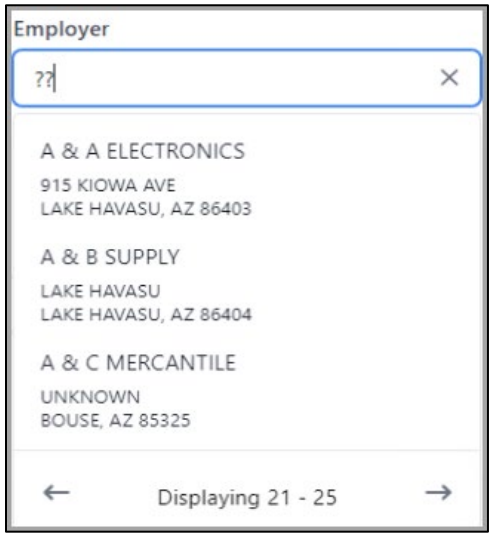

Figure 2-21: Expanded search using ?? example

- Type the full name (Figure 2-22) into the list field.

Note: You must type the name exactly as it is stored in RPMS.

Figure 2-22: Expanded search using full name example

- Use the format of LastName,FirstName (Figure 2-23) in the field if searching for a person.

Figure 2-23: Search name format example

3.0 Buttons

3.1 Save Button

Once any information is entered, click **Save** (Figure 3-1) to save the information you have entered and complete the registration.

Figure 3-1: Patient Registration Save button

The **Save** button will not be available until all the required fields are completed.

3.2 Discard Button

If you do not want to save the information you have entered, click **Discard** (Figure 3-2) to exit the dialog.

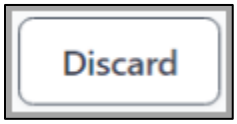

Figure 3-2: Patient Registration Discard button

3.3 Cancel Button

If you do not want to save the information you have entered, click **Cancel** (Figure 3-3) to exit the dialog.

Figure 3-3: Cancel button example

3.4 OK Button

When all information has been added to a field or dialog, click **OK** (Figure 3-4) to save the information.

Figure 3-4: OK button example

3.5 Add Button

Add buttons (Figure 3-5) enable users to add new information or additional fields. There are several different types.

Figure 3-5: Add button example

3.6 Edit Button

Edit buttons (Figure 3-6) enable users to add or update existing information in a dialog or window.

Figure 3-6: Edit button example

3.7 Delete Button

Delete buttons (Figure 3-7) enable users to delete existing entries.

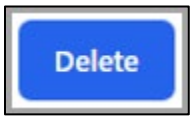

Figure 3-7: Delete button example

3.8 Delete Yes/No Toggle Button

The **Delete Yes/No** toggle button (Figure 3-8) enables the user to select **Yes** to confirm information exists or has been added or **No** if it does not exist.

Figure 3-8: Toggle button example

4.0 Entering Dates and Time

4.1 Date Fields

A number of the dialogs within BPRM require calendar dates. To simplify the entering of dates, date-entry fields (Figure 4-1) are provided with masking in place. The entered number is automatically formatted to MM-DD-YYYY.

Figure 4-1: Date entry field example

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

As in RPMS, you can type the letter **T** in any date-entry field 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** enters a date 90 days into the future from the current date.

4.2 Time Fields

A number of dialogs within BPRM require a time entry. To simplify entering time, time-entry fields (Figure 4-2) are provided with masking in place. Entered numbers are automatically formatted to HH:MM–AM/PM.

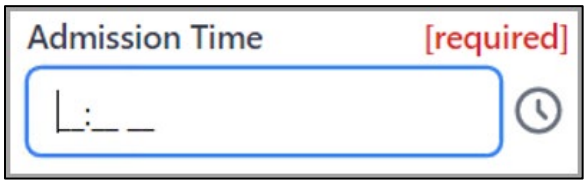

Figure 4-2: Time Entry field example

Alternatively, you can click the time icon on the right side of the time-entry field to display time options. The current time is selected by default, but users can scroll up or down to select another time.

As in RPMS, users can type the letter **N** in any time-entry field to enter the current time. Also, users can type **N-*x***, where ***x*** is the number of minutes before the current time the user wants to enter. Conversely, typing **N+*x*** enters additional **x minutes** from the current time. For example, typing **N+30** enters the current time plus 30 minutes.

5.0 Enter Patient Addresses

Background of Health Data, Technology, and Interoperability: ONC's HTI-1 final rule implements provisions of the 21st Century Cures Act and makes updates to the Certification Program with new and updated standards, implementation specifications, and certification criteria by December 31, 2025.

The Practice Management Application Suite will roll out the updated HTI-1 standards in a phased approach by December 31, 2025.

- Phase one (BPRM v4.0 p5) incorporated the US@ as the applicable vocabulary standard for Current Address in the Patient Demographics/Information data class. The new standard will advance the quality and safety of patient addresses and has the potential for use in other address-related data elements in the future.
- Phase two (BPRM v4.0 p6) allows the user to enter foreign addresses for Mexico or Canada. Additional functionality includes displaying a warning and an indicator to alert the user if an address in the patient's history (less than 1 year) has a non-standard format. The user is allowed to edit the historical address.

For more information on HTI-1, see the following:

United States Core Data for Interoperability (USCDI), Version 3, October 2022
https://www.healthit.gov/isa/sites/isa/files/2022-10/USCDI-Version-3-October-2022-Errata-Final.pdf

To support Project US@ where patient address is being standardized across healthcare systems to improve patient matching, standards and rules are applied to this field.

If the entered address does not meet the US@ standards/rules, the Address Verification screen will display. The user has the option to select the address entered or the suggested address which has been formatted using the US@ standards/rules. The Address Verification screen defaults to the suggested address being selected.

Figure 5-1: Address Verification screen

When entering the patient's address or editing an address in the patient's history, the user enters data in the following fields to be used by the Address Verification logic:

- **Street Address [Line 1]**. Contains the patient's current street address. Street Address [Line 1] is a free-text field allowing alphanumeric characters and must be between 3 and 35 characters in length.
- **City.** Contains the patient's current city.
- **State.** Contains the patient's current state.
- **Zip Code [Accepts Zip+4].** Contains the patient's city zip code, including the four-digit delivery-route code if known.

6.0 Entering Phone Numbers

A number of dialogs within BPRM require phone numbers. To simplify entering phone numbers, phone-number entry fields (Figure 6-1) with a predefined masking are provided. The field initially appears empty, but as the user enters numbers, the application begins to apply the mask.

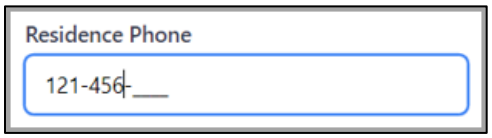

Figure 6-1: Phone number entry field example

The following lists the different types of phone numbers and their formats:

- **Residence Phone**. Use this field to enter the patient's residence phone number in the **+1 555-555-5555** format (be sure to include the area code). The field allows 20 numeric characters.
- **Cell Phone**. Use this field to enter the patient's cell phone number in the **+1 555-555-5555** format (be sure to include the area code). The field allows 20 numeric characters.
- **Work Phone**. Use this field to enter the patient's work phone number (be sure to include the area code). Four additional characters have been added to include an extension, such as **+1 555-555-5555 x555**. The number entered should be verified as correct.
- **Other Phone**. Use this field to enter any other phone numbers associated with the patient along with a short description. For example, **+1 555-555-5555 Mother**. Be sure to include the area code.

7.0 Error/Warning Icons and Messages

7.1 Errors/Warnings Icons

Errors (Errors) and **Warnings** (Warnings) message icons display for each patient in the individual patient header tabs and the left-navigation pane tabs (Figure 7-1).

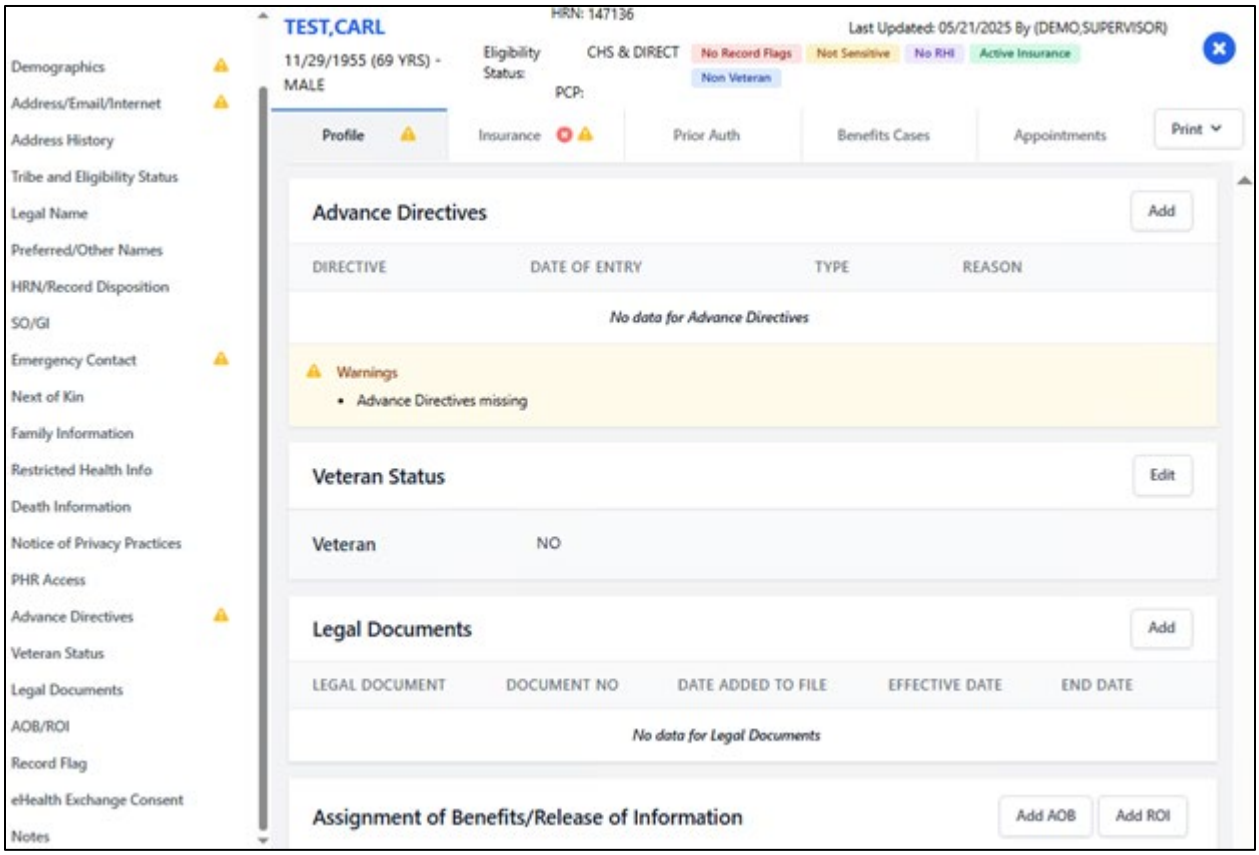

Figure 7-1: Errors/Warnings examples

For Errors/Warnings related to patient profile data, users can view the symbol(s) and their message(s) at the bottom of the window in the **Profile** area to determine the reason for each message. Figure 7-2 shows an example of the **Errors/Warnings** messages for **Demographics**.

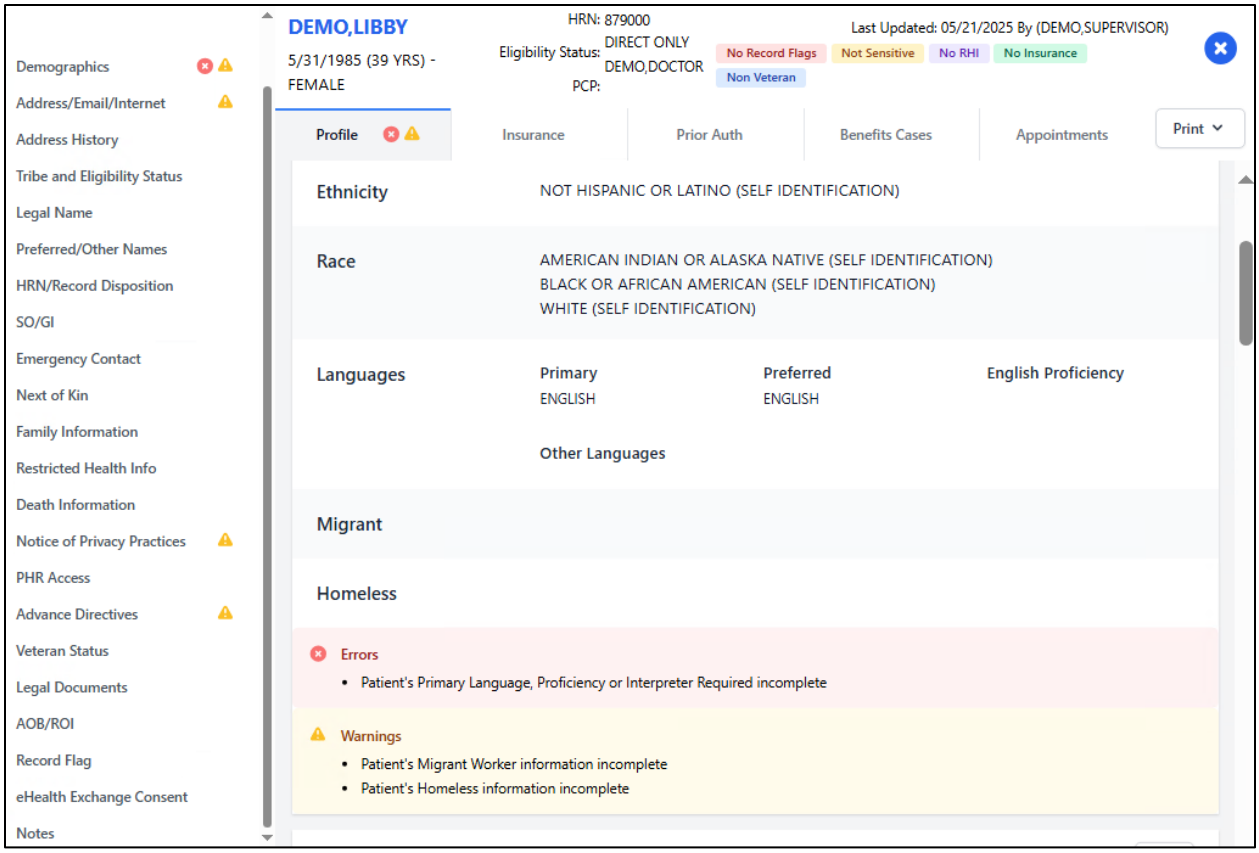

Figure 7-2: Demographics Errors and Warnings example

For Errors/Warnings related to insurance, view the messages by hovering over the icons on the **Insurance Coverage** summary list (Figure 7-3).

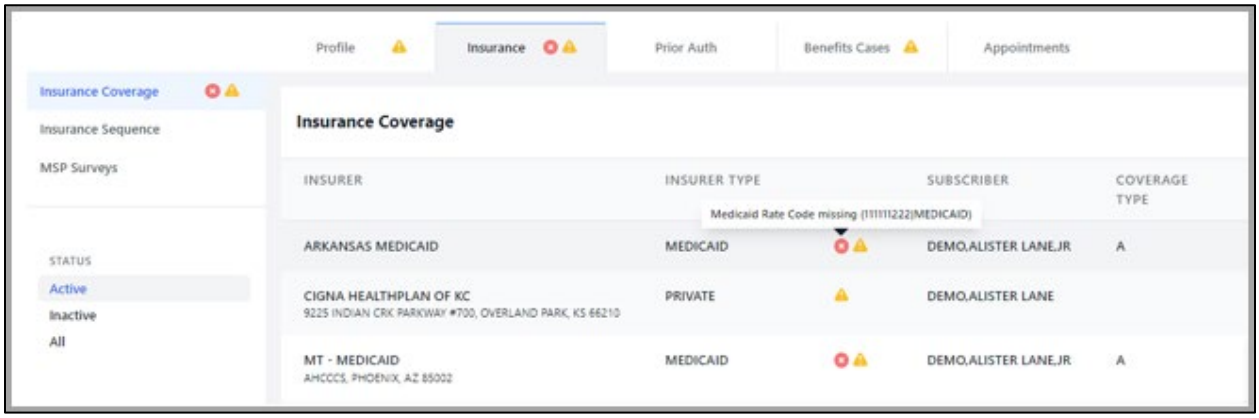

Figure 7-3: Insurance Errors and Warnings example

Other **Errors/Warnings** display on top of the list as shown in Figure 7-4.

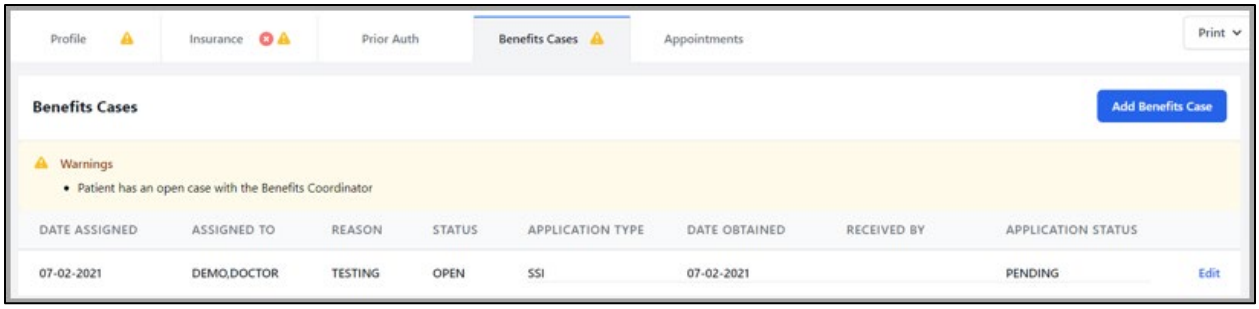

Figure 7-4: Errors/Warnings alternate display example

7.2 Pop-up Warning Messages

Pop-up messages alert users to important information that the user must pay attention to, such as a patient condition or that a window with unsaved data is about to close without saving. They can also be used to prompt the user to confirm before taking some action.

7.2.1 Confirm Close/Remove Warning Messages

When users select **Discard** or **Cancel** to close a section without saving the information, the **Confirm** warning message (Figure 7-5) and/or **Confirm Remove** warning message (Figure 7-6) displays. Clicking **Cancel** gives the user a chance to go back and determine if they really want to close without saving. Clicking **OK** or **Remove** enables the user to continue with the closing action without saving any changes.

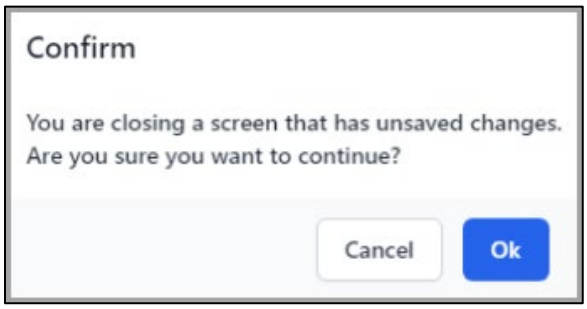

Figure 7-5: Confirm close warning message

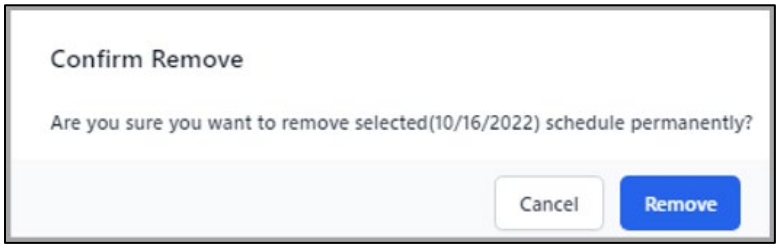

Figure 7-6: Confirm Remove warning message

7.2.2 Patient Record Warning Messages

When users attempt to access patient records that they do not have authorization to view, they receive patient record warning messages (Figure 7-7, Figure 7-8, and Figure 7-9).

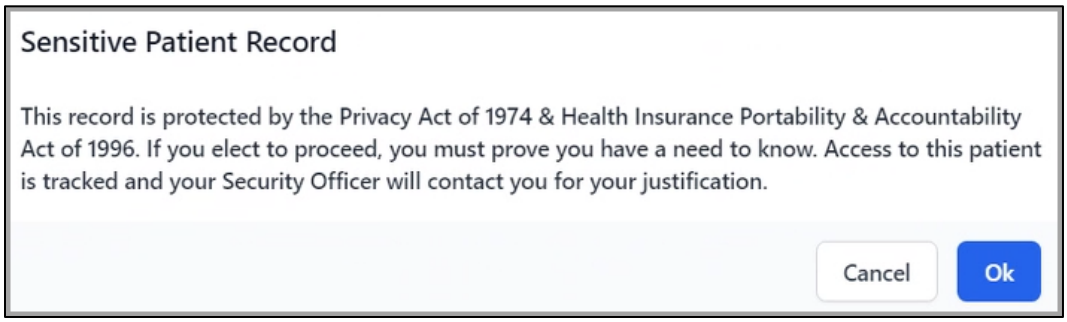

Figure 7-7: Sensitive Patient Record warning message

Figure 7-8: Warning Restricted Record message

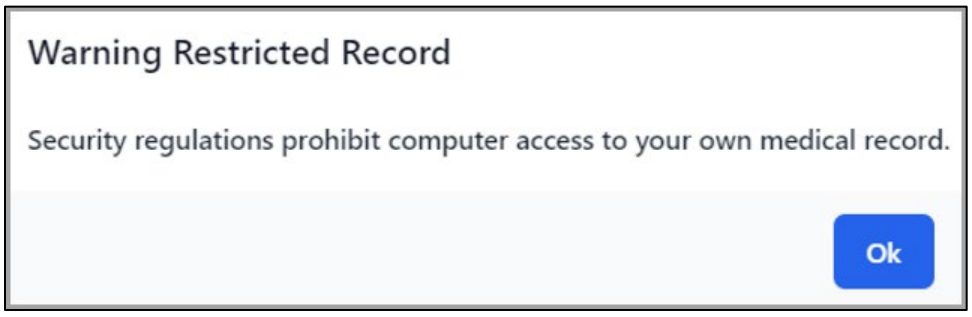

Figure 7-9: Warning Personal Restricted Record message example

8.0 Reports: Preview and Print Options

For every report in the **Reports** module, the user can view the report results in a couple of ways. After selecting the appropriate report parameters, do the following:

- Click **Preview** to view the report on the window.
- Click **Print** to print the report to an RPMS device or to the browser.

Figure 8-1 shows the **Preview** and **Print** options for all reports.

Figure 8-1: Preview and Print options

8.1 Reports: Page Selection

For every report in the **Reports** module, the user can utilize the following page selection buttons (Figure 8-2) to navigate through multi-page reports.

- Use the middle arrows () to move through the report one page at a time.
- Use the arrows with bars () to quickly scroll to the beginning or the end of the report.

Figure 8-2: Page selection buttons

8.2 Reports: Zoom Options

For every report in the **Reports** module, the user can utilize the following zoom in and zoom out functions (Figure 8-3) to perform those functions within the page view of the report.

- Use the  and  buttons to manually adjust the report view.
- Use the **100%** picklist option to set a specific report view (includes **Fit Page** and **Fit Width**).

Figure 8-3: Zoom buttons

9.0 Export List View

Each module provides the user with the ability to export lists as an Excel file with a maximum limit of 2000 records. The below lists are available for export and you will need to refer to the additional separate BPRM user manuals for additional information on how to export.

- Registration: Appointment Tab
- Scheduling: Wait List and Appointment List
- ADT: List View and Discharge List

The export is saved locally and requires a password that is case-sensitive.

> **Note:** If your browser is set to allow you to save each file before downloading, then the system will allow you to select the location and enter a name for the exported Excel file. If this browser setting is not turned on, then the system will automatically name the Excel file and save it to your downloads default location.

10.0 Device

Selecting the **Device** option allows the user to print to an RPMS device. An additional dialog (Figure 10-1) is presented to search for an RPMS printer defined on the database. Use a partial name search to find the appropriate RPMS device printer or type two question marks (**??**) to see all the available RPMS device printers. Printers can be searched by printer name or printer mnemonic or local synonym. Note: the mnemonic will display within the search results.

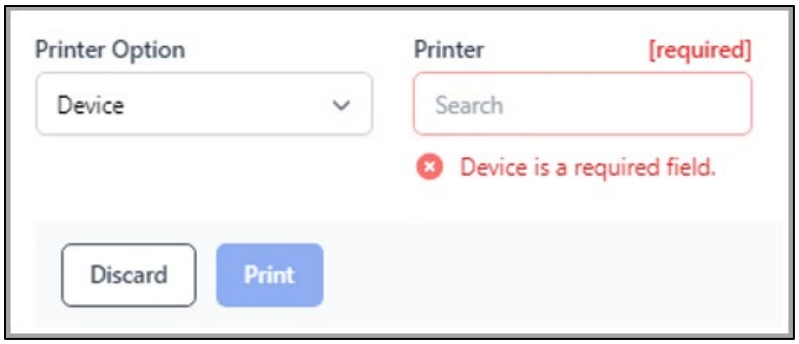

Figure 10-1: Device Printer Prompt dialog

Note: This section is also listed in BPRM *Patient Registration Module User Manual*.

Appendix A Rules of Behavior

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

All users (Contractors and IHS Employees) of RPMS will be provided a copy of the Rules of Behavior (ROB) and must acknowledge that they have received and read them prior to being granted access to a RPMS system, in accordance 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 the IHS websites below:

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 the documentation of that application (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 employer before providing any type of information system access, sensitive information, or nonpublic agency information.

- Be aware that personal use of information resources is authorized on a limited basis within the provisions Indian Health Manual Part 8, "Information Resources Management," Chapter 6, "Limited Personal Use of Information Technology Resources."

RPMS users shall not:

- Retrieve information for someone who does not have authority to access the information.
- Access, research, or change any user account, file, directory, table, or record not required to perform their *official* duties.
- Store sensitive files on a PC hard drive, or portable devices or media, if access to the PC or files cannot be physically or technically limited.
- Exceed their authorized access limits in RPMS by changing information or searching databases beyond the responsibilities of their jobs or by divulging information to anyone not authorized to know that information.

A.1.2 Information Accessibility

RPMS shall restrict access to information based on the type and identity of the user. However, regardless of the type of user, access shall be restricted to the minimum level necessary to perform the job.

RPMS users shall:

- Access only those documents they created and those other documents to which they have a valid need-to-know and to which they have specifically granted access through an RPMS application based on their menus (job roles), keys, and FileMan access codes. Some users may be afforded additional privileges based on the functions they perform, such as system administrator or application administrator.
- Acquire a written preauthorization in accordance with IHS policies and procedures prior to interconnection to or transferring data from RPMS.

A.1.3 Accountability

RPMS users shall:

- Behave in an ethical, technically proficient, informed, and trustworthy manner.
- Log out of the system whenever they leave the vicinity of their personal computers (PCs).
- Be alert to threats and vulnerabilities in the security of the system.
- Report all security incidents to their local Information System Security Officer (ISSO).

- Differentiate tasks and functions to ensure that no one person has sole access to or control over important resources.
- Protect all sensitive data entrusted to them as part of their government employment.
- Abide by all Department and Agency policies and procedures and guidelines related to ethics, conduct, behavior, and information technology (IT) information processes.

A.1.4 Confidentiality

RPMS users shall:

- Be aware of the sensitivity of electronic and hard copy information and protect it accordingly.
- Store hard copy reports/storage media containing confidential information in a locked room or cabinet.
- Erase sensitive data on storage media prior to reusing or disposing of the media.
- Protect all RPMS terminals from public viewing at all times.
- Abide by all Health Insurance Portability and Accountability Act (HIPAA) regulations to ensure patient confidentiality.

RPMS users shall not:

- Allow confidential information to remain on the PC screen when someone who is not authorized to that data is in the vicinity.
- Store sensitive files on a portable device or media without encrypting.

A.1.5 Integrity

RPMS users shall:

- Protect their systems against viruses and similar malicious programs.
- Observe all software license agreements.
- Follow industry standard procedures for maintaining and managing RPMS hardware, operating system software, application software, and/or database software and database tables.
- Comply with all copyright regulations and license agreements associated with RPMS software.

RPMS users shall not:

- Violate federal copyright laws.
- Install or use unauthorized software within the system libraries or folders.

- Use freeware, shareware, or public domain software on/with the system without their manager's written permission and without scanning it for viruses first.

A.1.6 System Logon

RPMS users shall:

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

A.1.7 Passwords

RPMS users shall:

- Change passwords a minimum of every 90 days.
- Create passwords with a minimum of eight characters.
- If the system allows, use a combination of alpha-numeric characters for passwords, with at least one uppercase letter, one lower case letter, and one number. It is recommended, if possible, that a special character also be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or store them in a safe place (do not store passwords in login scripts or batch files).
- Change passwords immediately if password has been seen, guessed, or otherwise compromised, and report the compromise or suspected compromise to their ISSO.
- Keep user identifications (IDs) and passwords confidential.

RPMS users shall not:

- Use common words found in any dictionary as a password.
- Use obvious readable passwords or passwords that incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Share passwords/IDs with anyone or accept the use of another's password/ID, even if offered.
- Reuse passwords. A new password must contain no more than five characters per eight characters from the previous password.
- Post passwords.

- Keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.
- Give a password out over the phone.

A.1.8 Backups

RPMS users shall:

- Plan for contingencies such as physical disasters, loss of processing, and disclosure of information by preparing alternate work strategies and system recovery mechanisms.
- Make backups of systems and files on a regular, defined basis.
- If possible, store backups away from the system in a secure environment.

A.1.9 Reporting

RPMS users shall:

- Contact and inform their ISSO that they have identified an IT security incident and begin the reporting process by providing an IT Incident Reporting Form regarding this incident.
- Report security incidents as detailed in the *IHS Incident Handling Guide* (SOP 05-03).

RPMS users shall not:

- Assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident gets reported more than once.

A.1.10 Session Timeouts

RPMS system implements system-based timeouts that back users out of a prompt after no more than 5 minutes of inactivity.

RPMS users shall:

- Utilize a screen saver with password protection set to suspend operations at no greater than 10 minutes of inactivity. This will prevent inappropriate access and viewing of any material displayed on the screen after some period of inactivity.

A.1.11 Hardware

RPMS users shall:

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).

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

RPMS users shall not:

- Eat or drink near system equipment.

A.1.12 Awareness

RPMS users shall:

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

A.1.13 Remote Access

Each subscriber organization establishes its own policies for determining which employees may work at home or in other remote workplace locations. Any remote work arrangement should include policies that:

- Are in writing.
- Provide authentication of the remote user through the use of ID and password or other acceptable technical means.
- Outline the work requirements and the security safeguards and procedures the employee is expected to follow.
- Ensure adequate storage of files, removal, and nonrecovery of temporary files created in processing sensitive data, virus protection, and intrusion detection, and provide physical security for government equipment and sensitive data.
- Establish mechanisms to back up data created and/or stored at alternate work locations.

Remote RPMS users shall:

- Remotely access RPMS through a virtual private network (VPN) whenever possible. Use of direct dial in access must be justified and approved in writing and its use secured in accordance with industry best practices or government procedures.

Remote RPMS users shall not

- Disable any encryption established for network, internet, and Web browser communications.

A.2 RPMS Developers

RPMS developers shall:

- Always be mindful of protecting the confidentiality, availability, and integrity of RPMS when writing or revising code.
- Always follow the IHS RPMS Programming Standards and Conventions (SAC) when developing for RPMS.
- Only access information or code within the namespaces for which they have been assigned as part of their duties.
- Remember that all RPMS code is the property of the U.S. Government, not the developer.
- Not access live production systems without obtaining appropriate written access and shall only retain that access for the shortest period possible to accomplish the task that requires the access.
- Observe separation of duties policies and procedures to the fullest extent possible.
- Document or comment all changes to any RPMS software at the time the change or update is made. Documentation shall include the programmer's initials, date of change, and reason for the change.
- Use checksums or other integrity mechanism when releasing their certified applications to assure the integrity of the routines within their RPMS applications.
- Follow industry best standards for systems they are assigned to develop or maintain and abide by all Department and Agency policies and procedures.
- Document and implement security processes whenever available.

RPMS developers shall not:

- Write any code that adversely impacts RPMS, such as backdoor access, "Easter eggs," time bombs, or any other malicious code or make inappropriate comments within the code, manuals, or help frames.
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

A.3 Privileged Users

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

Privileged RPMS users shall:

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government personnel and contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance.
- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to RPMS that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to RPMS.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the ISSO, Chief Information Security Officer (CISO), and systems owner.
- Protect the supervisor, superuser, or system administrator passwords.
- Avoid instances where the same individual has responsibility for several functions (i.e., transaction entry and transaction approval).
- Watch for unscheduled, unusual, and unauthorized programs.
- Help train system users on the appropriate use and security of the system.
- Establish protective controls to ensure the accountability, integrity, confidentiality, and availability of the system.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible from the time that the user is no longer authorized system. Passwords forgotten by their owner should be replaced, not reissued.
- Terminate user accounts when a user transfers or has been terminated. If the user has authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel logon IDs and passwords and delete or reassign related active and backup files.

- Use a suspend program to prevent an unauthorized user from logging on with the current user's ID if the system is left on and unattended.
- Verify the identity of the user when resetting passwords. This can be done either in person or having the user answer a question that can be compared to one in the administrator's database.
- Shall follow industry best standards for systems they are assigned to and abide by all Department and Agency policies and procedures.

Privileged RPMS users shall not:

- Access any files, records, systems, etc., that are not explicitly needed to perform their duties
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

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

Acronym	Definition
GUI	Graphical User Interface
HRN	Health Record Number
IHS	Indian Health Service
IP	Internet Protocol
RPMS	Resource and Patient Management System
URL	Uniform Resource Locator

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