RESOURCE AND PATIENT MANAGEMENT SYSTEM

IHS Emergency Department Dashboard

(BEDD)

User Manual

Version 2.0
June 2015

Office of Information Technology (OIT)
Division of Information Technology
# Table of Contents

1.0 Introduction ............................................................................................................. 1  

2.0 System Navigation ........................................................................................................ 2  
  2.1 Admit Patient via AMER ....................................................................................... 2  
  2.2 Triage Patient and Triage Actions ........................................................................... 5  
  2.3 Assign Patient to Room ......................................................................................... 9  
  2.4 Update Additional ED Data ................................................................................. 10  
  2.4.1 Injury Information ............................................................................................. 10  
  2.4.2 Visit Information .............................................................................................. 12  
  2.4.3 ED Consults ...................................................................................................... 12  
  2.4.4 ED Procedures .................................................................................................. 13  
  2.4.5 Diagnosis ......................................................................................................... 13  
  2.4.6 Additional Notes .............................................................................................. 14  
  2.5 Remove Patient from Room .............................................................................. 14  
  2.6 Discharge Patient ............................................................................................... 15  
  2.7 Discharge Reporting ............................................................................................ 19  
  2.8 ED Dashboard Reporting ..................................................................................... 21  

3.0 Package Management ........................................................................................................ 26  

4.0 Package Operation ....................................................................................................... 27  
  4.1 Access the EDD Manager Options ........................................................................ 27  
  4.1.1 Login to the EDD application ............................................................................ 27  
  4.1.2 Go to the Manager screen ............................................................................... 27  
  4.2 Add ER location .................................................................................................... 28  
  4.3 Access Setup & Configure Options ...................................................................... 29  
  4.3.1 Screen timeout (in seconds) ............................................................................. 31  
  4.3.2 Operate Dashboard Stand Alone .................................................................... 31  
  4.3.3 Use More than 1 Clinic .................................................................................... 31  
  4.3.4 Show Daily Summary on Dashboard ................................................................ 32  
  4.3.5 Print Med Rec Worksheet .............................................................................. 32  
  4.3.6 Print Patient Routing Sheet ............................................................................. 32  
  4.3.7 Print Arm Band ................................................................................................. 33  
  4.3.8 Show Used Room ............................................................................................ 33  
  4.3.9 Show Provider .................................................................................................. 34  
  4.3.10 Show Nurse ................................................................................................. 34  
  4.3.11 Show Consult ............................................................................................... 35  
  4.3.12 Use Auto Note ............................................................................................... 35  
  4.3.13 Use Comm Board ......................................................................................... 36  
  4.3.14 Print Triage Report on Save .......................................................................... 36  
  4.3.15 Switch EHR Patient on Edit .......................................................................... 37  
  4.3.16 Reg column on main display ....................................................................... 37  

Appendix A: Rules of Behavior ......................................................................................... 38
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1</td>
<td>All RPMS Users</td>
<td>38</td>
</tr>
<tr>
<td>A.1.1</td>
<td>Access</td>
<td>38</td>
</tr>
<tr>
<td>A.1.2</td>
<td>Information Accessibility</td>
<td>39</td>
</tr>
<tr>
<td>A.1.3</td>
<td>Accountability</td>
<td>39</td>
</tr>
<tr>
<td>A.1.4</td>
<td>Confidentiality</td>
<td>40</td>
</tr>
<tr>
<td>A.1.5</td>
<td>Integrity</td>
<td>40</td>
</tr>
<tr>
<td>A.1.6</td>
<td>System Logon</td>
<td>41</td>
</tr>
<tr>
<td>A.1.7</td>
<td>Passwords</td>
<td>41</td>
</tr>
<tr>
<td>A.1.8</td>
<td>Backups</td>
<td>42</td>
</tr>
<tr>
<td>A.1.9</td>
<td>Reporting</td>
<td>42</td>
</tr>
<tr>
<td>A.1.10</td>
<td>Session Timeouts</td>
<td>42</td>
</tr>
<tr>
<td>A.1.11</td>
<td>Hardware</td>
<td>42</td>
</tr>
<tr>
<td>A.1.12</td>
<td>Awareness</td>
<td>43</td>
</tr>
<tr>
<td>A.1.13</td>
<td>Remote Access</td>
<td>43</td>
</tr>
<tr>
<td>A.2</td>
<td>RPMS Developers</td>
<td>44</td>
</tr>
<tr>
<td>A.3</td>
<td>Privileged Users</td>
<td>44</td>
</tr>
</tbody>
</table>

- **Glossary**: 47
- **Acronym List**: 48
- **Contact Information**: 49
Preface

The purpose of this manual is to provide the user with the information required to use the IHS Emergency Department Dashboard (EDD).
1.0 Introduction

The EDD is a tool that electronically enables facilities to run and manage their emergency and or urgent care clinics. It is dependent on the Resource and Patient Management System (RPMS) Emergency Room System (ERS) in the AMER namespace. EDD was built on the ERS foundation to enhance patient flow and provider communication.

EDD can be set up to operate as a standalone icon on the staff computer or can be accessed from within the RPMS Electronic Health Record (EHR) application.

EDD gets its data and updates from one of four ways: ERS, Dashboard Edit, or EHR data or a combination of all three.
2.0 System Navigation

This section outlines a typical workflow for using the EDD. Be advised that some of these steps may be different for a given site.

- Admit a patient via the **RPMS AMER ADMISSION** option, which will register the patient on the dashboard (in the Check-In section)
- Triage the patient which moves the patient into the **Triaged** section of the dashboard
- Assign the patient to a room
  - Update various informational visit screens
  - Injury
  - General visit information
  - Emergency Department (ED) Consult Information
  - Procedure information
  - Diagnosis information
- Remove from room
- Discharge
- Run dashboard reports

2.1 Admit Patient via AMER

In order to list a patient in the EDD the patient must first be admitted to the ED using the **RPMS AMER ADMISSION** menu option as indicated in Figure 2-1.

```
Select OPTION NAME: AMER ADMISSION        Admit to Emergency Room
ER SYSTEM Ver 3.0: ADMISSION TO EMERGENCY ROOM       ^= back up       ^^ = quit
Questions preceded by a '*' are MANDATORY. Enter '?' to see choices.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Enter the patient's NAME or LOCAL CHART NUMBER: DEMO,PA
  1  DEMO,PATIENT  <A>  F 01-01-1970  602010170P   TST 1234
  2  DEMO,PATIENT  <A>  M 01-01-1980  602010180P   TST 123412
  3  DEMO,PATIENT BABYONE  <A>  F 01-01-2014  612010114P   TST 11000
  4  DEMO,PATIENT BARBARA  <A>  F 01-01-1968  612010168P   TST 111
  5  DEMO,PATIENT J JR LERR,TODD G JR  M 06-07-2009 XXX-XX-8408   TST 133778
ENTER '^' TO STOP, OR
CHOOSE 1-5: 1
DEMO,PATIENT  <A>  F 01-01-1970  602010170P   TST 1234

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
*Date and time of admission to ER: NOW//   (MAY 13, 2015@07:59)

**** APPOINTMENTS FROM TODAY FORWARD ****
```
May 13, 2015@07:29  PA EMERGENCY DEPARTMENT

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

*Presenting complaint: COMPLICATIONS FROM DIABETES

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

**********************************************************************
Date of Last Registration Update:

Additional Registration Information:

**********************************************************************

Want to Edit this Registration Record? NO//

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

*Visit type: UNSCHEDULED//

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

*Was this patient transferred from another facility? NO//

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

*Mode of transport to the ER: PRIVATE VEHICLE/WALK IN/

***THIS PATIENT HAS AN APPOINTMENT IN THIS CLINIC TODAY***

PA EMERGENCY DEPARTMENT FOR : May 13, 2015@07:29

PATIENT IS SCHEDULED FOR: May 13, 2015@07:29

OTHER INFO: :

Check-in to this scheduled visit? NO// NO

BY-PASSING THIS APPOINTMENT: May 13, 2015@07:29

Enter number of labels to print: (0-50): 4//

LABEL PRINTER: NUL// 0  Virtual

00-12-34   F
DEMO, PATIENT
01/01/70  SELLS

00-12-34   F
DEMO, PATIENT
01/01/70  SELLS

00-12-34   F
DEMO, PATIENT
01/01/70  SELLS

00-12-34   F
DEMO, PATIENT
01/01/70  SELLS

Do you want to PRINT a routing slip? YES//

FILE ROOM PRINTER: PAMED1// 0  Virtual
Page 1
OUTPATIENT ROUTING SLIP

DEMO, PATIENT
DOB: 01/01/1970

**CURRENT APPOINTMENTS**

<table>
<thead>
<tr>
<th>TIME</th>
<th>CLINIC</th>
<th>LOCATION</th>
<th>PHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:29 AM</td>
<td>WI PA EMERGENCY DEPARTMENT</td>
<td>ERD</td>
<td>928-669-3296</td>
</tr>
<tr>
<td>7:59 AM</td>
<td>WI PA EMERGENCY DEPARTMENT</td>
<td>ERD</td>
<td>928-669-3296</td>
</tr>
</tbody>
</table>

DATE PRINTED: May 13, 2015@08:00:25
Requested by: EVERETT, BRIAN

Setting data for Dashboard...

ER admission data collection is now complete. Thank you.

Figure 2-1: Sample AMER Admission

Please note that the information displayed above could differ across sites based upon the BEDD site setup options Print Med Rec Worksheet, Print Patient Routing Sheet and Print Arm Band that are described in Section 4-3 Access Setup & Configure Options.

After completing the AMER Admission process, the patient now appears in the EDD in the Check-In section as indicated in Figure 2-2.

Figure 2-2: Patient in “Check-In” status
2.2 Triage Patient and Triage Actions

Once the patient is admitted, triage information can be added before or after assigning the patient to a room. By clicking on the patient’s name in the **Patient (gender)** column indicated in Figure 2-3, the user is taken to the **Patient Edit** screen as shown in Figure 2-4.

![Figure 2-3: Click on patient to edit](image1)

![Figure 2-4: Patient Edit screen](image2)
Triage information is entered into the **Admission Information** section of the **Patient Edit** screen which includes **Presenting Complaint, Initial Acuity, Triaged Date/Time, Triage Nurse & Clinic Type** as indicated in Figure 2-5. After the information is entered, click the **Save/Close** button. The patient will then be moved to the **Triaged** section of the EDD as indicated in Figure 2-6.

If the **Auto Note** box is checked in the setup definition (as documented in section 4-12), actions can also be performed such as **Room Page, Observation** and **Triage Report** for the patient listed in the **Triage** section as indicated in Figure 2-7.
Checking the various actions will auto-populate the notes section in the Info column. See Figure 2-8 and Figure 2-9 for the Rm Page action.

**Figure 2-8:** "Rm Page" button pressed results in a pop-up stating message was added

**Figure 2-9:** Triage Page note appears in the Notes section

Checking the Obsv button will post a note stating that the patient was observed as shown in Figure 2-10. The action will result in an entry getting placed in the Info box as shown in Figure 2-11.

**Figure 2-10:** Message shown when Obsv button is clicked
Checking the **TrgRpt** button will display a triage report for the patient as indicated in Figure 2-12. Once the report is displayed, click the **Return to ED Tracking Board** link on the upper left of the triage report.

If the user checks the **Rm Page** action or the **Obsv** action, the **General Information/Notes** section found on the patient edit page will also be populated with the actions taken. See Figure 2-13 for a sample display.
2.3 Assign Patient to Room

To assign a patient to a room, go to the **Edit Patient** screen by clicking on the patient’s name on the dashboard and enter the room assignment and Primary Nurse information in the **Room Information** section, then click the **Save/Close** button as indicated in Figure 2-14. The user is then returned to the main screen.

The patient now appears in the **Room Management** section of the EDD as indicated in Figure 2-15.
2.4 Update Additional ED Data

Various additional informational elements exist that can be entered and tracked via the ED Dashboard. These include injury, general visit, consult, procedure and diagnosis information.

Each of these elements is accessed by clicking on the patient name anywhere on the EDD’s main screen, which takes the user to the Patient Edit screen.

Please note that a pop-up dialog indicating that a Save will be performed, appears to the user as they move between sections and add data to the various injury, general visit, consult, and procedure and diagnosis sections.

2.4.1 Injury Information

Indicate that the visit was caused by an injury by checking the Yes field in the Injury Information section of the Patient Edit screen, and clicking the Add Injury Information button (Figure 2-16). A pop-up will indicate that changes will be saved when the user clicks OK to continue or Cancel as mentioned in Section 3.4, which will bring up the Injury Worksheet screen (Figure 2-17).

Figure 2-16: Injury Information section of Patient Edit screen
Required data is indicated by fields identified with an asterisk, which include:

- **Town/village where injury occurred** – This is a free text field.
- **Date and time of injury** – This date and time must be prior to the admission date and time.
- **Cause** – To enter a cause, type a search string in the **Cause Lookup** field and then type the tab key once. This will initiate an ICD9/ICD10 lookup. Results will be returned in the **Cause** dropdown box. Select the appropriate ICD9/ICD10 code from the list of results returned.
- **Setting** – The setting in which the injury occurred – This is set of pre-populated choices.
2.4.2 Visit Information

General visit information is entered in the Visit Information section of the Patient Edit screen (Figure 2-18).

2.4.2.1 Visit Information – Date/Time & Provider information

Decision to Admit Time, Medical Screening Exam Time and ED Provider information is entered here.

2.4.3 ED Consults

By clicking on the ED Consult Information button in Figure 2-18, the user can enter consult information in the ED Consult Worksheet as indicated in Figure 2-19. Multiple consults can be entered.
2.4.4 ED Procedures

By clicking on the **Procedure Information** button in Figure 2-18, the user can enter procedure information in the **ED Procedure Worksheet** as seen in Figure 2-20. Multiple procedures can be entered.

![ED Procedure Worksheet](image)

**Figure 2-20 : Procedure Information**

2.4.5 Diagnosis

By clicking on the **Diagnosis Information** button in Figure 2-18, the user can enter diagnosis information in the **ED Diagnosis Worksheet** as shown in Figure 2-21. Multiple diagnoses can be entered.

Please note that a diagnosis is required. If no diagnosis entry is on file yet for the visit, a **.9999/ZZZ.999 UNCODED DIAGNOSIS** entry will be filled in. The narrative will need to be filled in by the user and the entry will need to be saved.

To enter a diagnosis, type a string to search on in the column to the right of the **Search for Diagnosis** label and press the Tab key once. This will initiate an ICD9/ICD10 lookup. Results will be returned in the dropdown box located below the **Search for Diagnosis** label. Select the appropriate code from the list.

At least one entry must be listed as a primary diagnosis.
2.4.6 Additional Notes

Additional general notes can be added on the Patient Edit screen by entering free-text notes in the General Information/Notes section (Figure 2-22) and clicking the Save/Close button.

2.5 Remove Patient from Room

The user can elect to remove the patient from the room before actual discharge in order to free up the room for another patient. This step is completely optional if the patient is being discharged, as the patient will be removed from the room in the event of performing the discharge step.

To remove the patient from a room, check the Remove from Room radio button in the Room Information section of the Patient Edit screen and press the Save/Close button as shown in Figure 2-23. The patient will then appear in the Pending Documentation section of the dashboard as indicated in Figure 2-24.
2.6 Discharge Patient

On the Patient Edit screen, click the Discharge Button. The EDD will validate that information required before proceeding with a discharge action has been entered. If any information is missing, the user is notified with one or more pop-up messages that additional information is required (Figure 2-25). If no additional data is needed, the patient discharge screen will appear as indicated in Figure 2-26.
Figure 2-25: Pop-up dialog stating Primary Diagnosis is required before proceeding with discharge
In order to discharge the patient, disposition information must be entered in the **Disposition Information** section in the **Discharge Patient** screen (Figure 2-27). Upon entering the information, click the **Complete Discharge** button to start the discharge process.

**Figure 2-27:** Disposition Information section of the Discharge page
The required discharge fields are:

- **Final Acuity**
- **Disposition**
- **Follow up Instructions**
- **Primary Provider who signed PCC form**
- **Discharge Nurse**
- **Departure Date/Time**

After clicking the **Discharge** button, the **Complete Discharge** verification is presented asking the user to complete the discharge (Figure 2-28).

![Figure 2-28: Confirm discharge action](image)

After clicking **OK**, the patient will be removed from EDD & AMER (Figure 2-29).
2.7 Discharge Reporting

To display a list of discharges by date from the EDD screen, click the **Discharges** button at the top of the dashboard (Figure 2-30) and the user will be presented with the **Emergency Department DISCHARGES** screen as indicated in Figure 2-31.
Enter the date range that you want to report on and click the Show button as indicated in Figure 2-32.

Select a visit by clicking on the patient name. This will bring up a discharge summary of the visit (Figure 2-33). Click the browser back button to return to the discharge listing.
2.8 ED Dashboard Reporting

A number of management reports can be generated, provided the user has access to the Manager screen. To access the report screen from the EDD main page, click Manager (Figure 2-34), click Reports (Figure 2-35), and the ERS/BEDD Reports screen will be shown (Figure 2-36).
Figure 2-34: Manager button

Figure 2-35: Reports button
Figure 2-36: ERS/BEDD Reports

For each of the reports listed, select the appropriate beginning and ending date for each and click the corresponding **Run Report** button. The browser will then display the requested report. To return to the manager screen, click the **ERS/BEDD Reports Menu** link in the upper right corner of any report.

Current reporting options are:

- Admission Activity (Figure 2-37)

![ERS Admission Summary Report](image)

- Central Log Report (Figure 2-38)
Figure 2-38: Central Log Report

- Check-In Summary by hour (Figure 2-39)

![ED Check-In Summary by Hour](image)

<table>
<thead>
<tr>
<th>Date</th>
<th>Hour</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 15, 2015</td>
<td>13:00</td>
<td>1</td>
</tr>
<tr>
<td>May 13, 2015</td>
<td>07:00</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>2</strong></td>
</tr>
</tbody>
</table>

Figure 2-39: ED Check-In Summary by Hour

- Length of Stay by Acuity (Figure 2-40)

![Length of Stay by Triage Acuity](image)

Figure 2-40: Length of Stay by Triage Acuity

- Discharge Activity by hour (Figure 2-41)

![ED Discharge Summary by Hour](image)

<table>
<thead>
<tr>
<th>Date</th>
<th>Hour</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 16, 2015</td>
<td>20:00</td>
<td>1</td>
</tr>
<tr>
<td>Jan 30, 2015</td>
<td>12:00</td>
<td>1</td>
</tr>
<tr>
<td>May 14, 2015</td>
<td>12:00</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>3</strong></td>
</tr>
</tbody>
</table>

Figure 2-41: ED Discharge Summary by Hour

- Room Utilization (Figure 2-42)
**ERS Room Utilization by Hour**

Between the dates of
01/01/2015 And 5/14/2015

<table>
<thead>
<tr>
<th>May 13, 2015</th>
<th>MUPREP 1</th>
<th>MUPREP 2</th>
<th>MUPREP 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:00</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12:00</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 2-42: ERS Room Utilization by Hour
3.0 Package Management

User access to the EDD is controlled by RPMS security keys. The BEDD application includes two security keys, BEDDZMGR and BEDDZDASH. These keys are documented in Section 5.1 of the BEDD Installation Guide and Release Notes.
4.0 Package Operation

Before using the EDD application, it must be set up to meet the needs of the site with respect to clinic information, and how the application will behave while admitting, processing and discharging patients.

Someone with EDD Manager Access, as described in the *BEDD Installation Guide and Release Notes*, is required to set up bed locations, site information and other settings before the application is used.

4.1 Access the EDD Manager Options

4.1.1 Login to the EDD application

Double-click the icon on your desktop to access the EDD, or enter the dashboard via the appropriate EHR tab, and provide the user’s **RPMS ACCESS/VERIFY** information (Figure 4-1). If accessing via the EHR, the user’s credentials may already have been entered with the initial login to RPMS via the current EHR session, and the user may not see the screen in Figure 4-1.

![Welcome to the BEDD Emergency Room Dashboard Login screen](image)

Figure 4-1: Welcome to the BEDD Emergency Room Dashboard Login screen

4.1.2 Go to the Manager screen

After the user logs in, the user will see the main EDD screen in Figure 4-2. The user should then click the **Manager** button on the top right as indicated below in Figure 4-2.
The first screen to appear is the Manager screen, and it will default to the Rooms definition page as seen in Figure 4-3. Note that unlike Figure 4-3, the user’s particular site will not have rooms defined yet and that definition will be performed in the next step.

4.2 Add ER location

In the screen defined in Figure 4-3, the user enters the room name being added into the Room Name label at the bottom. In the Status section select Active, and under Occupied section select No. Click the Save button and the room will be added as in Figure 4-4.
Note that when adding or changing a room, it can be flagged as No Longer Used or Temporarily Unavailable. The user can also update the room to be listed as Occupied preventing any patients from being assigned the location.

### 4.3 Access Setup & Configure Options

After the bed locations are added and while still in the room definition screen shown in Figure 4-3, click Setup in the upper right corner as indicated in Figure 4-5 and the user will be taken to the site Setup screen in Figure 4-6.
In order to make modifications to a site that is displayed, click on the site name in the ED Dashboard Setup section to make it active as indicated in Figure 4-7.
The site data is automatically populated with INSTITUTION file (#4) entries which are pointed to by the MEDICAL CENTER DIVISION file (#40.8), and new sites can only be added by clinic or hospital management. If the appropriate sites are not displaying, please contact the RPMS system administrator for this installation.

The following options on the site setup screen are available to configure the behavior of the EDD application. Screen shots, where appropriate, will indicate how the setting affects the display of the information in the EDD’s main page.

4.3.1 Screen timeout (in seconds)
This value affects how often screens are refreshed or timed out when logged in to the EDD application.

4.3.2 Operate Dashboard Stand Alone
Not implemented

4.3.3 Use More than 1 Clinic
Display the clinic column in the dashboard under the Check-In, Triaged, Room Management and Pending Documentation sections as indicated in Figure 4-8.
4.3.4 Show Daily Summary on Dashboard
Not implemented

4.3.5 Print Med Rec Worksheet
Print to screen as part of AMER admit (Figure 4-9).

```
Select printer for PATIENT MEDICATION WORKSHEET...

DEVICE: HOME// VT

PRINTED ON 06/21/2012 14:31 PAGE: 1

***ALERT*** PATIENT COPY *** PATIENT COPY *** ALERT ***
RED LAKE HOSPITAL
PATIENT MEDICATION RECONCILIATION
PATIENT APPOINTMENT: 06/21/2012 14:30
LOCATION: URGENT CARE

PATIENT NAME: SMITH, AARON MARK SEX: MALE
CHART #: 115905 DOB: 03/25/2011

***************************************************************************

Figure 4-9: AMER ADMISSION excerpt from Med Rec Worksheet print
```

4.3.6 Print Patient Routing Sheet
Print to screen as part of AMER ADMISSION (Figure 4-10).
Do you want to PRINT a routing slip? YES//

FILE ROOM PRINTER: UC WALKINS// 0 VT Right Margin: 80//

FACILITY: RED LAKE HOSPITAL **Confidential Patient Data**
PAGE 1 OUTPATIENT ROUTING SLIP

SMITH,AARON MARK HRCN: 115905
DOB: 03/25/2011 APPT DT: 6/21/2012@14:30
PO BOX 196
ALBERTA, MINNESOTA 56630

**CURRENT APPOINTMENTS**

<table>
<thead>
<tr>
<th>TIME</th>
<th>CLINIC</th>
<th>LOCATION</th>
<th>PHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:30 PM</td>
<td>WI URGENT CARE</td>
<td>URGENT CARE</td>
<td>218-679-3912</td>
</tr>
</tbody>
</table>

DATE PRINTED: Jun 21, 2012@14:31:04
Requested by: ADAM, SITE

Figure 4-10: AMER ADMISSION excerpt for Print Patient Routing Sheet

4.3.7 Print Arm Band

Print to screen as part of AMER ADMISSION (Figure 4-11).

Enter number of labels to print: (0-50): 4//

LABEL PRINTER: ERL// 0 VT Right Margin: 80//

11-59-05 M
SMITH,AARON MARK
03/25/11 BLACKDUCK

11-59-05 M
SMITH,AARON MARK
03/25/11 BLACKDUCK

11-59-05 M
SMITH,AARON MARK
03/25/11 BLACKDUCK

11-59-05 M
SMITH,AARON MARK
03/25/11 BLACKDUCK

Figure 4-11: AMER ADMISSION excerpt for Print Arm Band

4.3.8 Show Used Room

Not Implemented
4.3.9 Show Provider

Display the Provider column in the dashboard under the Triaged, Room Management and Pending Documentation sections as indicated in Figure 4-12.

![Figure 4-12: Provider column](image1)

4.3.10 Show Nurse

Display the Nurse column in the dashboard under the Triaged, Room Management and Pending Documentation sections as indicated in Figure 4-13.

![Figure 4-13: Nurse Column](image2)
4.3.11 Show Consult

Display the Consult column in the dashboard under the Triaged, Room Management and Pending Documentation sections as indicated in Figure 4-14.

![Figure 4-14: Consult Column](image)

4.3.12 Use Auto Note

Auto-update the notes field when Trg Page (Triage Page), Rm Page (Room Page) or Obsv (Patient Observed) options are checked on a patient in the dashboard in the Check-In, Triaged, Room Management or Pending Documentation sections. See an example of Trg Page being used to page for triage as indicated in Figure 4-15 through Figure 4-17.

![Figure 4-15: Click "Trg Page" action](image)
4.3.13 Use Comm Board
Not Implemented

4.3.14 Print Triage Report on Save
Not Implemented
4.3.15  Switch EHR Patient on Edit

If this box is checked, when utilizing the dashboard within EHR, whenever a patient is edited on the dashboard, the EHR patient and visit will automatically switch to the patient and visit being edited in the dashboard. If the box is not checked, the switch will not occur. Note that this setting only applies to EHR mode. When utilizing standalone mode, the patient/visit will not switch upon a patient edit.

4.3.16  Reg column on main display

The Reg column on the main display is used to indicate whether the patient’s registration file was updated on the current date. For example the user would have accessed RPMS Patient Registration (AG) and edited one of the patient’s fields. If an edit was not made, it will display No with a yellow background as indicated in Figure 4-18.

If a change is made, as in the case of modifying a street address, it will display Yes with a white background as indicated in Figure 4-19.

Finally, a check is performed on the patient’s AG Tribe of Membership field (AG page 2). If the tribe is NON-INDIAN BENEFICIARY, NoBens is attached as a suffix to the value in the Reg column as indicated in Figure 4-20.
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 this IHS Web site: [http://security.ihs.gov/](http://security.ihs.gov/).

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

A.1 All RPMS Users

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

A.1.1 Access

RPMS users shall

- Only use data for which 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

**Emergency Room System**

Refers to the RPMS ERS application (in the AMER namespace). The EDD is integrated with the ERS application so information gets transferred back and forth between the two applications.

**RPMS Patient Care Component**

Refers to functions within RPMS as a clinical data repository, storing visit-related data about a patient.
## Acronym List

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Term Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG</td>
<td>Patient Registration</td>
</tr>
<tr>
<td>ED</td>
<td>Emergency Department</td>
</tr>
<tr>
<td>EDD</td>
<td>IHS Emergency Department Dashboard</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>ERS</td>
<td>Emergency Room System</td>
</tr>
<tr>
<td>HHS</td>
<td>Health and Human Services</td>
</tr>
<tr>
<td>IHS</td>
<td>Indian Health Service</td>
</tr>
<tr>
<td>RPMS</td>
<td>Resource and Patient Management System</td>
</tr>
</tbody>
</table>
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/helpdesk/
Email:  support@ihs.gov