



RESOURCE AND PATIENT MANAGEMENT SYSTEM

CIA Generic Retrieval Utility

(GRU)

User Manual

Version 1.4
February 2012

Office of Information Technology (OIT)
Division of Information Resource Management
Albuquerque, New Mexico

Table of Contents

1.0	Introduction.....	1
2.0	Starting the Utility.....	2
2.1	Security Key	2
2.2	Host System	2
3.0	Query Status View	4
4.0	Query Result View	6
5.0	Query Management	9
5.1	Run a Query	10
5.2	Query Wizard dialog	11
5.2.1	View Field Descriptions	14
5.2.2	View and Edit Properties	14
5.2.3	Edit Criteria Values.....	17
5.2.4	Define a Computed Value	18
5.2.5	Define a Relation	20
5.2.6	Configure Linked Files.....	20
	Acronym List	32
	Contact Information	33

Preface

This manual contains the user guide for the Generic Retrieval Utility (GRU). Included are an introduction and information on starting the utility.

Warning: GRU is intended for use with the certified EHR to monitor the RPMS Audit Log for monitoring user access to patients and what data was entered or changed. Although other files are searchable, the GRU is not a replacement for standard FileMan searching at this time. Use with caution, and check search results carefully.

1.0 Introduction

The Generic Retrieval Utility (GRU) is an extremely powerful tool that permits constructing and executing complex queries against FileMan databases using an intuitive graphical user interface. Results of queries may be viewed, exported to external applications, or output in a variety of customizable report formats.

2.0 Starting the Utility

The GRU utilizes the VueCentric® Framework to communicate with the host system. The Framework handles user authentication and all host system interaction. Depending on how the system is configured, the logon sequence will vary.

2.1 Security Key

To access GRU the user must have the CIAZGRU security key assigned by the Clinical Application Coordinator (CAC). Otherwise, access to the application is denied.

2.2 Host System

If a host system is not specified in the command line when the application is started, and if more than one host system is defined for the Framework, the **Connect To** dialog displays (Figure 2-1).

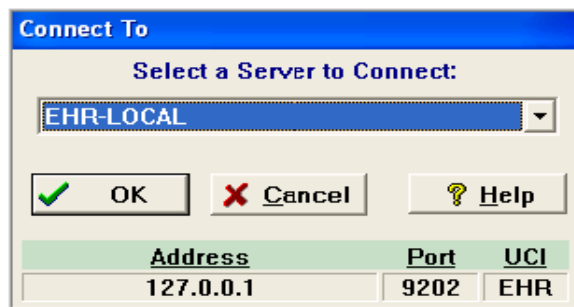


Figure 2-1: **Connect To** dialog

If so prompted, select the server and click **OK**.

If the system is not configured to use NT authentication, the **VueCentric Logon** dialog (Figure 2-2) displays.

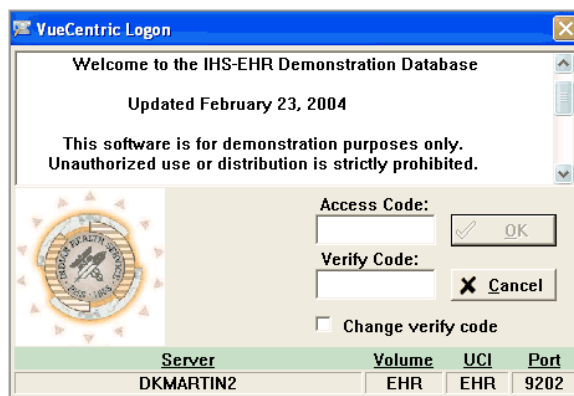


Figure 2-2: **VueCentric Logon** dialog

To log on:

1. Type the **Access Code**.
2. Type the **Verify Code**.
3. Click **OK**.

These are the same codes used to log on to the RPMS/VistA system.

3.0 Query Status View

Upon successful logon, the Generic Retrieval Utility window (Figure 3-1) displays showing all queries submitted by the user.

QUERY	TASK ID	STATUS	STARTED	COMPLETED	RETRIEVED	SCANNED
TEST	2150	ABORTED	7/14/2004 9:07:36 AM	7/14/2004 9:08:22 AM	1649	8395
TEST	2182	COMPLETED	7/16/2004 9:23:24 AM	7/16/2004 9:41:46 AM	2699	612106
PATIENTS	2185	PENDING			0	0
PATIENTS	2186	EXECUTING	7/16/2004 9:45:48 AM		2400	2400

Figure 3-1: **Generic Retrieval Utility** window, Initial Query view

The column entries have the following meanings:

- QUERY:** This is the name of the query. Uniqueness is not enforced, but is highly recommended to avoid confusion.
- TASK ID:** This is the identifier of the background task assigned to execute the query. This identifier is unique and may be used to distinguish different runs of the same query.
- STATUS:** This is the current status of the query. Possible statuses are:
- PENDING** The query has been submitted for execution, but has not begun execution.
 - EXECUTING** The query is currently executing.
 - ABORTING** The query has been asked to abort, but has not yet done so.
 - ABORTED** The query has been aborted.
 - COMPLETED** The query has executed to completion.
 - ERROR** An unexpected error has occurred during execution. The system error trap should provide additional information as to the cause.
- STARTED:** This is the date and time that execution of the query started. This is blank for queries that have not yet begun execution.
- COMPLETED:** This is the date and time that execution of the query stopped, regardless of the cause.

RETRIEVED: This is the number of top level records retrieved. For executing queries, this count is updated dynamically.

SCANNED: This is the number of top level records scanned. For executing queries, this count is updated dynamically.

The task bar has several buttons that perform various functions. Some buttons may be enabled or disabled, depending on which query is currently selected. The function of each button is described below:



Load

Loads the result of the selected query and displays it in the Query Result View (Section 4.0). This button is enabled only for queries whose status is COMPLETED or ABORTED.



Rerun

Re-runs the selected query using the same criteria as the original. This button is enabled only for queries whose status is COMPLETED or ABORTED.



Abort

Aborts a running query. When a running query is aborted, its status first changes to ABORTING while it is performing cleanup operations, and then to ABORTED when execution finally stops. This button is enabled only for queries whose status is EXECUTING.



Delete

Deletes the currently selected query. This button is enabled for queries whose status is COMPLETED, ABORTED, or ERROR.



Refresh

Refreshes the query list.



Query Manager

Invokes the **Query Manager** dialog (Section 5.0).



Help

Displays the online Help.

4.0 Query Result View

Clicking **Load** at the Query Status View displays the Query Result View (Figure 4-1) for the selected query. This dialog displays the results of the selected query in a grid. Scroll horizontally and vertically through the grid to view results:

#	VISIT/ADMIT DATE&TIME	CLINIC	HOSPITAL LOCATION	V MEDICATION.VISIT	V LAB.VISIT	V PROVIDER.VISIT	V POV.VISIT
29176	JUN 13, 1993@08:35			(DATASET)	(DATASET)	(DATASET)	(DATASET)
29177	JUN 13, 1993@10:06			(DATASET)	(DATASET)	(DATASET)	(DATASET)
29178	JUN 13, 1993@10:31			(DATASET)	(DATASET)	(DATASET)	(DATASET)
29182	JUN 13, 1993@13:29	OBSTETRICS		(DATASET)	(DATASET)	(DATASET)	(DATASET)
29183	JUN 13, 1993@14:50			(DATASET)	(DATASET)	(DATASET)	(DATASET)
29184	JUN 14, 1993@08:00	PHARMACY		(DATASET)	(DATASET)	(DATASET)	(DATASET)
29185	JUN 14, 1993@08:20	OPHTHALMOLOGY		(DATASET)	(DATASET)	(DATASET)	(DATASET)
29186	JUN 14, 1993@08:45	ENT		(DATASET)	(DATASET)	(DATASET)	(DATASET)
29189	JUN 14, 1993@08:50	PHARMACY		(DATASET)	(DATASET)	(DATASET)	(DATASET)

Figure 4-1: Query Result view

The title bar displays the query name, its associated task identifier, and total record count. Each exported field is represented in a column of the grid. A column may be resized by dragging its respective boundary lines, or re-ordered by dragging its column header.

Two types of fields deserve special mention: **MEMO** and **DATASET**. Each of these field types is displayed in the grid with the field type in parentheses.

A **MEMO** field is a variable length, free text field. Double-clicking a cell containing a **MEMO** field displays a dialog containing the contents of the field in a scrollable window (Figure 4-2).

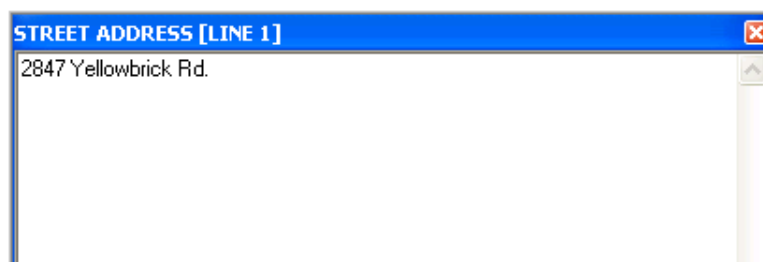
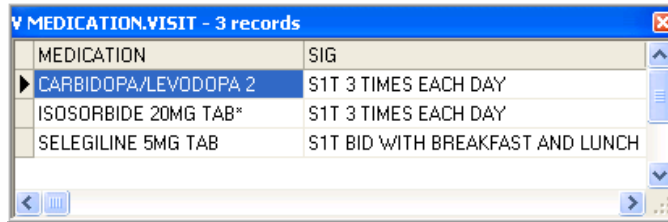


Figure 4-2: **MEMO** field dialog

A **DATASET** field is produced when the underlying query retrieves a field that is a multiple (for example, a subfile) or when a join links to a subset of another file's data. Double-clicking a cell containing a **DATASET** field displays a dialog containing all the data contained within that subfile or joined file (Figure 4-3).



MEDICATION	SIG
CARBIDOPA/LEVODOPA 2	S1T 3 TIMES EACH DAY
ISOSORBIDE 20MG TAB*	S1T 3 TIMES EACH DAY
SELEGILINE 5MG TAB	S1T BID WITH BREAKFAST AND LUNCH

Figure 4-3: **DATASET** field dialog

Changing the selected record in the parent grid also changes the data displayed in each child grid. Multiple child grids may be opened (which in turn may contain **DATASET** fields that may be similarly viewed) and their contents viewed while changing the selection in the parent grid. In this way, deeply nested results may be readily viewed.

The tool bar of the Query Result View has two buttons:



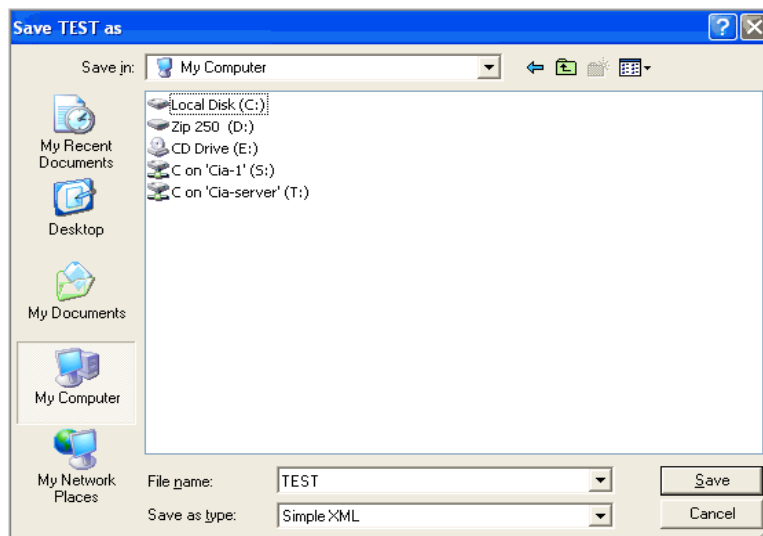
Links the result dataset with ReportBuilder®, a third party report generator.



This button permits saving the result dataset in one of three output formats:

- **Simple XML** – This is the most common format supported by third-party applications.
- **ADO XML** – This is the XML-based format defined in the Microsoft ADO specification.
- **ADO Binary** – This is the binary format defined in the Microsoft ADO specification.

Regardless of the output format chosen, the application prompts for a filename.

Figure 4-4: **Save as** dialog

To save the query results:

1. Choose a destination folder.
2. Type the **File name**.
3. Choose the **Save as type**.
4. Click **Save**.

The resulting file may be imported into a third-party application for further manipulation.

5.0 Query Management

Click **Query Manager** at the **Query Status View** (Figure 3-1) to display the **Query Management** dialog:

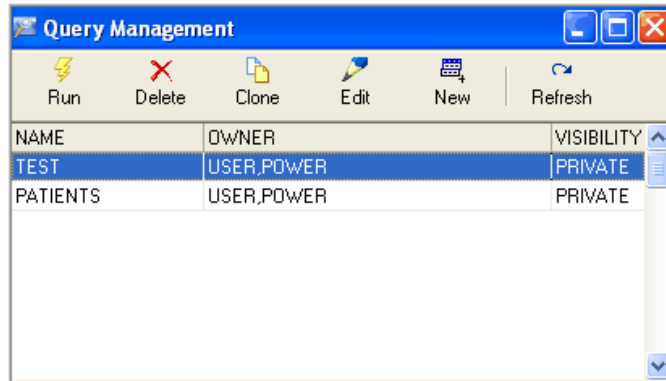


Figure 5-1: **Query Management** dialog

This dialog displays all available query definitions. Each user has access to any query definition that the user created as well as restricted access to all definitions declared as public. The following columns are displayed:

- **NAME** – The name of the query. Names do not have to be unique, but this practice is highly recommended to avoid confusion.
- **OWNER** – The owner (creator) of the query definition.
- **VISIBILITY** – The visibility level of the query definition and may be either:
 - **PUBLIC** – The query may executed or cloned by any user.
 - **PRIVATE** – The query is accessible only to the owner.

The tool bar contains the following buttons:



Run

Runs the selected query. If user-supplied criteria are required for the query, prompts are provided. Execution may be scheduled for a future time if desired. See Section 5.1



Delete

Deletes the selected query definition. This button is enabled only for queries that the user owns.



Clone

Clones the selected query definition. Prompts for a new query name and description are provided. Any public or owned query definition may be cloned.



Edit

Invokes the Query Wizard dialog (Section 5.2) for the selected query definition. Only edit owned queries may be edited.



Prompts for properties for a new query definition and then displays the Query Wizard dialog (Section 5.2) for the new definition.



Refreshes the contents of the Query Manager display.

5.1 Run a Query

Click **Run** at the **Query Management** dialog to display the **Run Query** dialog. The configuration of this dialog depends on the configuration of the associated query definition. If the query definition requires user-supplied criteria values, the dialog prompts for these values (Figure 5-2).

The dialog box is titled "Run Query - PATIENTS". It contains the following elements:

- A section titled "Date of birth must be between:" with two text boxes: "DATE OF BIRTH Start" and "DATE OF BIRTH End".
- A separator "- and -".
- A section titled "State of residence must be one of:" with a text box labeled "STATE" and a list box labeled "Values (1)" containing "INDIANA".
- A section titled "Schedule to run at:" with a text box showing "16-Jul-2004 11:12" and "..." and two buttons: "Submit" and "Cancel".

Figure 5-2: **Run Query** dialog, search criteria required

If no user-supplied criteria are defined, the **Run Query** dialog looks like Figure 5-3.

The dialog box is titled "Run Query - TEST". It contains the following elements:

- A message: "Click Submit to run this query or Cancel to cancel the request."
- A section titled "Schedule to run at:" with a text box showing "16-Jul-2004 11:13" and "..." and two buttons: "Submit" and "Cancel".

Figure 5-3: **Run Query** dialog, search criteria not required

To run a query:

1. Set any requested criteria values.
2. Set the **Schedule to run at** date and time (defaults to now).
3. Click **Submit**.

5.2 Query Wizard dialog

Click **Edit** or **New** at the **Query Management** dialog to display the **Query Wizard** dialog (Figure 5-4).

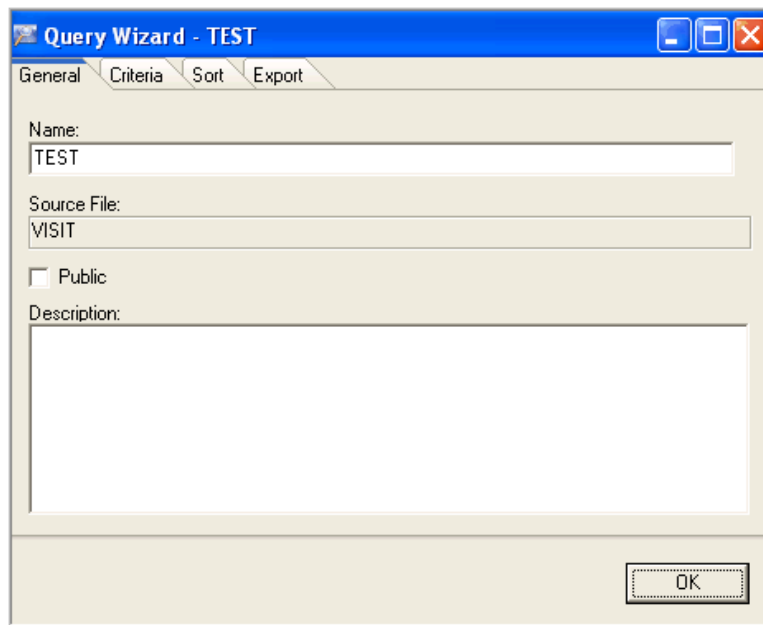


Figure 5-4: **Query Wizard** dialog, **General** tab

This dialog contains four tabs:

- **General** - The following values may be edited:
 - **Name** – The name of the query.
 - **Public** – Select to make the query public (available to all users).
 - **Description** – A free-form text field.

The **Source File** name (“VISIT” in Figure 5-4) cannot be changed.

- **Criteria** - Permits selecting fields to be used as selection criteria in determining which records are exported.
- **Sort** - Permits selecting fields that are used to sort the exported records.
- **Export** - permits specifying which fields are to be included in the exported data.

The **Criteria**, **Sort**, and **Export** tabs have a similar appearance.

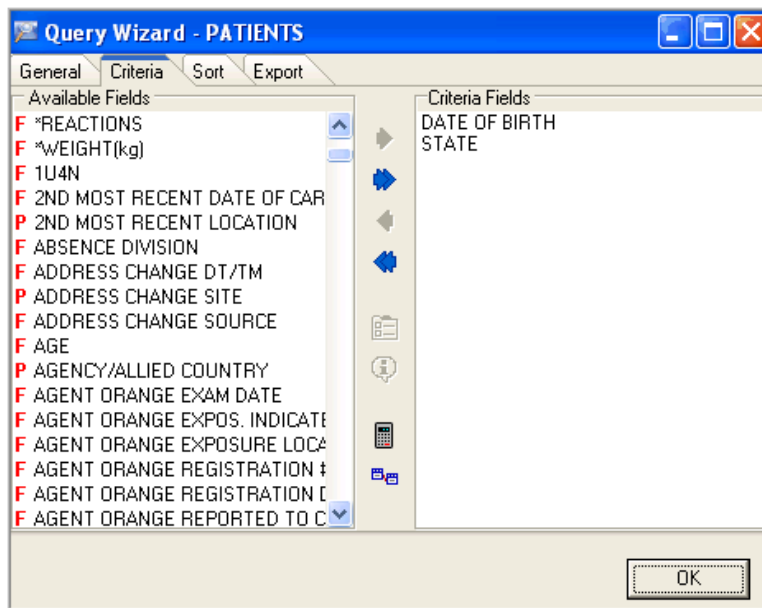


Figure 5-5: Query Wizard dialog, Criteria tab

The **Available Fields** (left) pane contains a list of all available fields from the source file, as well as any computed values or relations (joins) defined for the query. The single character to the left of each field name (displayed in red), indicates the type of entry. Possible values are:

- **C** – computed value
- **F** – other field
- **J** – join
- **M** – multiple field
- **P** – pointer field

This pane has the following functionality:

- Click an item to select it.
- To select multiple, non-contiguous items, press and hold the Ctrl key while clicking the desired items.
- To select multiple, contiguous items, select the first item, then press and hold the Shift key, and select the last item.
- Double-click an item to immediately add it to the right list box.

The right pane contains a list of fields that were previously added to the parameter list. For each of the three tabs, this list has a different name, and the contents will likely differ. This pane has the following functionality:

- Click an item to select it. Multiple selections are not permitted.
- Double-click an item to open the property editor for that item.
- Change the sequence of entries in this list by dragging an entry up or down to its desired location.

The tool bar located between the two lists contains the following buttons:



Right Arrow button - Moves the selected item(s) from the left list to the right list.

Note: Any item may be added more than once. While this makes sense for criteria and export operations, it does not for sort operations.



Double Right Arrow button - Moves all items in the left list to the right list.



Left Arrow button - Removes the selected item from the right list.



Double Left Arrow button - Removes all items from the right list.



Properties button - Opens the property editor for the selected entry. Each parameter type (criteria, sort, or export) has its own property editor (Figure 5-7, Figure 5-8, or Figure 5-9). In addition, items that represent field multiples or relations (joins) display another instance of the **Query Wizard** dialog for the target file or subfile. See Section 5.2.6 for more information on configuring linked files.



Information button - Displays detailed information on all items selected in the left list box. For fields, this includes the descriptive and prompt text associated with each field. For computed values and joins, the descriptive text associated with those entries is displayed.



Computed Value button - Opens the **Computed Value** dialog to define a computed value. This entry is added to the left list box.

Note: This entry does not become permanent unless it is added to at least one of the right list boxes before closing the wizard.



Relation button - Opens the **Define a Relation** dialog, permitting a relation (join operation) between the source file and another file to be defined.

5.2.1 View Field Descriptions

Click the Information button at the **Query Wizard** dialog to display the **Field Descriptions** dialog (Figure 5-6). This dialog displays information about all selected entries in the **Available Fields** list of the wizard.

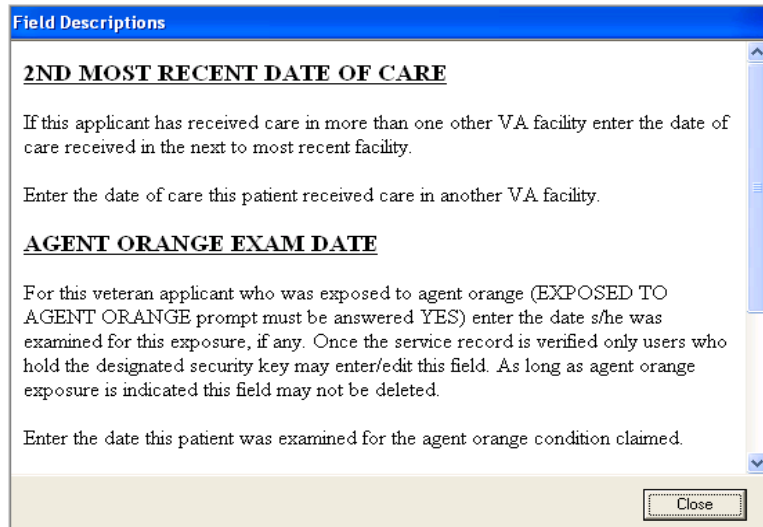


Figure 5-6: **Field Descriptions** dialog

5.2.2 View and Edit Properties

5.2.2.1 Criteria Properties

At the **Query Wizard** dialog, **Criteria** tab, select an item and click the Properties button (or double-click an item in the right list) to open the **Criteria Properties** dialog (Figure 5-7).

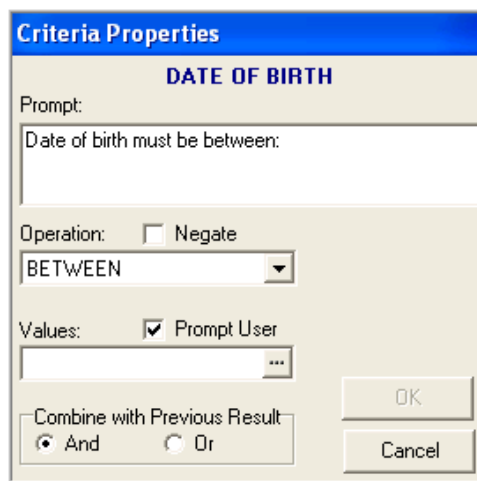


Figure 5-7: **Criteria Properties** dialog

Note: If the associated field is a pointer type, an additional button, labeled **Link**, displays. Click **Link** to configure parameters for the file that is the target of the pointer. See Section 5.2.6 for more information.

The **Criteria Properties** dialog contains the following fields:

Prompt	This is the prompt that displays when prompting for a criteria value. For criteria not marked as Prompt User (see below), this information is still useful for documenting the purpose of the criterion.
Operation	Shows the operation to be performed in the evaluation of this criterion. The available selections depend upon the datatype of the associated field or computed value. Possible selections are: <ul style="list-style-type: none"> < Field value must be less than the specified value. <= Field value must be less than or equal to the specified value. <> Field value must not be equal to the specified value. = Field value must be equal to the specified value. > Field value must be greater than the specified value. >= Field value must be greater than or equal to the specified value. BETWEEN Field value must be within the specified inclusive range. CONTAINS Field value must contain the specified value. ENDS WITH Field value must end with the specified value. STARTS WITH Field value must start with the specified value. ONE OF Field value must be one of the specified values.
Negate	Negate the result of the operation.
Values	One or more criterion values to be used in the operation. The number of values required depends upon the operator. Click ellipsis (...) to display the Edit Criteria Values dialog. If the criterion is marked as Prompt User , the values entered here become the default values seen by the user when prompted.
Prompt User	If checked, the user is prompted for values for this criterion when submitting the query for execution.

Combine with Previous Result Determines how the result of this operation is combined with the previous result.

5.2.2.2 Sort Properties

At the **Query Wizard** dialog **Sort** tab, select an item and click the Properties button to open the **Sort Properties** dialog (Figure 5-8).

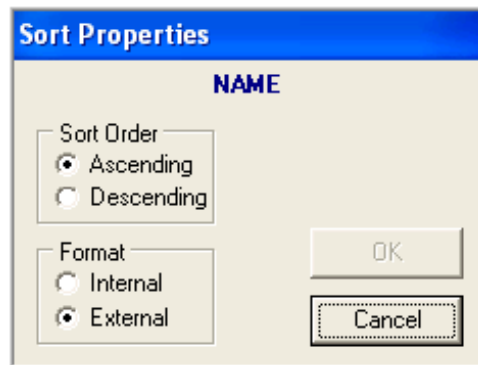


Figure 5-8: **Sort Properties** dialog

Note: If the associated field is a pointer type, an additional button, labeled **Link**, displays. Click **Link** to configure parameters for the file that is the target of the pointer. See Section 5.2.6 for more information.

Select the desired sort order and whether the field's internal or external format is to be used for sorting. The choice of format largely depends on the datatype of the field. For example, date fields should typically use internal format so that ordering is chronological. On the other hand, pointer fields should use external format so that sorting occurs alphabetically rather than based on internal entry number. The utility selects the best format for the datatype by default, but this may be overridden as desired.

5.2.2.3 Export Properties

At the **Query Wizard** dialog, **Export** tab, select an item and click the Properties button to open the **Export Properties** dialog (Figure 5-9).

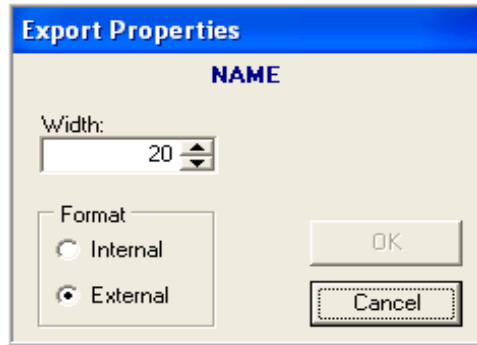


Figure 5-9: **Export Properties** dialog

Note: If the associated field is a pointer type, an additional button, labeled **Link**, displays. Click **Link** to configure parameters for the file that is the target of the pointer. See Section 5.2.6 for more information.

Set the width property to the maximum allowable width for this field. Field values in excess of this setting are truncated. Setting this to zero allows values of any width.

Set the format property to the format to be exported. When internal values are exported, the datatype for the corresponding field in the result dataset matches that of the source field whenever possible (for example, if the source field is a Boolean value, the corresponding field in the result dataset is also Boolean). When external values are exported, the datatype of the corresponding field in the result dataset is always of type string.

5.2.3 Edit Criteria Values

The Edit Criteria Values dialog permits entry of default criterion values. The appearance of this dialog is dependent upon the type of operation being performed in evaluation of the criterion.

For a simple comparison operator (for example, =), the dialog shown in Figure 5-10 displays:

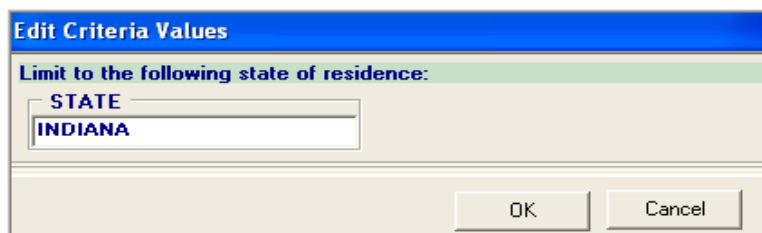


Figure 5-10: **Edit Criteria Values** dialog

For an operation that requires a range (for example, BETWEEN), the dialog shown in Figure 5-11 displays:

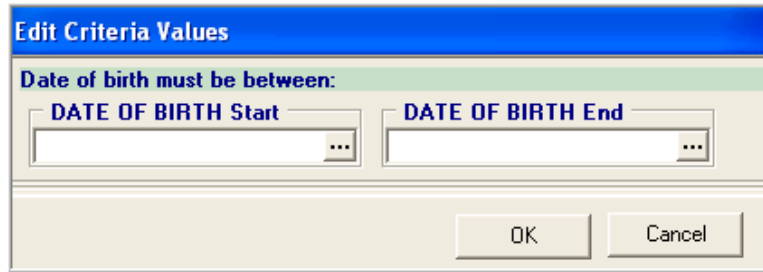


Figure 5-11: **Edit Criteria Values**, range of values dialog

For an operation that allows multiple values (for example, ONE OF), the dialog shown in Figure 5-12 displays:

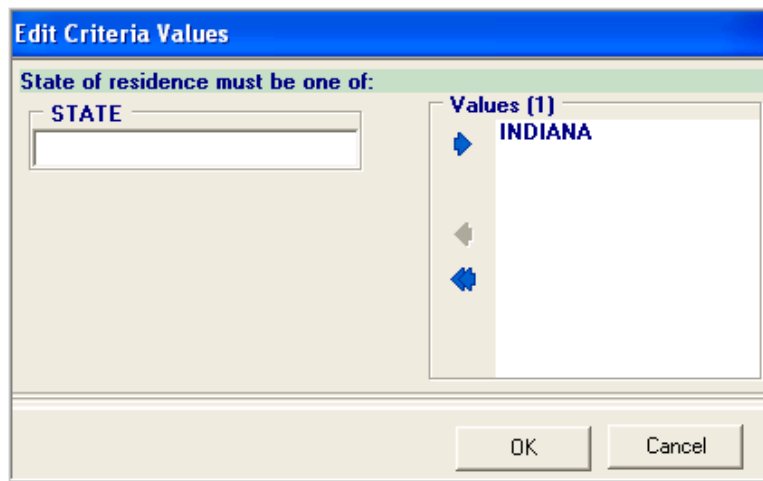


Figure 5-12: **Edit Criteria Values**, multiple values dialog

A value may be added to the rightmost list by typing it in the left field and clicking the right arrow button. The left arrow and double left arrow buttons remove the selected or all items, respectively, from the list.

5.2.4 Define a Computed Value

Click the Computed Value button on the **Query Wizard** dialog to display the **Create a Computed Value** dialog (Figure 5-13).

Figure 5-13: **Create a Computed Value** dialog

The following fields may be defined:

- Name** A descriptive name for the computed value. This is the name that will display in the Query Wizard dialog list boxes.
- Return Type** The datatype returned by the computed value. May be one of:
- **BOOL** – A Boolean value
 - **DATE** – A date only value
 - **DATETIME** – A date and time value
 - **INTEGER** – An integer
 - **REAL** – A real number
 - **TEXT** – Free text
 - **TIME** – A time only value
- Execution Logic** The M logic that sets the value of the computation. The value should be set in the variable X, or if different internal and external values are to be returned, in X("I") and X("E"), respectively.
- Description** An optional (but highly recommended) freeform text description of this computed value.

Once the required fields have been entered, click **OK** to add the computed value to the left list-box in the **Query Wizard** dialog. Once there, it is selectable for inclusion in criteria, sort, or export parameters.

Note: Unless the computed value is added to at least one of these parameter groups before closing the Wizard, it will be deleted.

5.2.5 Define a Relation

Click the Relation button on the **Query Wizard** dialog to display the **Define a Relation** dialog (Figure 5-14).

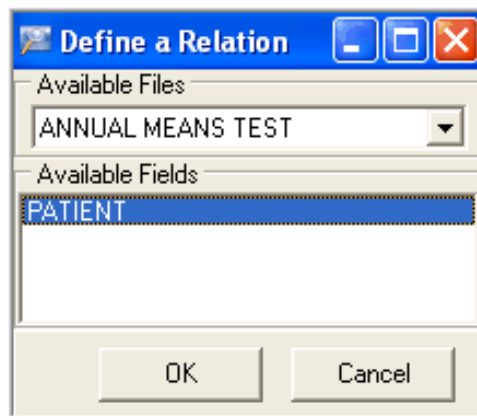


Figure 5-14: **Define a Relation** dialog

The **Available Files** list displays all files that have at least one indexed field that points to the source file. Once a file is selected, all candidate fields are displayed in the **Available Fields** list.

Note: A field is a candidate only if it is a top level field that is a pointer to the source file and for which a standard cross reference is defined.

Once a file and field are selected, click **OK** to add an entry to the left list-box of the **Query Wizard** dialog. The name of this entry consists of the file and field names separated by a period (for example, from the selections in Figure 5-14, the entry would be ANNUAL MEANS TEST.PATIENT).

5.2.6 Configure Linked Files

A linked file is a file (or subfile) that is linked to the source file via a pointer field, a multiple field, or a defined relation. The **Query Wizard** dialog is used to configure a linked file in a manner nearly identical to configuring the primary source file, with the following exceptions:

- The visibility (public/private) of a query definition associated with the linked file cannot be modified.

- Only one tab (**Criteria**, **Sort**, or **Export**) is visible in the **Query Wizard** dialog, depending on which of these tabs was used to display the wizard for the linked entry.

The **Query Wizard** dialog for a linked file may be displayed in one of three ways:

- Click the **Link** button in the Property Editor of a pointer field. In this case, the target (pointed to) file displays in the **Query Wizard** dialog.
- Click the Properties button in the **Query Wizard** dialog for an item that is a relation (join). In this case, the joined file displays in the **Query Wizard** dialog.
- Click the Properties button in the **Query Wizard** dialog for an item that is a multiple field. In this case, the subfile displays in the **Query Wizard** dialog.

For example, selecting properties for an export item that represents a join between the source file (for example, VISIT file) and a target file (for example, V MEDICATION file) would display a new instance of the **Query Wizard** dialog, but now with the target file becoming the source file.

Note: In this example, only the **Export** tab is visible, since this is the tab from which the **Query Wizard** dialog was displayed.



Figure 5-15: **Query Wizard** dialog, **Export** tab for linked file

Finally, one additional point about linked files merits discussion. Records from a file linked by way of a pointer field are considered to be at the same level as those from the parent file, since this type of link represents a one-to-one relationship between records from each of the two files. Think of this kind of link as concatenating records from two separate files. In contrast, records from a file linked by way of a relation or a multiple field are linked to the parent record in a many-to-one relationship. These linked records are represented as nested datasets. Think of this kind of link as analogous to subfiles in FileMan.

The distinction between these two classes of links is important in that criteria, sort, and export parameters apply to the current dataset level. For example, criteria parameters for a pointer-linked file affect whether or not the parent record is selected. In contrast, criteria parameters for a file linked by way of a relation or multiple fields affect selection of records within that file only.

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/>.

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.

Acronym List

CAC	Clinical Application Coordinator
GRU	Generic Retrieval Utility
IHS	Indian Health Service
RPMS	Resource and Patient Management System

Contact Information

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

Phone: (505) 248-4371 or (888) 830-7280 (toll free)

Fax: (505) 248-4363

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

Email: support@ihs.gov