RESOURCE AND PATIENT MANAGEMENT SYSTEM

Drug Accountability

(PSA)

GUI Invoice Upload Program User Guide

Version 1.0
April 2011

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

Table of Contents

Preface

The purpose of this document is to provide information about use of the PSA Graphical User Interface Invoice Upload Program.

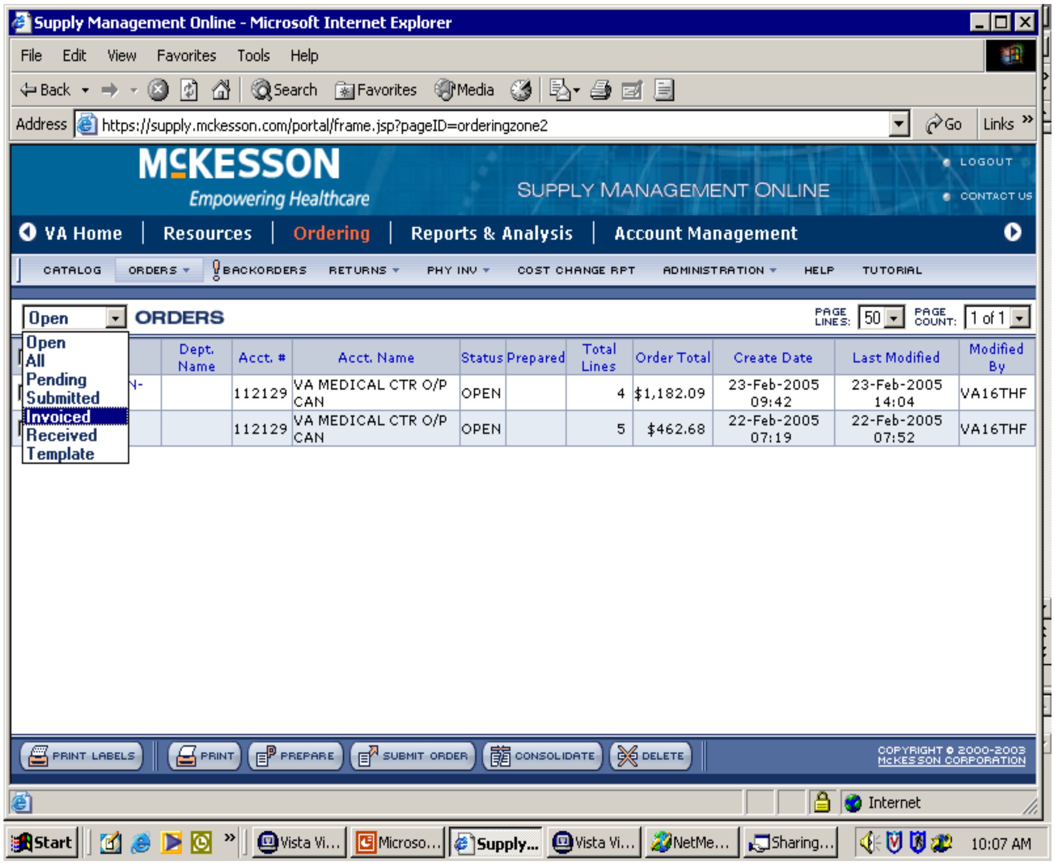
1.0 Introduction

This manual provides the information necessary for the use of the Graphical User Interface (GUI) Invoice Upload program for Inventory Management (PSA) in the Resource and Patient Management System (RPMS).

2.0 GUI Invoice Upload Program

The GUI Invoice Upload Program was released as part of APSP 1010.

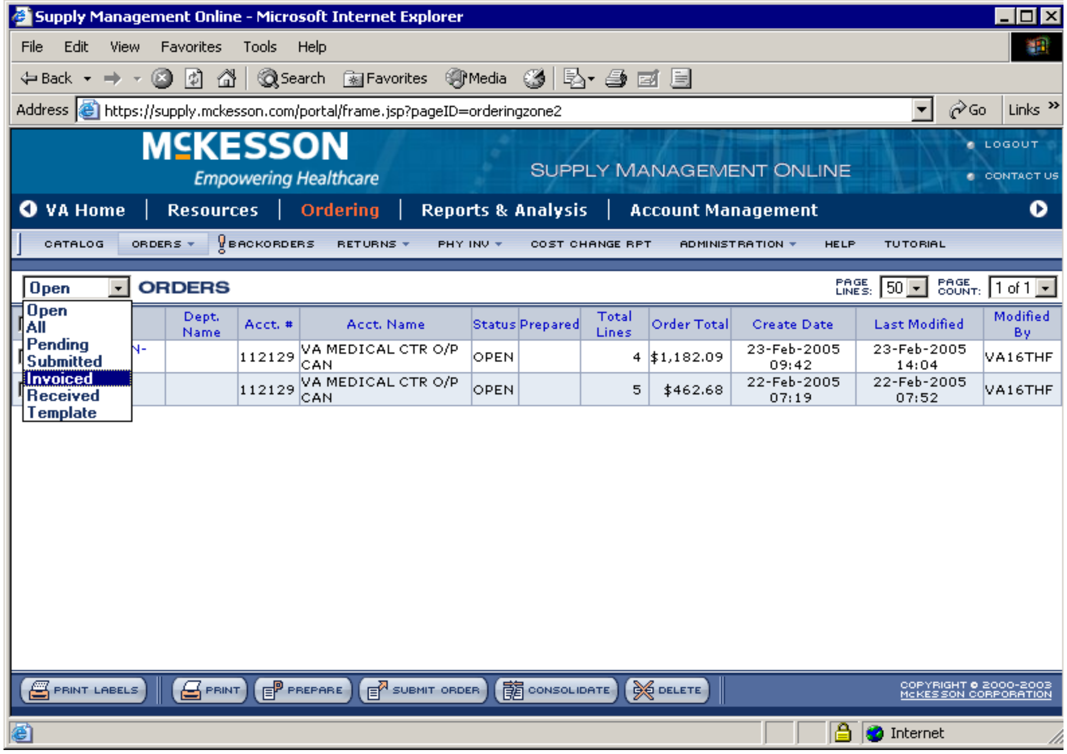
2.1 McKesson Invoice Download


Supply Management Online - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://supply.mckesson.com/portal/frame.jsp?pageID=orderingzone2
Go Links
MCKESSON
Empowering Healthcare
SUPPLY MANAGEMENT ONLINE
LOGOUT
CONTACT US
VA Home | Resources | Ordering | Reports & Analysis | Account Management
CATALOG ORDERS BACKORDERS RETURNS PHY INV COST CHANGE RPT ADMINISTRATION HELP TUTORIAL
Open
ORDERS
PAGE LINES: 50
PAGE COUNT: 1 of 1
Open
All
Pending
Submitted
Invoiced
Received
Template
PRINT LABELS PRINT PREPARE SUBMIT ORDER CONSOLIDATE DELETE
COPYRIGHT © 2000-2003 MCKESSON CORPORATION
Internet
Start Vista Vi... Microso... Supply... Vista Vi... NetMe... Sharing... 10:07 AM

Dept. Name	Acct. #	Acct. Name	Status	Prepared	Total Lines	Order Total	Create Date	Last Modified	Modified By
	112129	VA MEDICAL CTR O/P CAN	OPEN		4	$1,182.09	23-Feb-2005 09:42	23-Feb-2005 14:04	VA16THF
	112129	VA MEDICAL CTR O/P CAN	OPEN		5	$462.68	22-Feb-2005 07:19	22-Feb-2005 07:52	VA16THF

Figure 2-1: McKesson Orders Web page

Log on to the McKesson Web site and click **Ordering.**

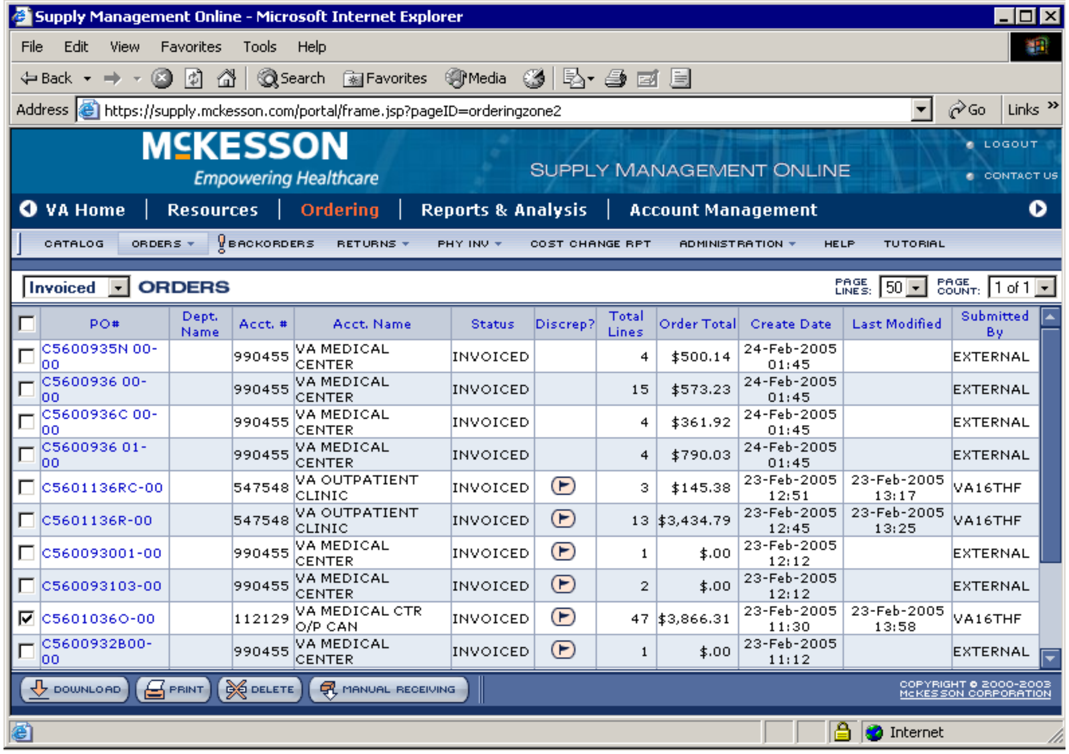

Supply Management Online - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://supply.mckesson.com/portal/frame.jsp?pageID=orderingzone2
Go Links
MCKESSON
Empowering Healthcare
SUPPLY MANAGEMENT ONLINE
LOGOUT
CONTACT US
VA Home | Resources | Ordering | Reports & Analysis | Account Management
CATALOG ORDERS BACKORDERS RETURNS PHY INV COST CHANGE RPT ADMINISTRATION HELP TUTORIAL
Open
ORDERS
PAGE LINES: 50
PAGE COUNT: 1 of 1
Open
All
Pending
Submitted
Invoiced
Received
Template
PRINT LABELS
PRINT
PREPARE
SUBMIT ORDER
CONSOLIDATE
DELETE
COPYRIGHT © 2000-2003 MCKESSON CORPORATION
Internet

	Dept. Name	Acct. #	Acct. Name	Status	Prepared	Total Lines	Order Total	Create Date	Last Modified	Modified By
N-		112129	VA MEDICAL CTR O/P CAN	OPEN		4	$1,182.09	23-Feb-2005 09:42	23-Feb-2005 14:04	VA16THF
		112129	VA MEDICAL CTR O/P CAN	OPEN		5	$462.68	22-Feb-2005 07:19	22-Feb-2005 07:52	VA16THF

Figure 2-2: Drop-down menu

In the drop down box at left, choose **Invoiced.**

If you do not have **Invoiced** as an option, contact your McKesson representative or Indian Health Service (IHS) National Supply Service Center to enable invoice downloading on your account.


Supply Management Online - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://supply.mckesson.com/portal/frame.jsp?pageID=orderingzone2
Go Links
MCKESSON
Empowering Healthcare
SUPPLY MANAGEMENT ONLINE
LOGOUT
CONTACT US
VA Home | Resources | Ordering | Reports & Analysis | Account Management
CATALOG ORDERS BACKORDERS RETURNS PHY INV COST CHANGE RPT ADMINISTRATION HELP TUTORIAL
Invoiced
PAGE LINES: 50
PAGE COUNT: 1 of 1
DOWNLOAD PRINT DELETE MANUAL RECEIVING
COPYRIGHT © 2000-2003 McKESSON CORPORATION
Internet

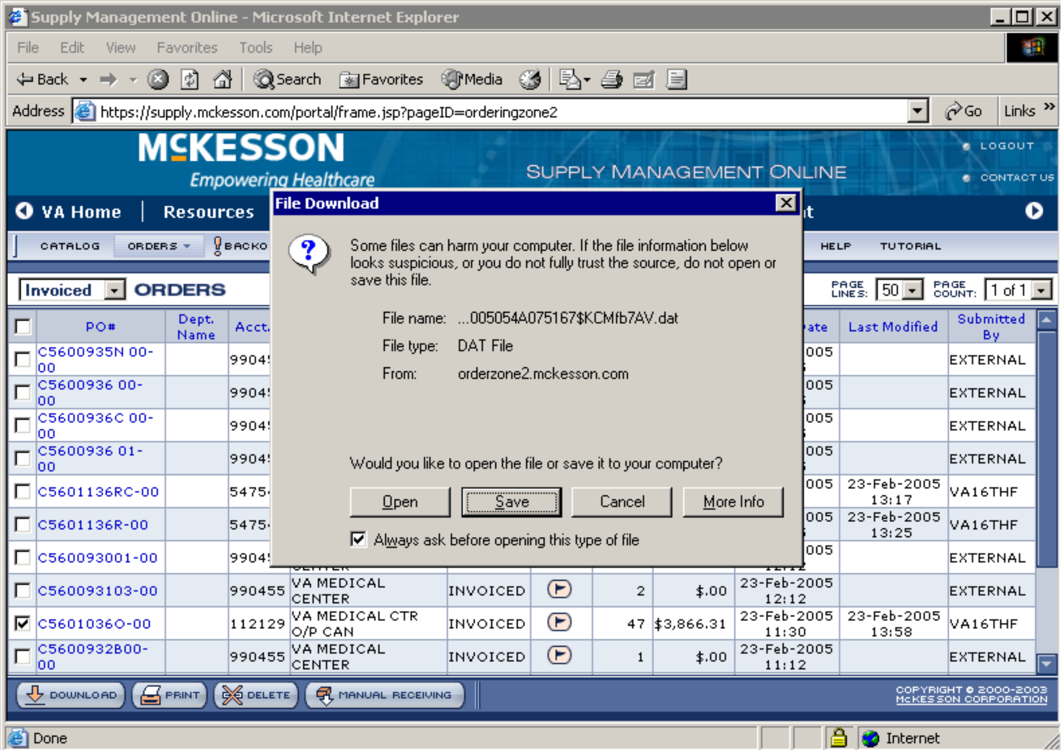
ORDERS

□	PO#	Dept. Name	Acct. #	Acct. Name	Status	Discrep?	Total Lines	Order Total	Create Date	Last Modified	Submitted By
□	C5600935N 00-00		990455	VA MEDICAL CENTER	INVOICED		4	$500.14	24-Feb-2005 01:45		EXTERNAL
□	C5600936 00-00		990455	VA MEDICAL CENTER	INVOICED		15	$573.23	24-Feb-2005 01:45		EXTERNAL
□	C5600936C 00-00		990455	VA MEDICAL CENTER	INVOICED		4	$361.92	24-Feb-2005 01:45		EXTERNAL
□	C5600936 01-00		990455	VA MEDICAL CENTER	INVOICED		4	$790.03	24-Feb-2005 01:45		EXTERNAL
□	C5601136RC-00		547548	VA OUTPATIENT CLINIC	INVOICED	⚑	3	$145.38	23-Feb-2005 12:51	23-Feb-2005 13:17	VA16THF
□	C5601136R-00		547548	VA OUTPATIENT CLINIC	INVOICED	⚑	13	$3,434.79	23-Feb-2005 12:45	23-Feb-2005 13:25	VA16THF
□	C560093001-00		990455	VA MEDICAL CENTER	INVOICED	⚑	1	$.00	23-Feb-2005 12:12		EXTERNAL
□	C560093103-00		990455	VA MEDICAL CENTER	INVOICED	⚑	2	$.00	23-Feb-2005 12:12		EXTERNAL
☑	C56010360-00		112129	VA MEDICAL CTR O/P CAN	INVOICED	⚑	47	$3,866.31	23-Feb-2005 11:30	23-Feb-2005 13:58	VA16THF
□	C5600932B00-00		990455	VA MEDICAL CENTER	INVOICED	⚑	1	$.00	23-Feb-2005 11:12		EXTERNAL

Figure 2-3: Screen displaying all orders

All invoices are displayed, and you must check which ones you will be downloading (Do *not* choose invoices that contain controlled substances. Simply select the boxes at the left of the screen for each Purchase Order number (PO#).

Select all boxes that you plan on downloading. This will put the boxes in the same DAT file. When finished checking, simply click **Download**.



Supply Management Online - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
McKESSON
Empowering Healthcare
SUPPLY MANAGEMENT ONLINE
LOGOUT
CONTACT US
VA Home | Resources
CATALOG ORDERS BACKO HELP TUTORIAL
DOWNLOAD PRINT DELETE MANUAL RECEIVING
COPYRIGHT © 2000-2003 McKESSON CORPORATION
Done
Internet

Address: https://supply.mckesson.com/portal/frame.jsp?pageID=orderingzone2

Invoiced ORDERS

PAGE LINES: 50 PAGE COUNT: 1 of 1

File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: ...005054A075167$KCMfb7AV.dat
File type: DAT File
From: orderzone2.mckesson.com

Would you like to open the file or save it to your computer?

Open | Save | Cancel | More Info

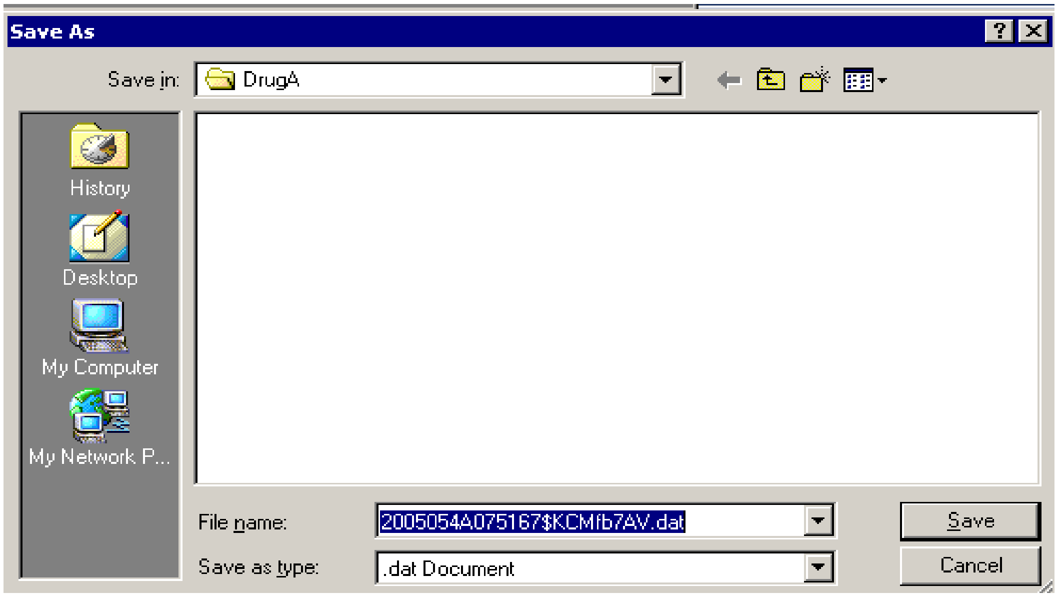
☑ Always ask before opening this type of file

☐	PO#	Dept. Name	Acct.						ate	Last Modified	Submitted By
☐	C5600935N 00-00		9904!						005		EXTERNAL
☐	C5600936 00-00		9904!						005		EXTERNAL
☐	C5600936C 00-00		9904!						005		EXTERNAL
☐	C5600936 01-00		9904!						005		EXTERNAL
☐	C5601136RC-00		5475						005	23-Feb-2005 13:17	VA16THF
☐	C5601136R-00		5475						005	23-Feb-2005 13:25	VA16THF
☐	C560093001-00		9904!						005		EXTERNAL
☐	C560093103-00		990455	VA MEDICAL CENTER	INVOICED	▶	2	$.00	23-Feb-2005 12:12		EXTERNAL
☑	C56010360-00		112129	VA MEDICAL CTR O/P CAN	INVOICED	▶	47	$3,866.31	23-Feb-2005 11:30	23-Feb-2005 13:58	VA16THF
☐	C5600932B00-00		990455	VA MEDICAL CENTER	INVOICED	▶	1	$.00	23-Feb-2005 11:12		EXTERNAL

Figure 2-4: **File Download** dialog box displays

A dialog box displays and prompts you to decide where to save the DAT file you are downloading from McKesson.

Click **Save**.



Save in: DrugA

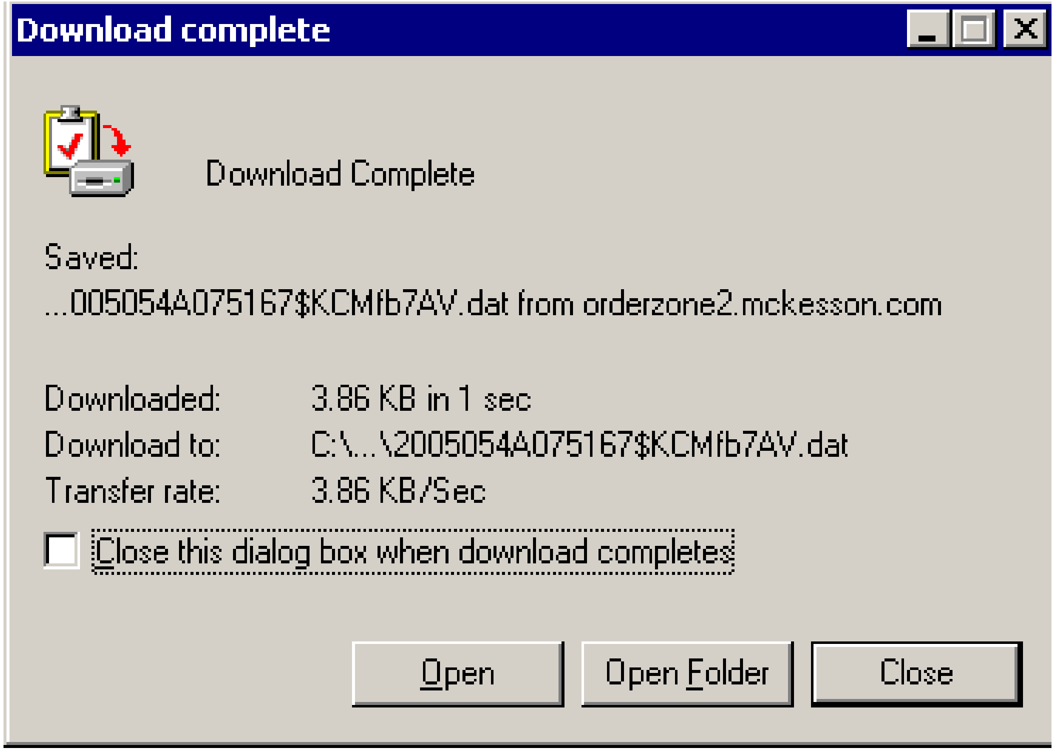
File name: 2005054A075167$KCMfb7AV.dat

Save as type: .dat Document

Figure 2-5: **Save As** window

This will either return you to the folder you previously set up, or you can simply add a new folder. You need to place this folder somewhere on the "C:\" drive. You can create a new folder by clicking on the new folder icon, and after choosing the folder to save the DAT file to, click **Save**.

Do *not* change the name of the file.



Download complete

Download Complete

Saved:
...005054A075167$KCMfb7AV.dat from orderzone2.mckesson.com

Downloaded: 3.86 KB in 1 sec
Download to: C:\...\2005054A075167$KCMfb7AV.dat
Transfer rate: 3.86 KB/Sec

□ Close this dialog box when download completes

Figure 2-6: **Download Complete** window

A window will display after the download is complete, and you are now finished downloading the invoice from McKesson to your hard drive. Click **Close**.

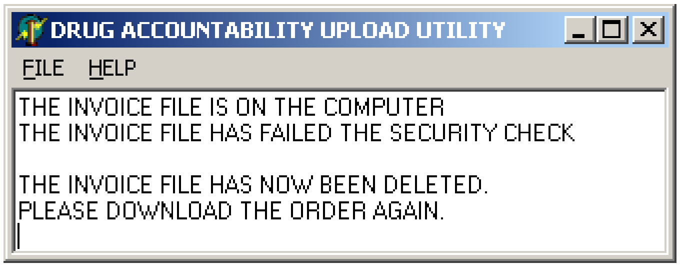
2.2 The GUI Invoice Upload Program

Included in the release of APSP 1010 is the PSA_MCKESSON_UPLOAD.exe file. This program will enable you to upload the McKesson invoice into RPMS.

Click on the PSA_MCKESSON_UPLOAD icon located on the Pharmacy PC's desktop.

Figure 2-7: Example: blowup of Shortcut icon

The program checks for the existence of the invoice file. Security checks are run to ensure the file has not been tampered with. If any of the security measures fail, the operation is aborted with the following message:



THE INVOICE FILE IS ON THE COMPUTER
THE INVOICE FILE HAS FAILED THE SECURITY CHECK

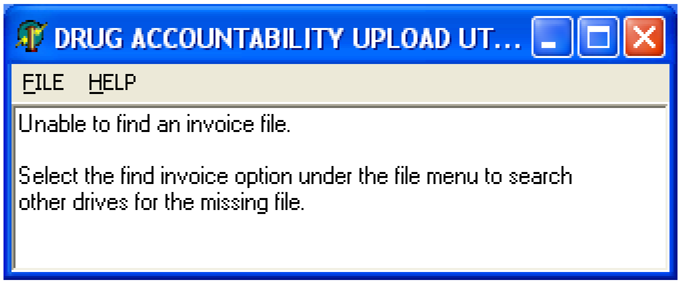
THE INVOICE FILE HAS NOW BEEN DELETED.
PLEASE DOWNLOAD THE ORDER AGAIN.

Figure 2-8: Example: Error screen for any failed security measures

If all checks are passed successfully, you will be prompted for the correct IP address.

2.3 Locate the Invoice File

When the upload utility is executed, it only searches for the file on the “C:\” drive. If the file cannot be located, the following message displays:

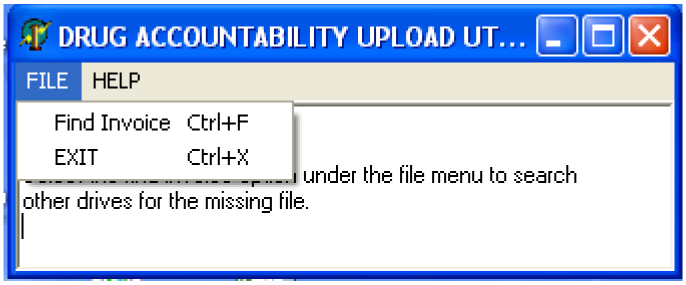


Unable to find an invoice file.

Select the find invoice option under the file menu to search other drives for the missing file.

Figure 2-9: Example: error message when invoice file not found

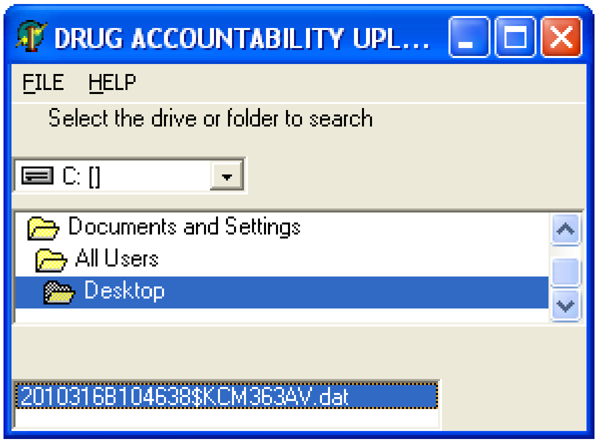
Select the **Find Invoice** option located under the **File** menu.



under the file menu to search
other drives for the missing file.

Figure 2-10: Example: finding the Invoice file

You can navigate to where you stored the file on your PC. When the appropriate folder is opened, the program will search for the **Invoice** file using predefined search parameters. If the file is found, the filename will display in the text box at the bottom of the screen. Double click on the file name.



Select the drive or folder to search

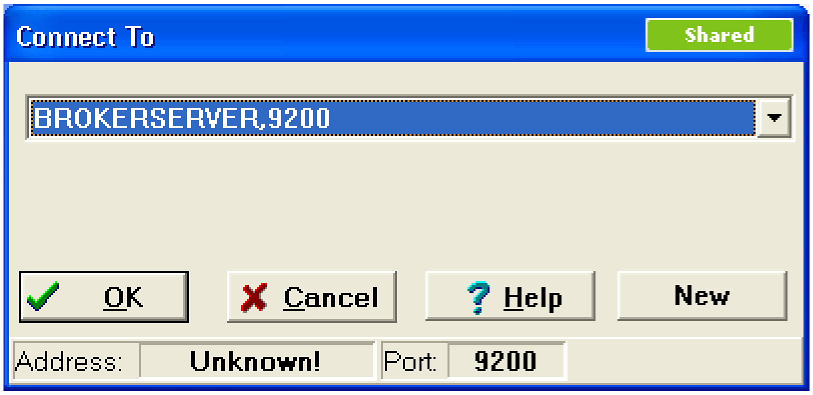
C: []

Documents and Settings
All Users
Desktop

20103168104638$KCM363AV.dat

Figure 2-11: Example: **Invoice** file found

If all checks are passed successfully, you will be prompted for the correct RPMS server IP address and port number. Local Information Technology (IT) support should be able to provide this information.



BROKERSERVER,9200

Address: Unknown! Port: 9200

Figure 2-12: Example: connecting to the IP address screen

Enter the IP address of the server and the port number (this is the port number for the TCP listener that was set in Section 2.1 of the GUI Invoice Upload Program Installation and Configuration Guide). The site should only have to do this for the initial setup. Once entered, it will be available from the dropdown menu on the **Connect To** screen.

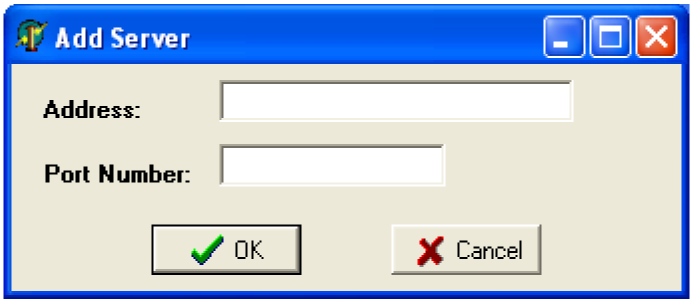
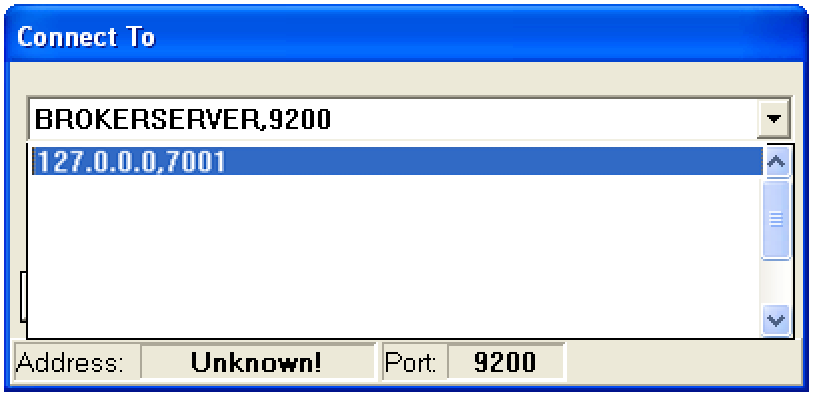


Figure 2-13: Example: **Add Server** window

Once you click **OK,** use the dropdown menu option to find your server.



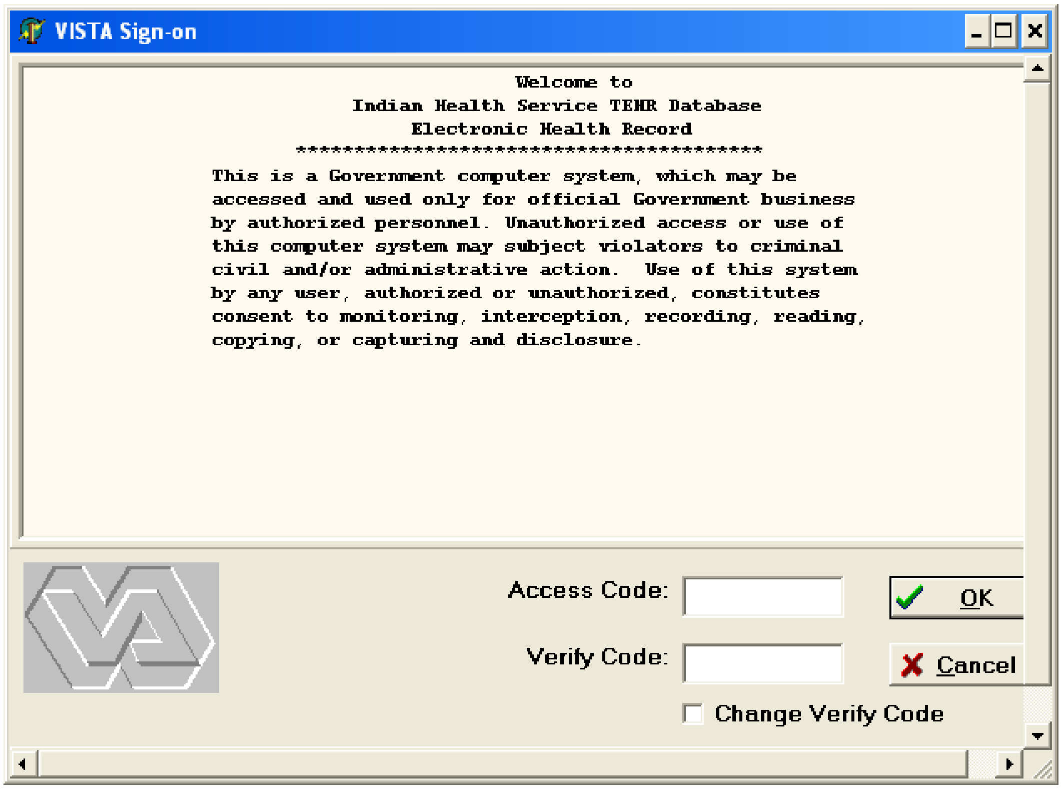
BROKERSERVER,9200

127.0.0.0,7001

Address: Unknown! Port: 9200

Figure 2-14: Example: **Connect To** window

You are then prompted to enter a proper access and verify code combination.



Welcome to
Indian Health Service TEHR Database
Electronic Health Record
****
This is a Government computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal civil and/or administrative action. Use of this system by any user, authorized or unauthorized, constitutes consent to monitoring, interception, recording, reading, copying, or capturing and disclosure.

Access Code:

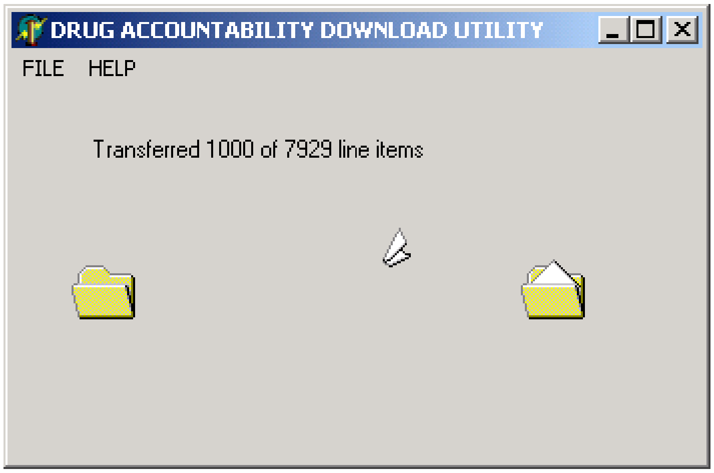
Verify Code:

□ Change Verify Code

Figure 2-15: Example: access and verify code screen

After successful logon, the program will upload the invoice files into RPMS. A running tally of the process is displayed.

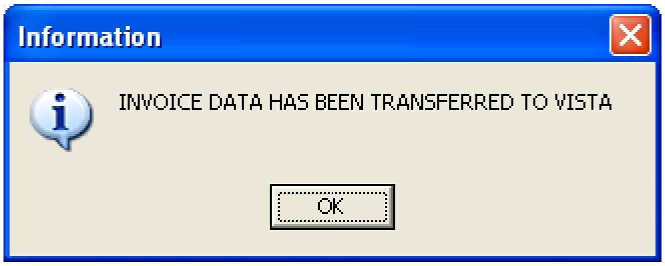
> **Note**: Due to the speed of the transfer, the 'file to file' progress display may not show at all. The program can upload a 360kb file in less than 30 seconds.



Transferred 1000 of 7929 line items

Figure 2-16: Example: uploading of invoices screen

After the data has been uploaded, the program will display this message:



INVOICE DATA HAS BEEN TRANSFERRED TO VISTA

Figure 2-17: Example: successful upload screen

The utility will automatically shut down at this point. After you have uploaded the invoice(s), you may proceed to process the invoice in the RPMS Drug Accountability package.

Appendix A: RPMS 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.

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
E-mail:	support@ihs.gov