Individuals Authorized Access to the CMS Computer Services

(IACS)

IACS User Guide

Document Version 2.0

November 2013

Document No.: 132-IACS_User_Guide-D
Contract No.: HHSM-500-2007-00024I

Prepared for:
Centers for Medicare & Medicaid Services (CMS)
OIS/ISDDG
7500 Security Boulevard, N3-00-01
Baltimore, Maryland 21244-1850

Prepared by:
Quality Software Services, Inc. (QSSI)
10025 Governor Warfield Parkway
Suite 401
Columbia, Maryland 21044

REVISION HISTORY

Date	Version	Reason for Change	Author
06/23/2012	1.0	Initial Release 2012.01	QSSI
09/21/2012	1.1	Draft – Release 2012.02 changes	QSSI
11/10/2012	1.2	Release 2012.02 changes Section 2.2 Internet browser requirement change New Appendix A: IACS Application Role Approval Matrix	QSSI
04/22/2013	2.0	Draft – Release 2013.01	QSSI
04/24/2013	3.0	Final – Release 2013.01 *(Archived)*	QSSI
09/10/2013	0.1	Draft – Release 2013.02 *(Version numbering restarted)* Release 2013.02 change: Frequently Asked Question's (FAQ's) answer for terminated contracts has been updated, based on Change Request (CR) – 502.	QSSI
09/11/2013	0.2	Draft – Release 2013.02	QSSI
09/11/2013	0.3	Draft – Release 2013.02	QSSI
09/30/2013	0.4	Draft – Release 2013.02	QSSI
10/18/2013	0.5	Draft – Release 2013.02	QSSI
10/18/2013	0.6	Draft – Release 2013.02	QSSI
10/18/2013	1.0	Version for CMS review	QSSI
10/28/2013	1.1	CMS comments incorporated in this version.	QSSI
10/29/2013	2.0	Final – Release 2013.02	QSSI

CONTENTS

FIGURES

TABLES

1.0 Introduction

Individuals Authorized Access to the CMS Computer Services (IACS) is an identity management system that provides the means for users needing access to CMS applications to:

- Apply for and receive login credentials in the form of a User Identifier (User ID) and password.
- Apply for and receive approval to access the required system(s).

2.0 Overview

The sensitivity of CMS data, and the improved ability to access that data, combine to create a substantial risk to CMS and Beneficiaries. Legislation, such as the Health Insurance Portability and Accountability Act (HIPAA), various federal standards published by the National Institute of Standards and Technology (NIST), and certain CMS policies, has been established to control risk. IACS is the application CMS uses to:

- Implement the security requirements of federal legislation, federal standards, and CMS policies.
- Provide secure, high quality services to protect CMS systems and data.
- Register users and control the distribution of User IDs and passwords used to access CMS web-based applications.

The IACS User Guide provides procedural information and representative screens for the End-Users, Approvers, Authorizers, and Help Desk roles. This document will cover the following topics:

- Registering as a New User of one of the CMS applications supported by IACS.
- Modifying user registration information.
- Certifying annually the need for continued access to CMS systems.
- Processing (approving, rejecting, or deferring) access requests for new user registration, certifications, or profile modifications for IACS users.
- Using IACS to manage requests and users under an individual Approver’s authority.
- Performing help desk functions to view users, disable user accounts, unlock user accounts, and reset passwords.

Procedural information that is particular to specific applications is noted for reference. The IACS Application is designed to be user-friendly by providing on-screen help and error messages to assist the user in completing procedures not illustrated in this user guide.

The IACS User Guide is available on the CMS IACS website: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/IACS/Downloads/User-Guide.pdf to provide additional information and instruction for IACS users.

3.0 What is IACS?

The Centers for Medicare & Medicaid Services (CMS) has developed the IACS application to control issuance of electronic identities and access to CMS web-based applications. Through IACS, an individual will be able to register for any of the CMS applications listed in Section 5.0.

Registration requests are reviewed and approved using a hierarchical system of approvals referred to as the Chain of Trust. Typically, the requests are approved in the following manner:

- End User requests are approved by Approvers (for some applications, the Helpdesk functions as the Approver).
- Approvers are approved by Authorizers (for some applications, the Helpdesk functions as the Authorizer).
- Helpdesks that do not have approval authority are approved by Authorizers.
- Authorizers are approved by the Business Owner or their designee. Business Owners typically do not have an IACS User ID. Thus, Authorizers are referred to as Top of the Chain Users, since they are the last users in the chain who must have an IACS User ID.

Note: Refer to Appendix A for a listing of the roles and approval hierarchy for CMS applications integrated with IACS.

Once approved, IACS will create a User ID and will send an E-mail to the user with an initial password pattern. To complete the registration process, the user will log in to IACS with the User ID and the initial password pattern. The system will prompt the user to change the password to a new password. At this point, the user will be able to access the approved CMS application(s). When the user logs in to the approved CMS application with the IACS User ID, the user will be able to perform the functions associated with the approved role.

A user authorized to access other applications supported by IACS will use the same User ID to log in to those applications. IACS also manages the life cycle of User IDs and passwords. IACS ensures: passwords expire every 60 days; accounts are disabled after 60 days of inactivity; and, users annually certify their continued need to access CMS applications.

Once registered, the user can use IACS to:

- "Forgot Your Password?" self-service recovery
- "Forgot Your User ID?" self-service recovery
- Change password, at least every 60 days
- Re-enable an account disabled following 60 days of inactivity
- Add new application or role
- Remove role
- Modify user and professional contact information
- Complete the mandatory Annual Certification

4.0 User Guide Conventions

This document provides screen prints and corresponding narratives to describe the typical procedures for account registration and account management. When functions are similar, the more common functions will be illustrated with notes indicating differences, such as specific information users must provide for different applications. When appropriate, these notes will be illustrated with screen shots.

Every effort has been made to keep the screen shots and formatting conventions used in this document up to date. There may be, however, minor differences between on-screen text and what is shown in the figures in this user guide. These differences should not affect the user's ability to request desired access or perform desired activities.

Note: The term 'user' is used throughout this document to refer to a person who requires and/or has acquired access to the IACS application.

Note: The term 'Helpdesk' is used throughout this document to refer to users with the help desk role.

The following formatting conventions have been used in this user guide or are used on the IACS screens:

- Screen and feature names are shown in **bold.**
- References to partial screens displayed or buttons to be acted upon are shown in ***bold italics***.
- References to hyperlinks are shown in blue, underlined text.
- Field names are shown in *plain italics*.
- Action statements will begin with the word **Action:**
- Explanatory notes will be indicated with the word **Note:**
- IACS screens display required input fields with an asterisk (*) to the right of the field. These fields must be completed.
- IACS screens provide online help. The iHelp icon will be displayed next to a field, as a small blue letter i inside a white box.

Examples of specific screens are used in this user guide to illustrate what users would see during common registration and account modification procedures. The names and/or data on these screens are meant to be representative and do not reflect actual IACS users and/or accounts.

4.1 Browser Requirements

To optimize access to the IACS screens, the user needs to ensure that the following criteria are met:

1. **Screen Resolution:** CMS screens are designed to be best viewed at a screen resolution of 800 x 600.

2. **Internet Browser:** Use Internet Explorer, version 8.0 or higher.
3. **Plug-Ins:** Verify that the latest version of JAVA and ActiveX are installed on the PC.
4. **Pop-up Blockers:** Disable pop-up blockers.

4.2 Cautions and Warnings

Users of United States Government Computer Systems must be aware of warnings regarding unauthorized access to those systems, computer usage and monitoring, and local system requirements. The user must read and agree to such notices before accessing the IACS online application.

5.0 IACS Supported CMS Applications

This IACS User Guide provides the procedures to obtain an IACS User ID, manage an IACS account, review and approve requests, and manage users for the following CMS applications:

- Bundled Payments EFT
- Center for Strategic Planning - Health System Tracking Project (CSP - HSTP)
- Center for Strategic Planning - Medicaid and Children's Health Insurance Program (CHIP) State Information Sharing System (CSP - MCSIS)
- CMS Administration – Physician Value (PV)
- Comprehensive Primary Care (CPC) Initiative
- Coordination of Benefits (COB)
- Customer Service Representatives (1-800-Medicare CSR)
- Durable Medical Equipment, Prosthetics, Orthotics & Supplies (DMEPOS) Bidding System (DBidS)
- Electronic Correspondence Referral System (ECRS) Web
- Electronic Submission of Medical Documentation (esMD)
- GENTRAN
- HIPAA Eligibility Transaction System User Interface (HETS UI)
- HIPAA Eligibility Transaction System Provider Graphical User Interface (HPG)
- Internet Server (ISV)
- Medicaid and CHIP Program System (MACPro)
- Medicaid Drug Rebate (MDR) State Exchange
- Medicare Advantage/Medicare Advantage-Prescription Drug/Prescription Drug Plan/Cost Contracts (MA/MA-PD/PDP/CC)
- Medicare Exclusion Database (MED)
- MyCGS
- Novitasphere - Internet Provider Portal for Novitas Solutions, Inc.

- Physician Quality Reporting System and E-Prescribing Incentive Programs (PQRS/eRx)
- Provider Statistical and Reimbursement (PS&R)
- PV/PQRS Registration System
- System Tracking for Audit and Reimbursement (STAR)
- The SPOT – First Coast Service Options' Internet portal (FCSO)
- VMS Client Letter

6.0 New User Registration

The following section provides instructions for the most common registration steps. The MA/MA-PD/PDP/CC Application and the MA Submitter role will be used for this example. Registration steps for the other applications are not significantly different from those provided in this section. Noteworthy differences for other roles will be identified in Section 6.3.

Prior to registering in IACS, the user should have received information on registration details from his organization or CMS point of contact. If the user has not received registration information for IACS, the user should contact his organization or CMS contact.

6.1 Register for a CMS Application

To register in IACS, the user must first access the CMS website.

Action: Navigate to https://applications.cms.hhs.gov.

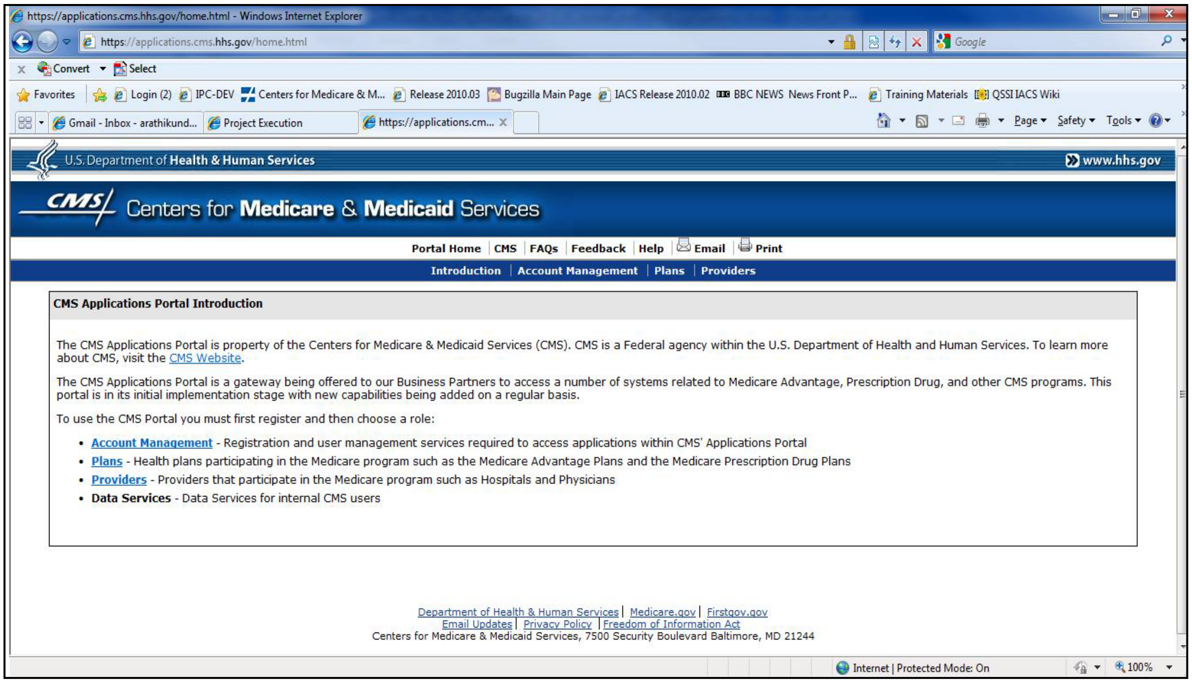
> **Note**: Alternatively, users may navigate to http://www.cms.gov/iacs and select the link for New User Registration.

The CMS Applications Portal WARNING/REMINDER screen will display.

The user will have the option to enter the **CMS Applications Portal** or return to the CMS home page by selecting the ***Leave*** button.

Action: Read the important information on this screen and indicate your agreement by selecting the ***Enter CMS Applications Portal*** button.

The **CMS Applications Portal Introduction** screen will display, as illustrated in Figure 1.


https://applications.cms.hhs.gov/home.html - Windows Internet Explorer
https://applications.cms.hhs.gov/home.html
Google
Convert
Select
Favorites
Login (2)
IPC-DEV
Centers for Medicare & M...
Release 2010.03
Bugzilla Main Page
IACS Release 2010.02
BBC NEWS News Front P...
Training Materials
QSSI IACS Wiki
Gmail - Inbox - arathikund...
Project Execution
https://applications.cm...
Page
Safety
Tools
U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
Portal Home | CMS | FAQs | Feedback | Help | Email | Print
Introduction | Account Management | Plans | Providers
Internet | Protected Mode: On
100%

CMS Applications Portal Introduction

The CMS Applications Portal is property of the Centers for Medicare & Medicaid Services (CMS). CMS is a Federal agency within the U.S. Department of Health and Human Services. To learn more about CMS, visit the CMS Website.

The CMS Applications Portal is a gateway being offered to our Business Partners to access a number of systems related to Medicare Advantage, Prescription Drug, and other CMS programs. This portal is in its initial implementation stage with new capabilities being added on a regular basis.

To use the CMS Portal you must first register and then choose a role:

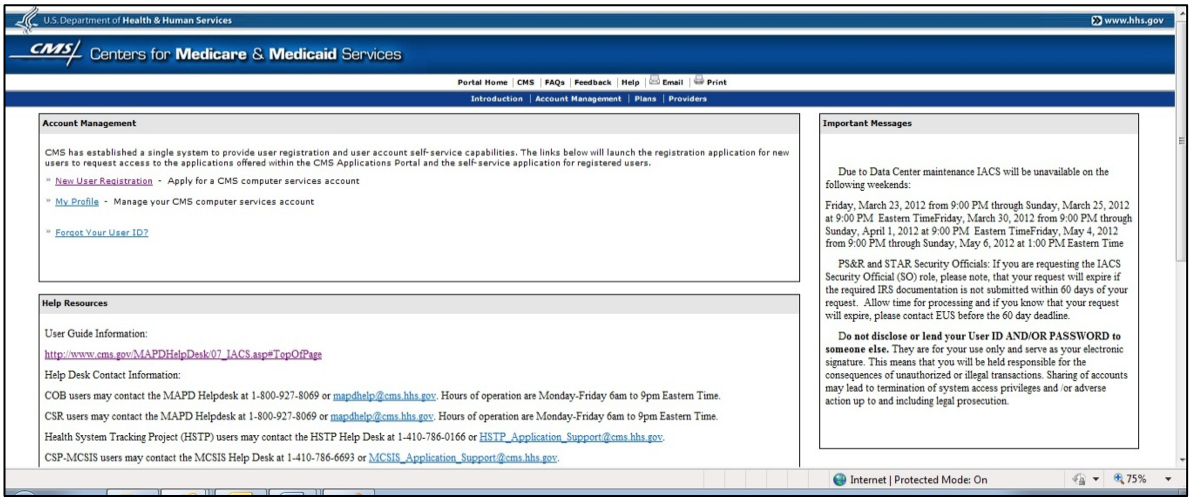
- **Account Management** - Registration and user management services required to access applications within CMS' Applications Portal
- **Plans** - Health plans participating in the Medicare program such as the Medicare Advantage Plans and the Medicare Prescription Drug Plans
- **Providers** - Providers that participate in the Medicare program such as Hospitals and Physicians
- **Data Services** - Data Services for internal CMS users

Department of Health & Human Services | Medicare.gov | Firstgov.gov
Email Updates | Privacy Policy | Freedom of Information Act
Centers for Medicare & Medicaid Services, 7500 Security Boulevard Baltimore, MD 21244

Figure 1: CMS Applications Portal Introduction Screen

Action: Select the Account Management hyperlink in the center of the screen or from the menu bar toward the top of the screen.

The Account Management screen will display, as illustrated in Figure 2. The hyperlinks within the Account Management section are used to access IACS registration or to manage a user's IACS account. The **Help Resources** section located below the Account Management section provides a link to this user guide, the application Help Desk contact information and E-mail hyperlinks.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
Portal Home | CMS | FAQs | Feedback | Help | Email | Print
Introduction | Account Management | Plans | Providers
Internet | Protected Mode: On
75%

Account Management

CMS has established a single system to provide user registration and user account self-service capabilities. The links below will launch the registration application for new users to request access to the applications offered within the CMS Applications Portal and the self-service application for registered users.

» New User Registration - Apply for a CMS computer services account

» My Profile - Manage your CMS computer services account

» Forgot Your User ID?

Help Resources

User Guide Information:

http://www.cms.gov/MAPDHelpDesk/07_IACS.asp#TopOfPage

Help Desk Contact Information:

COB users may contact the MAPD Helpdesk at 1-800-927-8069 or mapdhelp@cms.hhs.gov. Hours of operation are Monday-Friday 6am to 9pm Eastern Time.

CSR users may contact the MAPD Helpdesk at 1-800-927-8069 or mapdhelp@cms.hhs.gov. Hours of operation are Monday-Friday 6am to 9pm Eastern Time.

Health System Tracking Project (HSTP) users may contact the HSTP Help Desk at 1-410-786-0166 or HSTP_Application_Support@cms.hhs.gov.

CSP-MCSIS users may contact the MCSIS Help Desk at 1-410-786-6693 or MCSIS_Application_Support@cms.hhs.gov.

Important Messages

Due to Data Center maintenance IACS will be unavailable on the following weekends:

Friday, March 23, 2012 from 9:00 PM through Sunday, March 25, 2012 at 9:00 PM Eastern TimeFriday, March 30, 2012 from 9:00 PM through Sunday, April 1, 2012 at 9:00 PM Eastern TimeFriday, May 4, 2012 from 9:00 PM through Sunday, May 6, 2012 at 1:00 PM Eastern Time

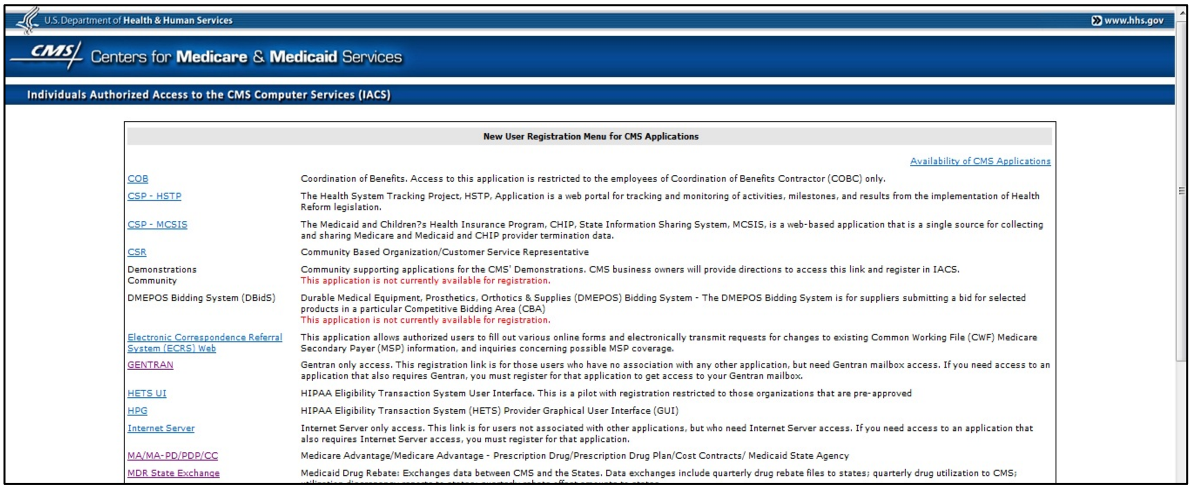
PS&R and STAR Security Officials: If you are requesting the IACS Security Official (SO) role, please note, that your request will expire if the required IRS documentation is not submitted within 60 days of your request. Allow time for processing and if you know that your request will expire, please contact EUS before the 60 day deadline.

Do not disclose or lend your User ID AND/OR PASSWORD to someone else. They are for your use only and serve as your electronic signature. This means that you will be held responsible for the consequences of unauthorized or illegal transactions. Sharing of accounts may lead to termination of system access privileges and /or adverse action up to and including legal prosecution.

Figure 2: Account Management Screen

Action: Select the New User Registration hyperlink.

The **New User Registration Menu** screen will display, as illustrated in Figure 3.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
Individuals Authorized Access to the CMS Computer Services (IACS)

New User Registration Menu for CMS Applications

Availability of CMS Applications

COB	Coordination of Benefits. Access to this application is restricted to the employees of Coordination of Benefits Contractor (COBC) only.
CSP - HSTP	The Health System Tracking Project, HSTP, Application is a web portal for tracking and monitoring of activities, milestones, and results from the implementation of Health Reform legislation.
CSP - MCSIS	The Medicaid and Children?s Health Insurance Program, CHIP, State Information Sharing System, MCSIS, is a web-based application that is a single source for collecting and sharing Medicare and Medicaid and CHIP provider termination data.
CSR	Community Based Organization/Customer Service Representative
Demonstrations Community	Community supporting applications for the CMS' Demonstrations. CMS business owners will provide directions to access this link and register in IACS. This application is not currently available for registration.
DMEPOS Bidding System (DBidS)	Durable Medical Equipment, Prosthetics, Orthotics & Supplies (DMEPOS) Bidding System - The DMEPOS Bidding System is for suppliers submitting a bid for selected products in a particular Competitive Bidding Area (CBA) This application is not currently available for registration.
Electronic Correspondence Referral System (ECRS) Web	This application allows authorized users to fill out various online forms and electronically transmit requests for changes to existing Common Working File (CWF) Medicare Secondary Payer (MSP) information, and inquiries concerning possible MSP coverage.
GENTRAN	Gentran only access. This registration link is for those users who have no association with any other application, but need Gentran mailbox access. If you need access to an application that also requires Gentran, you must register for that application to get access to your Gentran mailbox.
HETS UI	HIPAA Eligibility Transaction System User Interface. This is a pilot with registration restricted to those organizations that are pre-approved
HPG	HIPAA Eligibility Transaction System (HETS) Provider Graphical User Interface (GUI)
Internet Server	Internet Server only access. This link is for users not associated with other applications, but who need Internet Server access. If you need access to an application that also requires Internet Server access, you must register for that application.
MA/MA-PD/PDP/CC	Medicare Advantage/Medicare Advantage - Prescription Drug/Prescription Drug Plan/Cost Contracts/ Medicaid State Agency
MDR State Exchange	Medicaid Drug Rebate: Exchanges data between CMS and the States. Data exchanges include quarterly drug rebate files to states; quarterly drug utilization to CMS;

Figure 3: New User Registration Menu Screen

Note: When an application is not available for registration, the link will be “grayed out” and a message will be displayed in red stating “***The Application is currently not available for registration***.”

Action: From the **New User Registration Menu** screen, select the CMS application hyperlink for which you want to register.

The CMS Computer Systems Security Requirements **Terms and Conditions** screen will display. This screen contains the *Privacy Act Statement* and the *Rules of Behavior,* which presents the terms and conditions for accessing CMS computer systems.

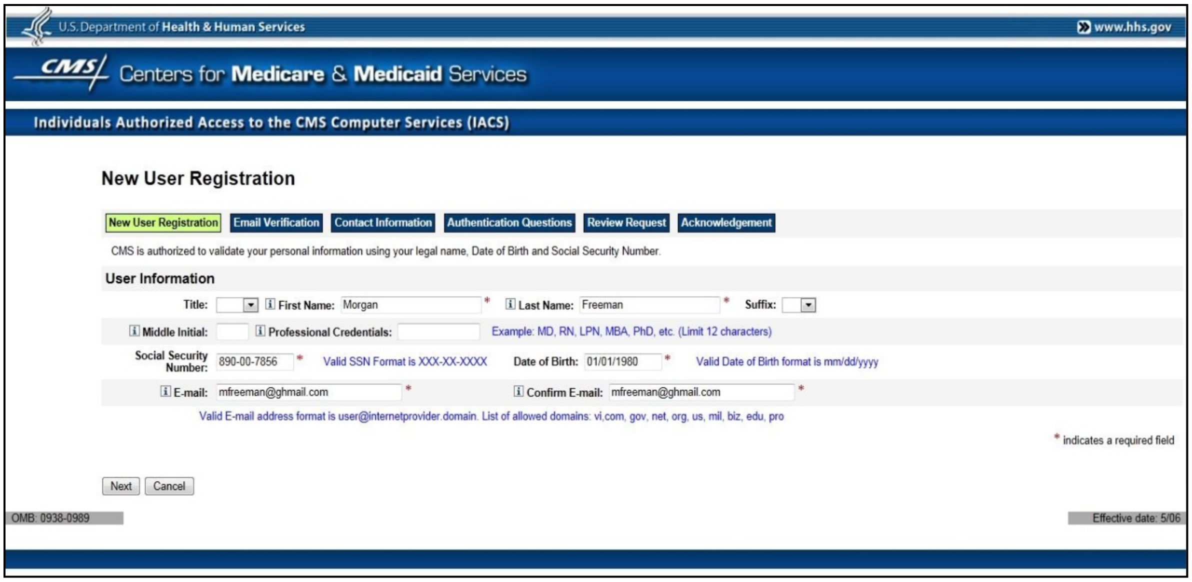
Action: Accept the terms and conditions to be authorized to access CMS systems and applications, and select the ***I Accept*** button.

The **New User Registration** screen will display, as illustrated in Figure 4. The registration process guides you through the steps. Select the ***Next*** button to proceed to the next step.

Note: If the ***Cancel*** button is selected during the registration process, the request will be cancelled and all information that was entered will be lost. A warning message will be displayed for the user. The user selects the ***OK*** button to cancel the request or ***Cancel*** to continue with the registration process. If the user selects ***OK,*** then select ***OK*** again to close the browser.

In the ***User Information*** area of the screen, the user will enter information needed by the system to identify the user and allow the system to communicate with the user through E-mail. These common fields must be filled in by all CMS Application requesters regardless of the type of access requested.

Required fields are indicated by an asterisk (*) to the right of the field. The iHelp icon i inside a white box button next to the field can be selected to obtain additional information about the field.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
Individuals Authorized Access to the CMS Computer Services (IACS)
New User Registration
Email Verification
Contact Information
Authentication Questions
Review Request
Acknowledgement
Next
Cancel

New User Registration

CMS is authorized to validate your personal information using your legal name, Date of Birth and Social Security Number.

User Information

Title: [▾] First Name: Morgan * Last Name: Freeman * Suffix: [▾]

Middle Initial: [ ] Professional Credentials: [ ] Example: MD, RN, LPN, MBA, PhD, etc. (Limit 12 characters)

Social Security Number: 890-00-7856 * Valid SSN Format is XXX-XX-XXXX Date of Birth: 01/01/1980 * Valid Date of Birth format is mm/dd/yyyy

E-mail: mfreeman@ghmail.com * Confirm E-mail: mfreeman@ghmail.com *

Valid E-mail address format is user@internetprovider.domain. List of allowed domains: vi,com, gov, net, org, us, mil, biz, edu, pro

* indicates a required field

OMB: 0938-0989

Effective date: 5/06

Figure 4: New User Registration Screen

Action: Complete the required fields in the ***User Information*** area of the screen. The optional fields may be completed as well.

- The First and Last Name must be those on file with the Social Security Administration (SSA).
- A unique, work related E-mail address where the user may be contacted is required.
- The E-mail address should be entered a second time for verification. Values should not be cut and pasted from one field to the other.

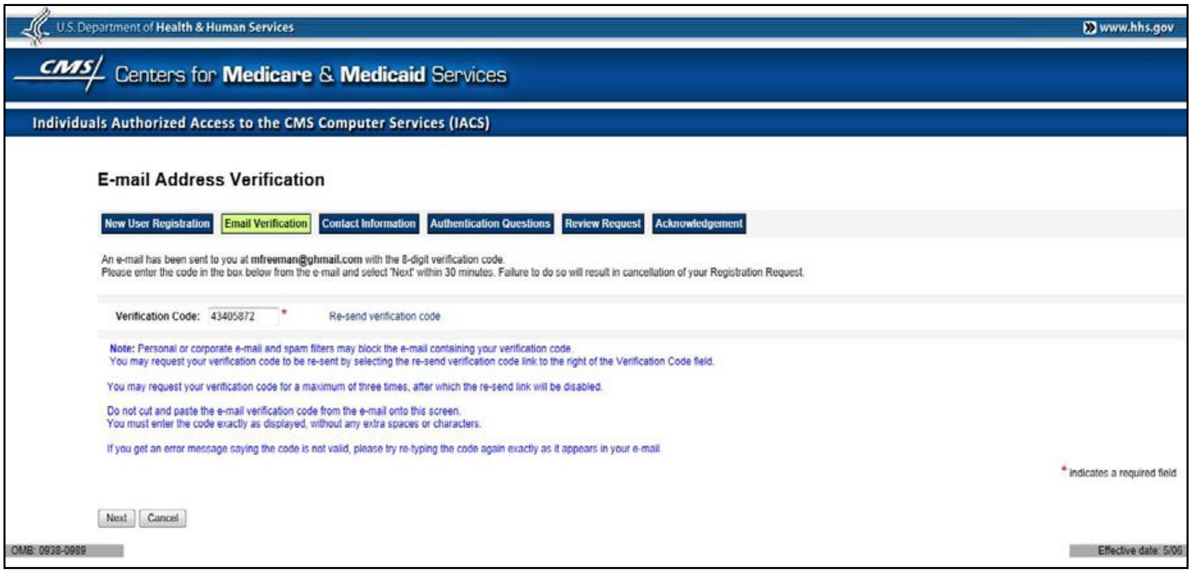
Note: The information must be entered in the format specified.

Action: Select the ***Next*** button when all the required fields have been completed.

When the ***Next*** button is selected, the system validates the entered data.

- The SSN is validated to verify that it does not already exist for another IACS account.
- The E-mail address is validated to verify that it does not already exist for another IACS account.

If the user information is successfully validated, the **E-mail Address Verification** screen will display, as illustrated in Figure 5.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
Individuals Authorized Access to the CMS Computer Services (IACS)

E-mail Address Verification

New User Registration
Email Verification
Contact Information
Authentication Questions
Review Request
Acknowledgement

An e-mail has been sent to you at **mfreeman@ghmail.com** with the 8-digit verification code.
Please enter the code in the box below from the e-mail and select 'Next' within 30 minutes. Failure to do so will result in cancellation of your Registration Request.

Verification Code: 43405872 * Re-send verification code

Note: Personal or corporate e-mail and spam filters may block the e-mail containing your verification code.
You may request your verification code to be re-sent by selecting the re-send verification code link to the right of the Verification Code field.

You may request your verification code for a maximum of three times, after which the re-send link will be disabled.

Do not cut and paste the e-mail verification code from the e-mail onto this screen.
You must enter the code exactly as displayed, without any extra spaces or characters.

If you get an error message saying the code is not valid, please try re-typing the code again exactly as it appears in your e-mail.

* indicates a required field

OMB: 0938-0989

Effective date: 5/06

Figure 5: E-mail Address Verification

The user will be sent an E-mail to the E-mail address the user has entered that confirms IACS has received the user's request. The E-mail subject line will be: ***IACS: E-mail Address Verification****. The* E-mail will contain a Verification Code that has to be entered on the **E-mail Address Verification** screen.

Note: Do not close the **E-mail Address Verification** screen. If the user closes the **E-mail Address Verification** screen, the request will be cancelled and all information entered will be lost.

The user will have 30 minutes to enter the Verification Code on the **E-mail Address Verification** screen. The Verification Code will expire after 30 minutes, if the user has not entered the code. The user's request will be cancelled and all information that has been entered will be lost.

Action: Proceed to the user's E-mail Inbox and open the E-mail with the subject line: **IACS: E-mail Address Verification**. Record the Verification Code. It will be used in the next action.

If the user does not receive the verification E-mail, he may select the Re-send verification code hyperlink to the right of the *Verification Code* field on the **E-mail Address Verification** screen. The user may ask to have the Verification Code re-sent up to three times. The user may also contact the Help Desk if he needs assistance or does not receive the Address Verification E-mail. If the user realizes that he may have entered an incorrect E-mail address, then he must cancel the registration process and start over.

Once the user has the Verification Code, the user must return to the **E-mail Address Verification** screen.

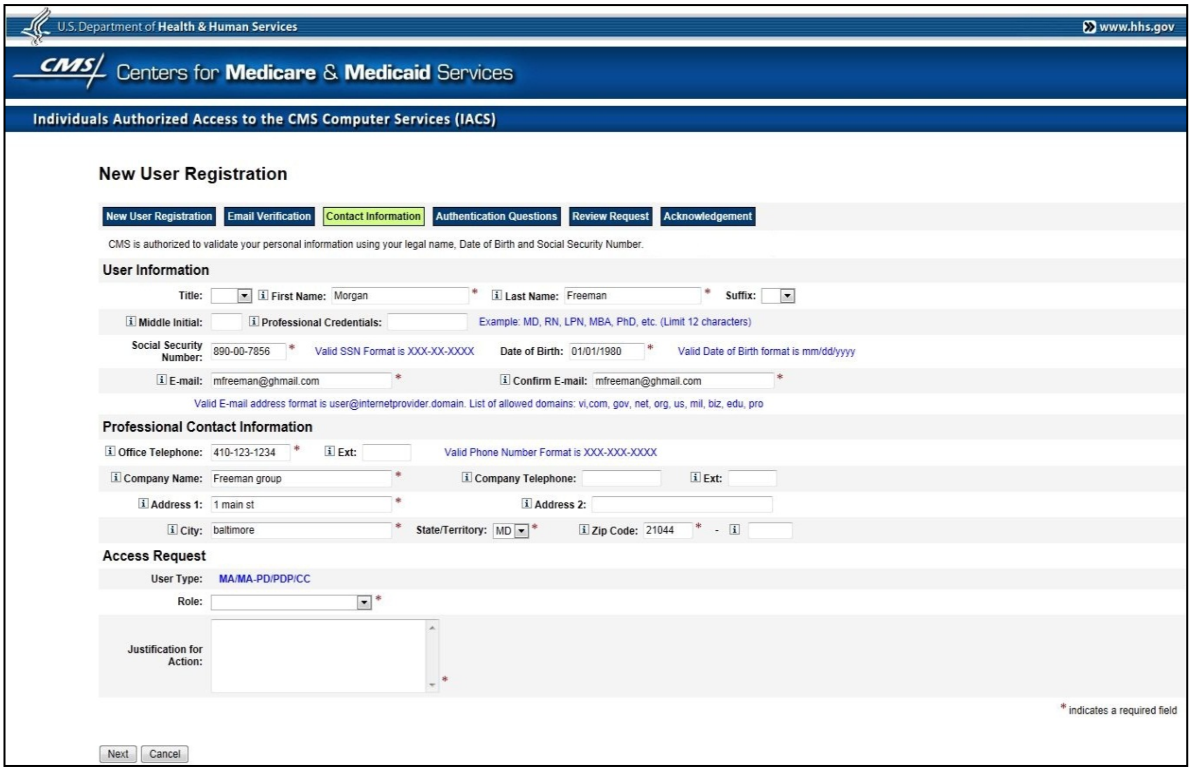
Action: Enter the Verification Code in the *Verification Code* field on the **E-mail Address Verification** screen, as illustrated in Figure 5.

Note: The code must be entered exactly as it is displayed in the E-mail message without any extra spaces or characters.

Action: Select the ***Next*** button.

Note: After three unsuccessful attempts to enter the Verification Code, the IACS registration request will be cancelled and all information that has been entered will be lost.

When the user enters the correct verification code and selects the ***Next*** button on the **E-mail Address Verification** screen, the screen will refresh and the **New User Registration** screen will display, as illustrated in Figure 6.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
Individuals Authorized Access to the CMS Computer Services (IACS)
New User Registration
Email Verification
Contact Information
Authentication Questions
Review Request
Acknowledgement
Next
Cancel

New User Registration

CMS is authorized to validate your personal information using your legal name, Date of Birth and Social Security Number.

User Information

Title: ▾ First Name: Morgan * Last Name: Freeman * Suffix: ▾

Middle Initial: Professional Credentials: Example: MD, RN, LPN, MBA, PhD, etc. (Limit 12 characters)

Social Security Number: 890-00-7856 * Valid SSN Format is XXX-XX-XXXX Date of Birth: 01/01/1980 * Valid Date of Birth format is mm/dd/yyyy

E-mail: mfreeman@ghmail.com * Confirm E-mail: mfreeman@ghmail.com *

Valid E-mail address format is user@internetprovider.domain. List of allowed domains: vi,com, gov, net, org, us, mil, biz, edu, pro

Professional Contact Information

Office Telephone: 410-123-1234 * Ext: Valid Phone Number Format is XXX-XXX-XXXX

Company Name: Freeman group * Company Telephone: Ext:

Address 1: 1 main st * Address 2:

City: baltimore * State/Territory: MD ▾ * Zip Code: 21044 * -

Access Request

User Type: MA/MA-PD/PDP/CC

Role: ▾ *

Justification for Action: *

* indicates a required field

Figure 6: New User Registration Screen: Contact Information

This screen has additional sections that need to be completed. The top area of the **New User Registration** screen labeled ***User Information***, as illustrated in Figure 6, will be pre-populated with the user information completed prior to the E-mail address verification.

The center of the screen contains an area labeled ***Professional Contact Information***.

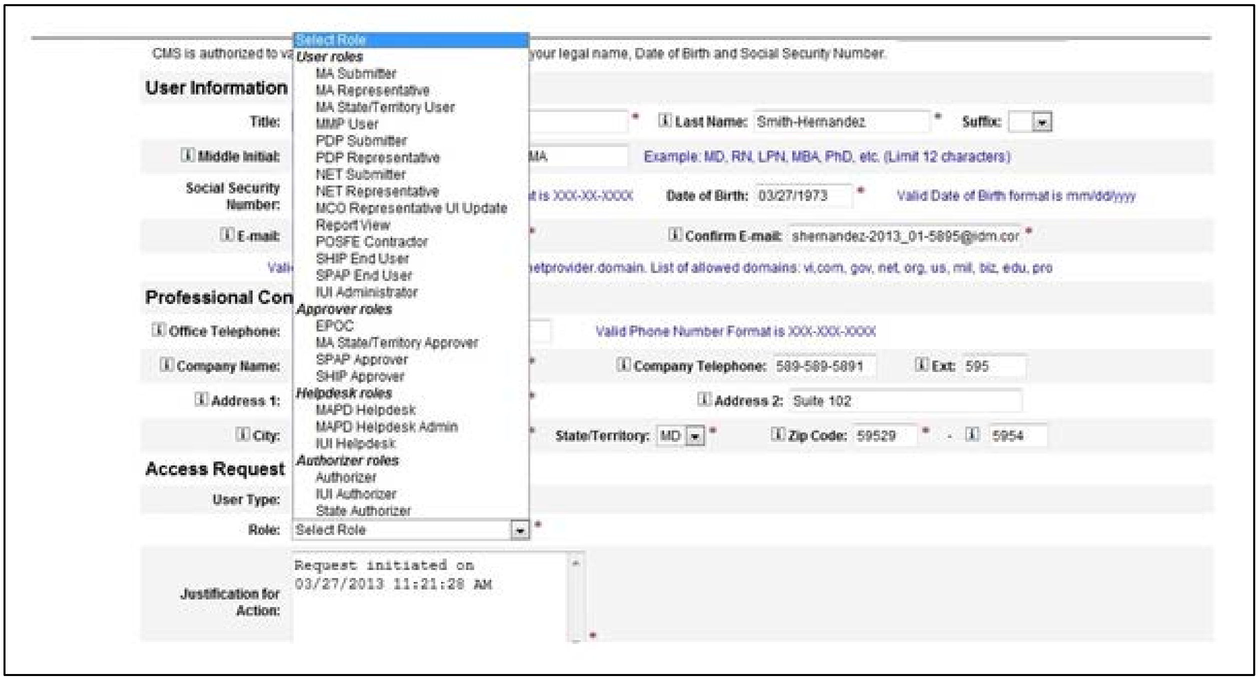
Action: Enter the professional contact information in the fields provided in the ***Professional Contact Information*** area of the **New User Registration** screen.

All required fields must be completed. Required fields are indicated by an asterisk (*) to the right of the field.

Action: Continue on to the ***Access Request*** area of the **New User Registration** screen.

The ***Access Request*** area of the **New User Registration** screen contains fields that are specific to the CMS application that has been selected.

The ***Access Request*** area, as illustrated in Figure 7, will display the application selected, the *Role* and *Justification for Action* fields. The *Role* field contains a drop-down list of roles, as illustrated in Figure 7.



CMS is authorized to va… your legal name, Date of Birth and Social Security Number.

User Information

Title: * Last Name: Smith-Hernandez * Suffix:

Middle Initial: MA Example: MD, RN, LPN, MBA, PhD, etc. (Limit 12 characters)

Social Security Number: …t is XXX-XX-XXXX Date of Birth: 03/27/1973 * Valid Date of Birth format is mm/dd/yyyy

E-mail: * Confirm E-mail: shernandez-2013_01-5895@idm.cor *

Vali… …etprovider.domain. List of allowed domains: vi,com, gov, net, org, us, mil, biz, edu, pro

Professional Con…

Office Telephone: Valid Phone Number Format is XXX-XXX-XXXX

Company Name: * Company Telephone: 589-589-5891 Ext: 595

Address 1: * Address 2: Suite 102

City: * State/Territory: MD * Zip Code: 59529 * - 5954

Access Request

User Type:

Role: Select Role *

Justification for Action: Request initiated on 03/27/2013 11:21:28 AM *

Figure 7: New User Registration Screen: Access Request Area, Role Drop-Down List

Action: Select the *Role* field to display the list of roles. Select a role***.***

Note: The MA Submitter role will be used to illustrate common registration procedures and techniques that apply to registering for access to most other CMS Applications.

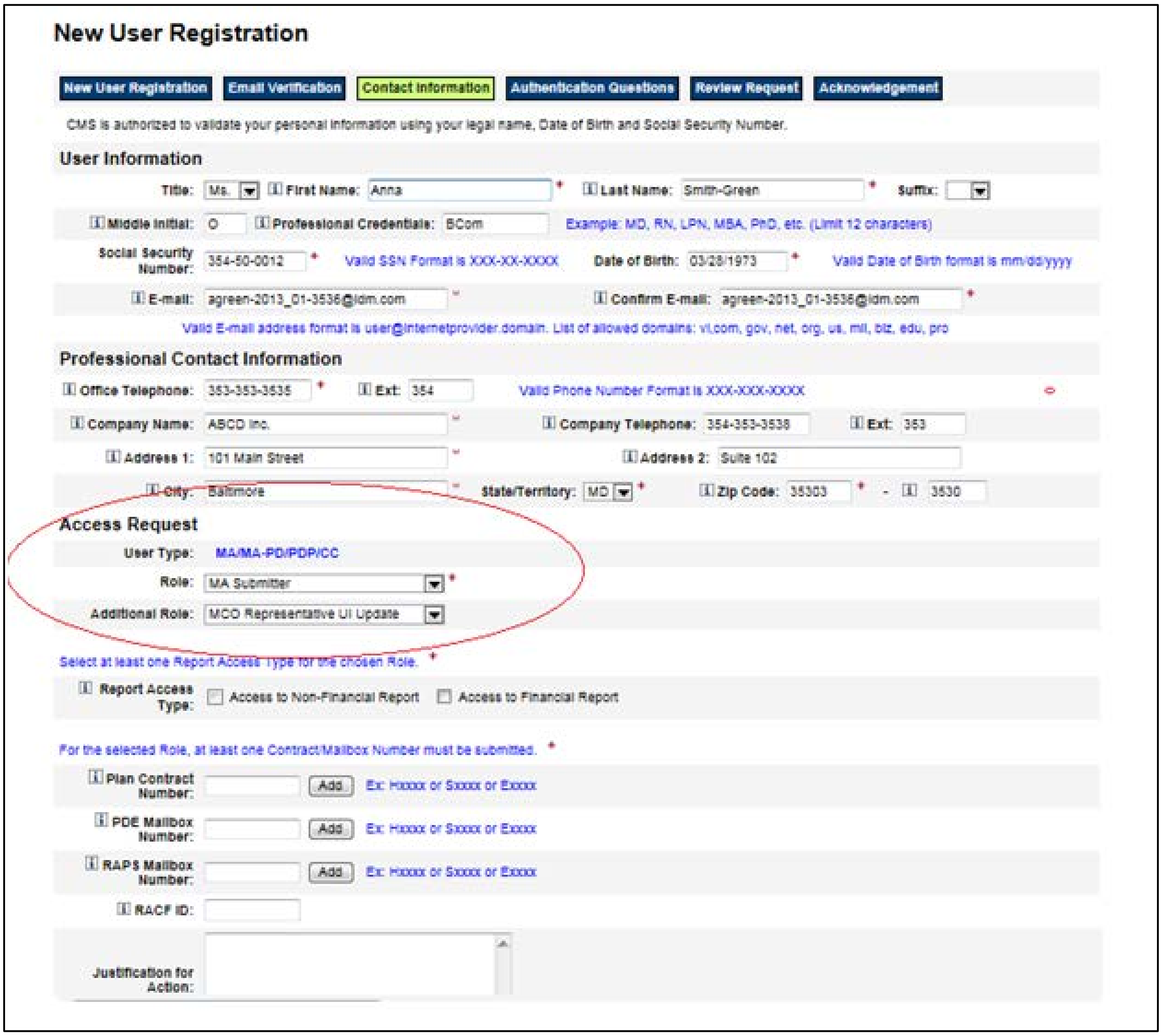
Note: The *Role* field displays the roles within the appropriate subheadings: *User roles, Approver roles, Helpdesk roles and Authorizer roles.*

If the user selects the role of MA Submitter, the screen will refresh and the following fields will display, as illustrated in Figure 8.

- *Additional Role*: The user may select an additional role during New User Registration. Refer to Table 1 for all the possible combinations that are allowed.
- *Report Access Type*: The user is required to select at least one report access type before continuing to add contract(s) by choosing one or both of the following check boxes, as needed.
    - Access to Non-Financial Report
    - Access to Financial Report

- Contract: The user may enter a contract number in the following fields:
  - Plan Contract Number field
  - Prescription Drug Event, PDE Mailbox Number field
  - Risk Adjustment Processing System, RAPS Mailbox Number field

The user can enter contract numbers in any, or all, of the Contract/Mailbox Number fields as they apply to the user's work.



New User Registration

CMS is authorized to validate your personal information using your legal name, Date of Birth and Social Security Number.

User Information

Title: Ms. First Name: Anna * Last Name: Smith-Green * Suffix:

Middle Initial: O Professional Credentials: BCom Example: MD, RN, LPN, MBA, PhD, etc. (Limit 12 characters)

Social Security Number: 354-50-0012 * Valid SSN Format is XXX-XX-XXXX Date of Birth: 03/28/1973 * Valid Date of Birth format is mm/dd/yyyy

E-mail: agreen-2013_01-3536@idm.com * Confirm E-mail: agreen-2013_01-3536@idm.com *

Valid E-mail address format is user@internetprovider.domain. List of allowed domains: vi,com, gov, net, org, us, mil, biz, edu, pro

Professional Contact Information

Office Telephone: 353-353-3535 * Ext: 354 Valid Phone Number Format is XXX-XXX-XXXX

Company Name: ABCD Inc. * Company Telephone: 354-353-3538 Ext: 353

Address 1: 101 Main Street * Address 2: Suite 102

City: Baltimore * State/Territory: MD * Zip Code: 35303 * - 3530

Access Request

User Type: MA/MA-PD/PDP/CC

Role: MA Submitter *

Additional Role: MCO Representative UI Update

Select at least one Report Access Type for the chosen Role. *

Report Access Type: □ Access to Non-Financial Report □ Access to Financial Report

For the selected Role, at least one Contract/Mailbox Number must be submitted. *

Plan Contract Number: Ex: Hxxxx or Sxxxx or Exxxx

PDE Mailbox Number: Ex: Hxxxx or Sxxxx or Exxxx

RAPS Mailbox Number: Ex: Hxxxx or Sxxxx or Exxxx

RACF ID:

Justification for Action:

Figure 8: New User Registration Screen: Access Request Area, MA Submitter

Action: Enter valid contract numbers one at a time in the appropriate fields.

Action: Select the ***Add*** button after each entry to record the contract number.

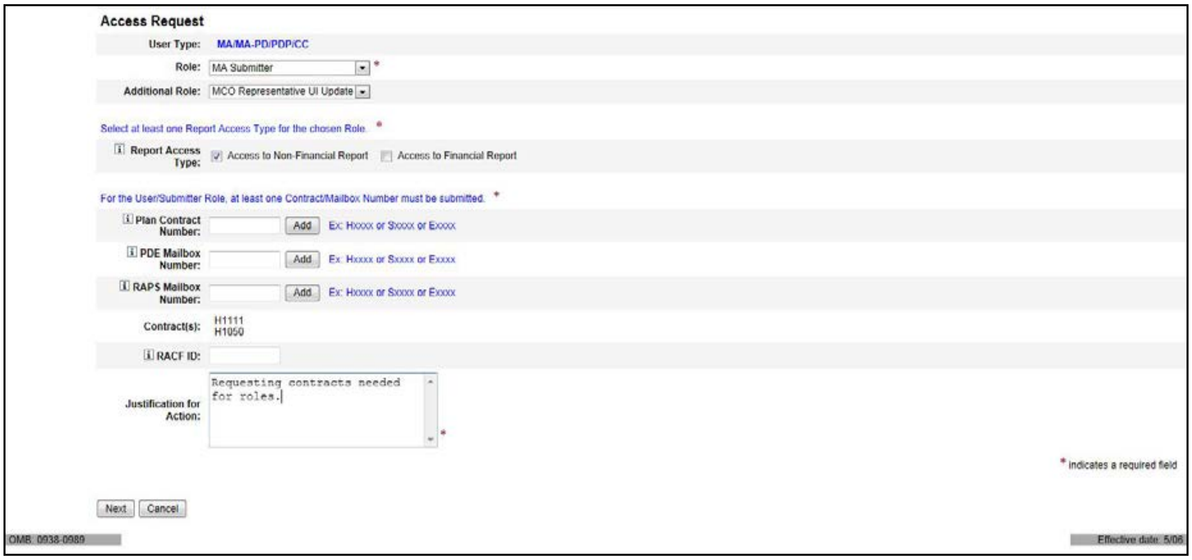
Note: Once a contract number has been added to the registration screen, it cannot be changed or removed. The user needs to ensure that he is requesting a valid contract for him to access on behalf of the company prior to selecting the ***Add*** button. If the user enters an incorrect contract number, he must cancel the registration request and start a new request.

Note: In this example, the MA Submitter user can only enter contracts starting with 'H', 'E', 'S', and '9'.

After each contract number is entered, the screen will refresh and display the entered contract numbers in separate, labeled fields under the *Plan Contract Number, PDE Mailbox Number*, and *RAPS Mailbox Number* fields, as illustrated in Figure 9.

Below the Contract Number fields is an additional field for the user to enter the RACF ID. If the user has an existing CMS four character RACF ID, enter it here. If the user has forgotten the RACF, the user can contact the MAPD Help Desk to obtain the RACF ID information.

If the user does not have a *RACF ID* at the time he completes the IACS New User Registration and the user's role requires a *RACF ID*, the system will automatically assign him a *RACF ID* once his request is approved.



Access Request

User Type: MA/MA-PD/PDP/CC

Role: MA Submitter *

Additional Role: MCO Representative UI Update

Select at least one Report Access Type for the chosen Role. *

Report Access Type: ☑ Access to Non-Financial Report □ Access to Financial Report

For the User/Submitter Role, at least one Contract/Mailbox Number must be submitted. *

Plan Contract Number: Ex: Hxxxx or Sxxxx or Exxxx

PDE Mailbox Number: Ex: Hxxxx or Sxxxx or Exxxx

RAPS Mailbox Number: Ex: Hxxxx or Sxxxx or Exxxx

Contract(s): H1111
H1050

RACF ID:

Justification for Action: Requesting contracts needed for roles. *

* indicates a required field

OMB: 0938-0989

Effective date: 5/06

Figure 9: New User Registration Screen: Access Request Area, Contract Number and RACF ID Field – MA Submitter

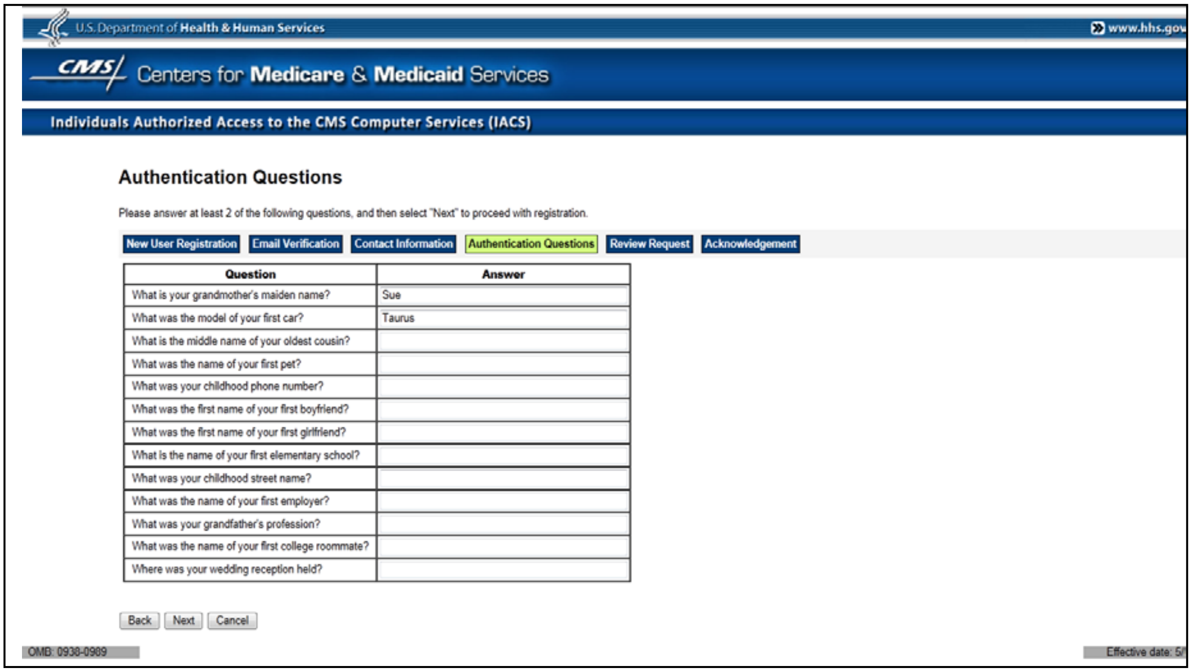
Action: Enter your *RACF ID*, if you have one.

Action: Enter a justification statement for the request in the *Justification for Action* field. This field must include the reason for requesting this action.

Action: Select the ***Next*** button when you are done filling in all the required fields on the **New User Registration** screen.

Once the data is validated, the system will display the **Authentication Questions** screen, as illustrated in Figure 10.

The user must answer a minimum of two Authentication Questions in order to complete his registration. These answers will be used to validate the user's identity should he attempt to recover his User ID or password using IACS' ***Forgot your User ID?*** or ***Forgot your Password?*** self-service features.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
Individuals Authorized Access to the CMS Computer Services (IACS)

Authentication Questions

Please answer at least 2 of the following questions, and then select "Next" to proceed with registration.

New User Registration
Email Verification
Contact Information
Authentication Questions
Review Request
Acknowledgement

Question	Answer
What is your grandmother's maiden name?	Sue
What was the model of your first car?	Taurus
What is the middle name of your oldest cousin?	
What was the name of your first pet?	
What was your childhood phone number?	
What was the first name of your first boyfriend?	
What was the first name of your first girlfriend?	
What is the name of your first elementary school?	
What was your childhood street name?	
What was the name of your first employer?	
What was your grandfather's profession?	
What was the name of your first college roommate?	
Where was your wedding reception held?	

OMB: 0938-0989

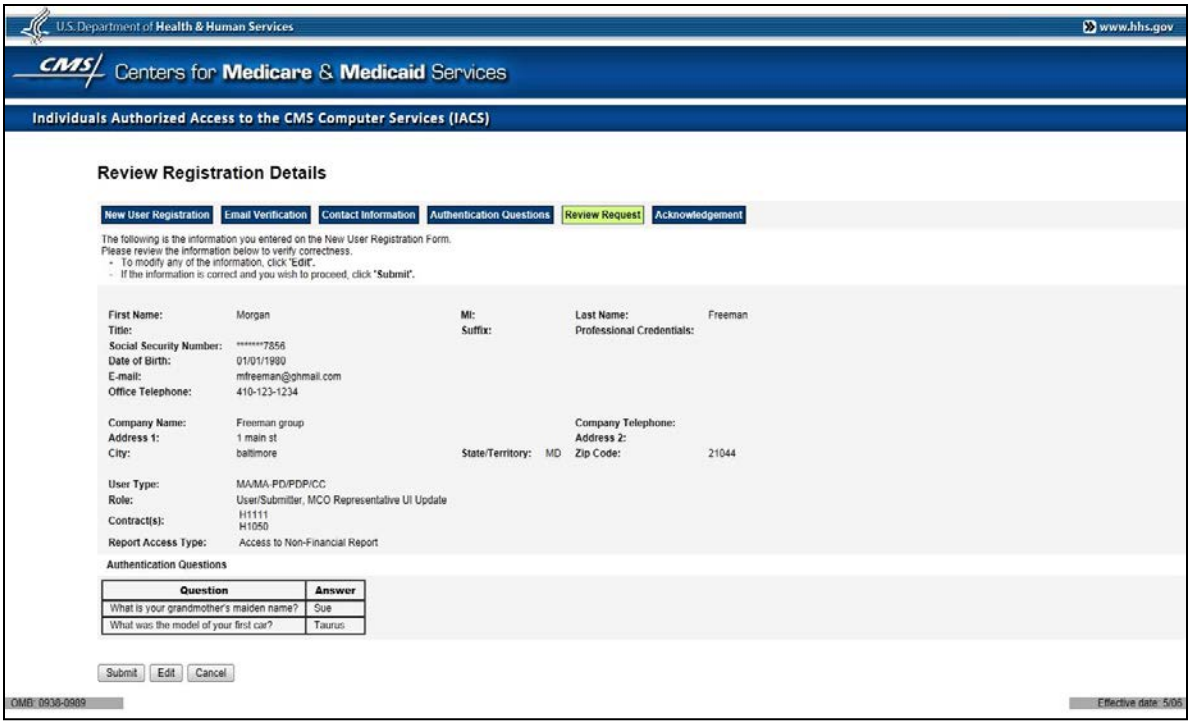
Effective date: 5/

Figure 10: Authentication Questions Screen

Action: Answer at least two of the Authentication Questions listed.

Action: Select the ***Next*** button.

The system will display the **Review Registration Details** screen, as illustrated in Figure 11.



Review Registration Details

The following is the information you entered on the New User Registration Form.
Please review the information below to verify correctness.
- To modify any of the information, click 'Edit'.
- If the information is correct and you wish to proceed, click 'Submit'.

First Name:	Morgan	MI:		Last Name:	Freeman
Title:		Suffix:		Professional Credentials:	
Social Security Number:	*******7856				
Date of Birth:	01/01/1980				
E-mail:	mfreeman@ghmail.com				
Office Telephone:	410-123-1234				
Company Name:	Freeman group			Company Telephone:	
Address 1:	1 main st			Address 2:	
City:	baltimore	State/Territory:	MD	Zip Code:	21044
User Type:	MA/MA-PD/PDP/CC				
Role:	User/Submitter, MCO Representative UI Update				
Contract(s):	H1111 H1050				
Report Access Type:	Access to Non-Financial Report				

Authentication Questions

Question	Answer
What is your grandmother's maiden name?	Sue
What was the model of your first car?	Taurus

Figure 11: Review Registration Details Screen

Action: Review the information presented in the **Review Registration Details** screen.

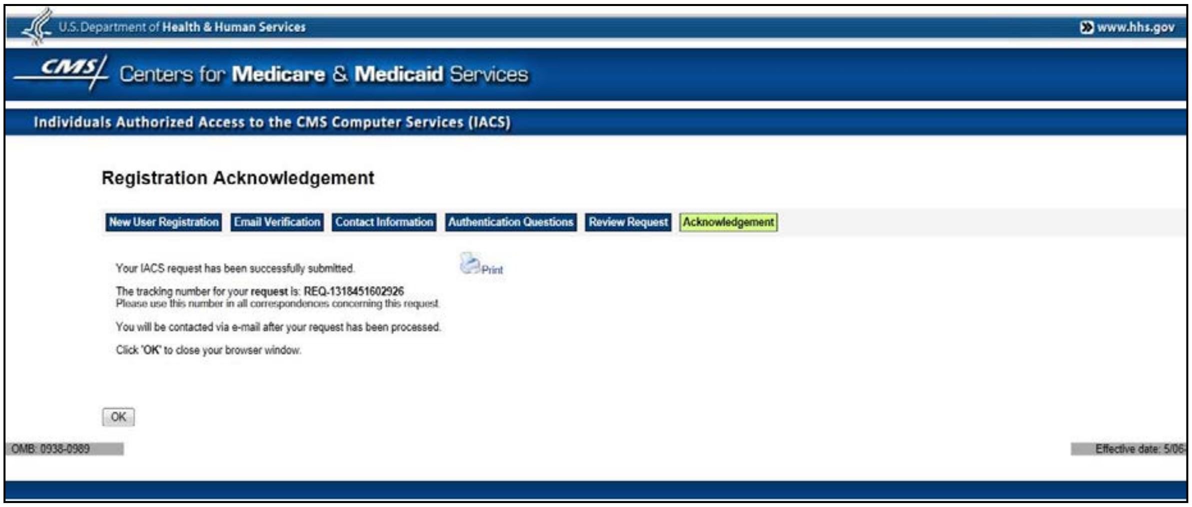
If you need to make any modifications to the registration information, use the ***Edit*** button. The **New User Registration** screens will be redisplayed with all information populated in the appropriate fields. The user may modify the information except for the previously entered E-mail address; and, when finished, he should select the ***Next*** button. He will again be presented with the **Review Registration Details** screen.

Note: The user will not be allowed to modify the *E-mail and Confirm E-mail* fields by selecting the ***Edit*** button from the **Review Registration Details** screen.

Action: Select the ***Submit*** button when you are satisfied that your registration information is correct. The **Registration Acknowledgement** screen will display, as illustrated in the example in Figure 12.

The **Registration Acknowledgement** screen indicates that the registration request has been successfully submitted and the request tracking number has been assigned. This tracking number should be recorded and used when the user has questions about the status of his request.

Note: The user can print the information contained on the **Registration Acknowledgement** screen by selecting the ***Print*** icon.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
Individuals Authorized Access to the CMS Computer Services (IACS)

Registration Acknowledgement

Your IACS request has been successfully submitted.

The tracking number for your **request** is: **REQ-1318451602926**
Please use this number in all correspondences concerning this request.

You will be contacted via e-mail after your request has been processed.

Click '**OK**' to close your browser window.

Figure 12: Registration Acknowledgement Screen

Action: Select the ***OK*** button.

> **Note:** The registration will not be completed unless the ***OK*** button is selected.

The **Registration Acknowledgement** screen will close and the system will return to the **Account Management** screen.

6.2 Registration Completion

After the user completes the IACS New User Registration, the user will be sent an E-mail confirming IACS has received the user's request with the request tracking number. The user should use the tracking number when referencing the request.

Note: If the E-mail notification has not been received within 24 hours after registration, the user should contact the Help Desk. See Section 18.0 for Help Desk contact information.

The user's Approver will be notified of the pending request via E-mail.

Once the Approver has approved the request and the account has been created, two separate E-mail messages are sent automatically to the user.

1. The first E-mail (Subject: FYI: User Creation Completed – Account ID Enclosed) will contain the IACS User ID.
2. The second E-mail (Subject: FYI: User Creation Completed – Password Enclosed) will contain the format of the initial password and instructions to change the initial password. The user will be required to change the initial password on the first login.

If the user's request for registration is rejected, the user will be sent an E-mail that the request was denied with the justification for the rejection.

If the Approver or External Point of Contact (EPOC) has not processed the registration request within 12 or 24 calendar days (depending on the role) of submission, the request will be cancelled. The registrant will be notified by E-mail of the cancelled request and the user will need to re-submit the request. Refer to Appendix B for a listing of request timeout days by role types.

6.3 CMS Applications Registration Tips

6.3.1 Bundled Payments EFT Registration:

- A user registering as a Bundled Payments EFT user will be required to enter the user's 4-digit Bundled Payments Participant ID (BPID).

6.3.2 COB Registration:

- A user registering as a User/Transmitter for the COB Application will be required to select an *Organization Identifier* from the drop-down list and add the organization numbers one at a time.

6.3.3 CPC Registration:

- A user registering as a CPC Market User should enter the *Market* and the *Organization Name*. The *Market* field is the geographic area of the selected practices they want to view. The *Organization Name* should match the CPC practice application or what has been updated through the CPC Support Team.
- A user registering as a CPC Basic User should enter the *Organization Name*, *Organization TIN*, *Provider NPI*, and the *Practice ID*. The *Practice ID* is the 8 character alphanumeric code unique to the practice and is a required field. If the user is not a provider and does not have a Provider NPI, then the *Practice ID* should be entered as N/A.
- A user registering as a CPC CMMI User; CPC Contractor - Operations Support; CPC Contractor - Learning and Diffusion; CPC Contractor – Evaluation or CPC Contractor – Payment should enter the *Organization Name*.

6.3.4 CSR Registration:

- The Approver or User registering for the CSR Application will select a *Call Center* from a list of existing call centers.

6.3.5 DMEPOS Registration:

- DMEPOS registration is divided into roles for bidders and their organizations and roles for the DBidS application Help Desk and system administration functions. After selecting "DMEPOS Bidding System (DBidS)" from the **New User Registration Menu** screen, the user will have to select one of two radio buttons to proceed. The text of the radio buttons is shown below:
  - I want to register as an Authorized Official, Backup Authorized Official, or End User for the DMEPOS Competitive Bidding System (DBidS)
  - I want to register as a DBidS Help Desk User

- A user registering as an Authorized Official, Backup Authorized Official, or End User for the DMEPOS Competitive Bidding System (DBidS), must provide the Provider Transaction Access Number (PTAN).
- A user registering as an Authorized Official should enter the *Organization Name*.
- A user registering as an Authorized Official may associate to more than one PTAN.

6.3.6 Gentran Registration:

- The Gentran registration link is for those users who only need access to a Gentran mailbox that is not associated with any other IACS supported application.
- A user registering for the Gentran User role will be able to enter one or more Gentran mailbox numbers.

Note: If you are registering for the COB, HPG, or MA/MA-PD/PDP/CC applications, do not register for Gentran through this link. The application registration process will associate the new User ID with the appropriate Gentran mailbox.

6.3.7 HETS UI Registration:

- A user registering as a Security Official, Approver, or End User must enter the *Billing Provider NPI* and select the *Provider Type*.
- A user registering as a Security Official will have to complete the ***EDI Registration Form*** to create an organization. The Security Official should select at least one *Contractor Name* from the drop-down list and enter the associated *Billing Provider Number*.

6.3.8 HPG Registration:

- A user registering as an HPG User will not be required to enter the Submitter ID. If the user has a valid Submitter ID, he may choose to enter it during registration.
- The user will have access to a Gentran mailbox once the Submitter ID has been added to his profile.

Notes:

- Submitter ID starting with ‘P’ will not have access to the Gentran mailbox.
- The user will have to contact the MCARE Help Desk in order to have their profile updated with the Submitter ID for Gentran mailbox access.

6.3.9 Internet Server Registration:

- A user registering as an Internet Server User will be required to enter the business application high level qualifier in the *Business Application* field.

6.3.10 MA/MA-PD/PDP/CC Registration:

- A user registering for roles in the MA/MA-PD/PDP/CC Application will be allowed to register for two roles at a time, as illustrated in Figure 8 and Figure 9. The possible role combinations and the shared attribute are listed in Table 1.

Roles	Additional Role to Request	Shared Attribute
MCO Representative UI Update	MA Submitter OR PDP Submitter	Contracts
MA Submitter	MCO Representative UI Update	Contracts
PDP Submitter	MCO Representative UI Update	Contracts
Report View	MA Representative OR PDP Representative	Contracts
MA Representative	Report View	Contracts
PDP Representative	Report View	Contracts
SPAP End User	MA State/Territory User	State/Territory Access
MA State/Territory User	SPAP End User	State/Territory Access

Table 1: Possible Role Combinations for MA/MA-PD/PDP/CC

MA Representative and MA Submitter:

- A user registering as an MA Submitter or MA Representative may only enter Contracts starting with ‘H’, ‘E’, ‘S’, and ‘9’.
- A user registering as an MA Submitter or MA Representative may add an additional role listed by using the *Additional Role* drop-down list on the **New User Registration** screen.
- A user registering as an MA Submitter must select the type of report they need access to: financial, non-financial or both, by selecting the appropriate *Report Access Type* check boxes.

MA State/Territory Approver:

- A user registering as a MA State Territory Approver will be required to select a State from the *State/Territory Access* drop-down list.

MA State/Territory User:

- A user registering as a MA State Territory User will be required to select a State from the *State/Territory Access* drop-down list.
- A user registering as a MA State/Territory User may add an additional SPAP End User role by using the *Additional Role* drop-down list on the **New User Registration** screen.

MMP User:

- A user registering as an MMP User may only enter Plan Contracts starting with ‘H’.

MCO Representative UI Update:

- A user registering as an MCO Representative UI Update may only enter Contracts starting with ‘H’, ‘E’, ‘S’, and ‘9’.
- A user registering as an MCO Representative UI Update may add an additional role by using the *Additional Role* drop-down list that provides the available roles on the **New User Registration** screen.

NET Submitter and NET Representative:

- A user registering as a NET Submitter cannot add a PDE / RAPs Mailbox.
- A user registering as a NET Submitter or NET Representative may only enter contracts starting with ‘X’.
- The user will have access to a Gentran mailbox.
- A user registering as a NET Submitter must select the type of report they need access to: financial, non-financial or both, by selecting the appropriate *Report Access Type* check boxes.

PDP Submitter and PDP Representative:

- A user registering as a PDP Submitter or PDP Representative may only enter contracts starting with ‘S’, ‘E’ and ‘9’.
- A user registering as a PDP Submitter or PDP Representative may add an additional role by using the *Additional Role* drop-down list that provides the available roles on the **New User Registration** screen.
- A user registering as a PDP Submitter must select the type of report they need access to: financial, non-financial or both, by selecting the appropriate *Report Access Type* check boxes.

Report View:

- A user registering as a Report View may add an additional role by using the *Additional Role* drop-down list that provides the available roles on the **New User Registration** screen.
- A user registering as a Report View must select the type of report they need access to: financial, non-financial or both, by selecting the appropriate *Report Access Type* **check boxes.**

POSFE Contractor:

- A user registering as a POSFE Contractor cannot enter contracts. The contract is defaulted to ‘R0000’.

SHIP Approver:

- A user registering as a SHIP Approver will not be associated with a State/Territory.

SHIP End User:

- A user registering as a SHIP End User will be required to select a State/Territory from the *State/Territory Access* drop-down list.

SPAP Approver:

- A user registering as a SPAP Approver will not be associated with a State/Territory.

SPAP End User:

- A user registering for a SPAP End User will be required to select a State/Territory from the *State/Territory Access* drop-down list.
- A user registering as a SPAP End User may add an additional MA State/Territory User role by using the *Additional Role* drop-down list on the **New User Registration** screen.

6.3.11 MACPro Registration:

- A user registering for the MACPro Application will enter the User and Professional Contact information and select the role.

6.3.12 MED Registration:

- A user registering as a MED Administrator or a MED Power User will be required to select a *Gentran Mailbox*.
- A user registering as a MED User will be required to select a *Gentran Mailbox* and the *Request Type*. The *Contract Number*, *Agency Name* and *COR Name* fields are optional.

6.3.13 MyCGS Registration:

- The user registering as an Authorized Official for the CGS Application will be able to create the organization or associate to an existing organization.
- The Authorized Official creating the organization will enter the organization details, *NPI*, *PTAN*, *Tax ID/EIN*, and *Total amount of the last check received*. An Authorized Official that associates to an organization will search for the organization by entering the *Tax ID/EIN* and the Total amount of last check received. A list of the organizations matching the search criteria will be displayed for the user to select.
- The Back-up Authorized Official will be able to associate to an organization. The user will search for the organization by entering the *Tax ID/EIN* and *Total amount of the last check received*. A list of the organizations matching the search criteria will be displayed for the user to select.

- The CGS End User will be able to associate to an organization. The user searches for the organization by entering the *Tax ID/EIN* and then selects the ***Search*** button. A list of the organizations matching the *Tax ID/EIN* will be displayed for the user to select.

6.3.14 Novitasphere Registration:

- A user registering as a Provider Office Approver, Billing Office Approver, or Novitas Solutions Approver will be able to create the organization or associate to an existing organization.
- The Provider Office Approver or Billing Office Approver creating the organization will enter the organization details, *TIN/SSN*, and *NPI-PTAN-Submitter ID* combinations. The organization *NPI-PTAN-Submitter ID* combination should be in the following format: NPI1,PTAN1,SubmitterID1,NPI2,PTAN2,SubmitterID2, etc.
- The Novitas Solutions Approver should leave *the NPI, PTAN and Submitter ID(s)* field blank.
- IACS allows multiple approvers for an organization. One approver will create the organization. Once the request has been approved, the other approvers will be able to search and associate to that existing organization.
- The Provider Office Approver, Billing Office Approver, or Novitas Solutions Approver that associate to an organization will search for the organization by entering the *Legal Business Name* and *State/Territory*. The list of organizations matching the search criteria will display for the Approver to select.
- A user registering as a Back-up Approver or Novitasphere End User will be able to search for the organization by entering the *Legal Business Name* and *State/Territory*. The list of organizations matching the search criteria will display for the user to select.

6.3.15 PQRS/eRx Registration:

Security Official (SO):

- A user registering as a Security Official can choose either to create a new organization or associate to an existing organization.
- The Security Official will be able to select the option to have approval authority for users requesting 2-Factor Authentication.
- The Security Official for PQRS/eRx will be able to enter multiple *NPI(s)* and *PTAN(s)* values during New User Registration.

Backup Security Official (BSO):

- A user registering as a Backup Security Official will be required to search and associate to an existing PQRS organization during the registration process.
- The Backup Security Official will be able to select the option to have approval authority for users requesting 2-Factor Authentication.

- The Backup Security Official for PQRS/eRx will be able to enter multiple *NPI* and *PTAN* values during New User Registration.

EHR Submitter:

- A user registering as an EHR Submitter will have the 2-Factor Authentication role by default.
- The user will not be able to proceed with the registration, if there is no corresponding Approver with a 2-Factor Authentication Approver role for the organization selected by the user.
- The user will be able to choose the *Preferred 2nd Factor Notification Method* by selecting the E-mail, SMS/Mobile or Interactive Voice Response Number (IVR) option from the drop-down list, labeled as the *Preferred 2nd Factor Notification Method*.
- The user will be required to enter the mobile phone number, if SMS/Mobile was selected as the *Preferred 2nd Factor Notification Method*.
- The user will be required to input the interactive voice response number if IVR number was selected as the *Preferred 2nd Factor Notification Method*.
- The user will be required to search and associate to an existing PQRS organization.

EHR Vendor:

- A user registering as an EHR Vendor will be able to select an organization from a pre-defined list of EHR vendor organizations.

End User:

- A user registering as an End User will be required to search and associate to an existing PQRS organization.

Health Information Exchange (HIE) User:

- A user registering as an HIE User will have the 2-Factor Authentication role by default.
- A user registering as an HIE User will be able to select an organization from a pre-defined list of HIE organizations.
- The user will be able to choose the *Preferred 2nd Factor Notification Method* by selecting the E-mail, SMS/Mobile or Interactive Voice Response Number (IVR) from the drop-down list, labeled as *Preferred 2nd Factor Notification Method*.
- The user will be required to enter the mobile phone number, if SMS/Mobile was selected as the *Preferred 2nd Factor Notification Method*.
- The user will be required to input the interactive voice response number, if IVR number was selected as the *Preferred 2nd Factor Notification Method*.

Individual Practitioner:

- A user registering as an Individual Practitioner will have the option to select the 2-Factor Authentication role.
- The user will be required to acknowledge and confirm that registration as an eligible Individual Practitioner is only for those who receive their Medicare payment under their Social Security Number.

Individual Practitioner with 2-Factor Authentication:

- The user will be able to choose the *Preferred 2nd Factor Notification Method* by selecting the E-mail, SMS/Mobile or Interactive Voice Response Number (IVR) from the drop-down list, labeled as *Preferred 2nd Factor Notification Method*.
- The user will be required to enter the mobile phone number, if SMS/Mobile was selected as the *Preferred 2nd Factor Notification Method*.
- The user will be required to input the interactive voice response number, if IVR number was selected as the *Preferred 2nd Factor Notification Method*.

Registry End User:

- A user registering as a Registry End User will be able to select the organization from a pre-defined list of organizations.

PQRS Submitter User:

- A user who chooses to register as a PQRS Submitter without associating to an organization must indicate this by selecting the *I want to register without associating to an Organization* radio button.
- A user registering as a PQRS Submitter will have the 2-Factor Authentication role by default.
- The user will be able to choose the *Preferred 2nd Factor Notification Method* by selecting the E-mail, SMS/Mobile or Interactive Voice Response Number (IVR) from the drop-down list, labeled as *Preferred 2nd Factor Notification Method*.
- The user will be required to enter the mobile phone number, if SMS/Mobile was selected as the *Preferred 2nd Factor Notification Method*.
- The user will be required to input the interactive voice response number, if IVR number was selected as the *Preferred 2nd Factor Notification Method*.
- If a user chooses to associate to an organization, the user will be required to search and associate to an existing PQRS organization.
- The PQRS Submitter that is not associated to an organization will be able to enter multiple *NPI* and *PTAN* values during New User Registration.

PQRS Representative User:

- A user who chooses to register as a PQRS Representative, without associating to an organization, must indicate this by selecting the *I want to register without associating to an Organization* radio button.
- The user will be required to search and associate to an existing PQRS organization if he chooses to associate to an organization.
- The PQRS Representative that is not associated to an organization will be able to enter multiple *NPI* and *PTAN* values during New User Registration.

6.3.16 PS&R/STAR Registration:

- After selecting the PS&R/STAR hyperlink from the **New User Registration Menu** screen, users registering for the PS&R and STAR Applications will have to select one of the following four radio buttons to proceed:
    - I work for an FI/Carrier/MAC, and I want to register for PS&R and/or STAR.
    - I work for a Medicare Provider, and I want to register for PS&R.
    - I work for CMS or the PS&R/STAR System Maintainer, and I want to register for PS&R and/or STAR.
    - I work for the IACS Help Desk, and I want to register for PS&R and/or STAR.

PS&R/STAR Security Official:

- A user registering as a PS&R/STAR Security Official will be required to associate to an existing organization by selecting from a pre-defined list of FI/Carrier/MAC organizations.

PS&R/STAR Backup Security Official:

- A user registering as a PS&R/STAR Backup Security Official will be required to select an organization from a pre-defined list of FI/Carrier/MAC organizations.

PS&R Security Official:

- A user working for a Medicare Provider and registering as a PS&R Security Official may choose either to create a new organization or associate to an existing organization.
- If a user registering as a PS&R Security Official chooses to create a new organization, then he will be required to provide one or more CMS Certification Numbers (CCN).

PS&R Backup Security Official:

- A user registering as a PS&R Backup Security Official will be required to search and associate to an existing FI/Carrier/MAC organization.

PS&R Admin:

- A user registering as a PS&R Admin for an FI/Carrier/MAC organization will be required to select an organization from a pre-defined list of FI/Carrier/MAC organizations.
- A user registering as a PS&R Admin for a Provider organization will be required to search and associate to an existing Provider organization.

PS&R User:

- A user registering as a PS&R User for an FI/Carrier/MAC organization will be required to select an organization from a pre-defined list of FI/Carrier/MAC organizations.
- A user registering as a PS&R User for a Provider organization will be required to search and associate to an existing Provider organization.

STAR User:

- A user registering as a STAR User for an FI/Carrier/MAC organization will be required to select an organization from a pre-defined list of FI/Carrier/MAC organizations.

6.3.17 PV/PQRS Registration System Registration:

- A user registering as a PV PQRS Group Security Official or PV PQRS Individual can choose to either create a new organization or associate to an existing organization.
- The PV PQRS Group Security Official creating the organization will enter the organization details, *TIN, Legal Business Name*, *NPI* and Individual Physician's *PTAN* corresponding to the *NPI*. The organization must have at least two Individual Physicians in the group.
- The PV PQRS Individual will create the Individual Eligible Professional group by providing the *TIN*, *NPI* and *PTAN* corresponding to the *NPI*.
- A user registering as a PV PQRS Group Representative will be required to associate to an existing organization. The user will select the organization from the drop-down list based on the search criteria.
- A user registering as a PV PQRS Individual Representative will be required to associate to an existing Individual Eligible Professional group. The user will select the organization from the drop-down list based on the search criteria.

6.3.18 The SPOT– First Coast Service Options Internet Portal Registration:

- A user registering for the FCSO Portal User role will be required to enter the *NPI*, *PTAN*, and the *last 5 digits of TIN/SSN*. Then, the user will select the *Practice Official Role, Provider Type,* and the *Line of Business* from the drop-down list.

6.3.19 VMS Client Letter Registration:

- A user registering as any of the End User roles will be required to enter an eight character *Tulsa RACF ID*.

6.3.20 Top of the Chain User Registration:

- IACS uses a chain of trust for approvals and authorizations; that is, End Users are approved by Approvers, Approvers are approved by Authorizers or by Helpdesk users in certain applications. Thus, the Top of the Chain user is either the Authorizer or the Helpdesk user and is the highest level in the chain that is expected to have an IACS User ID.
- IACS Administration approves the Top of the Chain user's request for New User Registration, Profile Modification, and Annual Certification request upon the receipt of a service request from the Business Owner/Representative. After the Top of the Chain user submits a request, the Business Owner or their representative will receive an E-mail that there is a pending registration request and the role being requested and the following Required Action(s) must be completed to approve or reject the request:
  1. Please forward this E-mail to CMS IT Service Desk (cms_it_service_desk@cms.hhs.gov).
  2. Request a Service Request (SR) be directed to IACS Administration.
  3. IMPORTANT: Indicate that you either "Approve" or "Reject" the pending Registration Request for <UserName> for the <RoleName> role.

The Top of the Chain roles for each application are described in Appendix A.

6.3.21 Create or Associate to an Organization

Some applications require users to be organized by organization. For the CMS applications that require organizational structure, authorized users will create the organization.

Table 2 lists the applications and the roles that will be able to create the organization. These roles will also be able to associate to an existing organization and will be able to approve requests for that organization.

CMS Application	Roles that Can Create an Organization or Associate to an Organization
PQRS/eRx	Security Official
PV/PQRS Registration System	PV/PQRS Group Security Official PV PQRS Individual
Novitasphere	Provider Office Approver Billing Office Approver Novitas Solutions Approver
MyCGS	CGS Authorized Official

CMS Application	Roles that Can Create an Organization or Associate to an Organization
PS&R (Medicare Provider)	PS&R Security Official

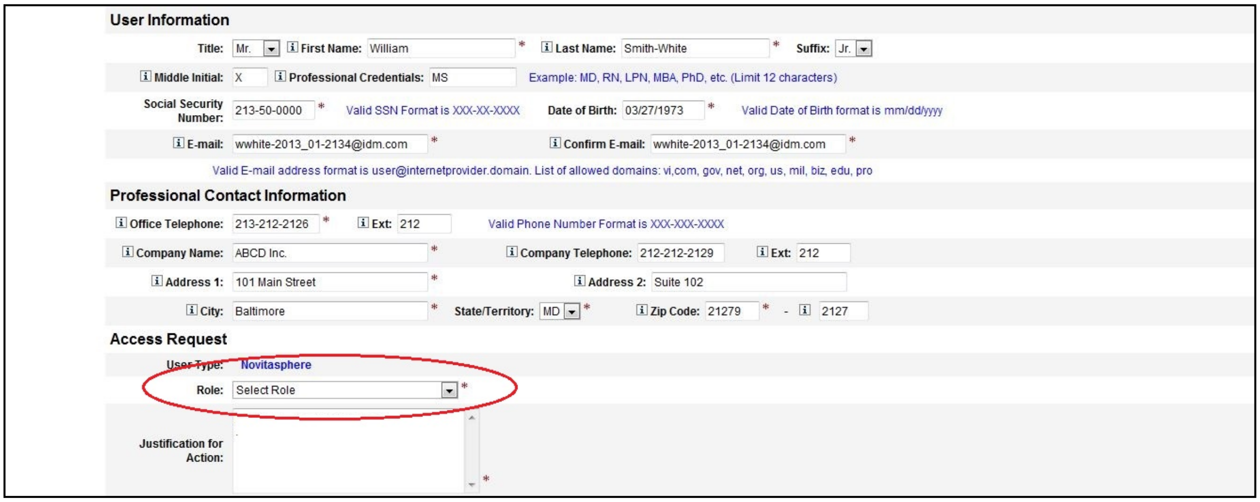
Table 2: CMS Application and Roles Create an Organization

The ***Access Request*** section of the **New User Registration** screen will prompt the user for the information needed by the CMS application based on the role selected.

The Novitasphere application will be used as an example to illustrate how the Provider Office Approver role can create an organization and how another Provider Office Approver can associate to the same organization. The registration steps for the applications and roles listed in Table 2 are the same. The ***Organization Information*** will be application specific.

Provider Office Approver Creates an Organization

Action: In the ***Access Request*** section, select the Provider Office Approver role, from the *Role* drop-down list.



User Information

Title: Mr. First Name: William * Last Name: Smith-White * Suffix: Jr.

Middle Initial: X Professional Credentials: MS Example: MD, RN, LPN, MBA, PhD, etc. (Limit 12 characters)

Social Security Number: 213-50-0000 * Valid SSN Format is XXX-XX-XXXX Date of Birth: 03/27/1973 * Valid Date of Birth format is mm/dd/yyyy

E-mail: wwhite-2013_01-2134@idm.com * Confirm E-mail: wwhite-2013_01-2134@idm.com *

Valid E-mail address format is user@internetprovider.domain. List of allowed domains: vi,com, gov, net, org, us, mil, biz, edu, pro

Professional Contact Information

Office Telephone: 213-212-2126 * Ext: 212 Valid Phone Number Format is XXX-XXX-XXXX

Company Name: ABCD Inc. * Company Telephone: 212-212-2129 Ext: 212

Address 1: 101 Main Street * Address 2: Suite 102

City: Baltimore * State/Territory: MD * Zip Code: 21279 * - 2127

Access Request

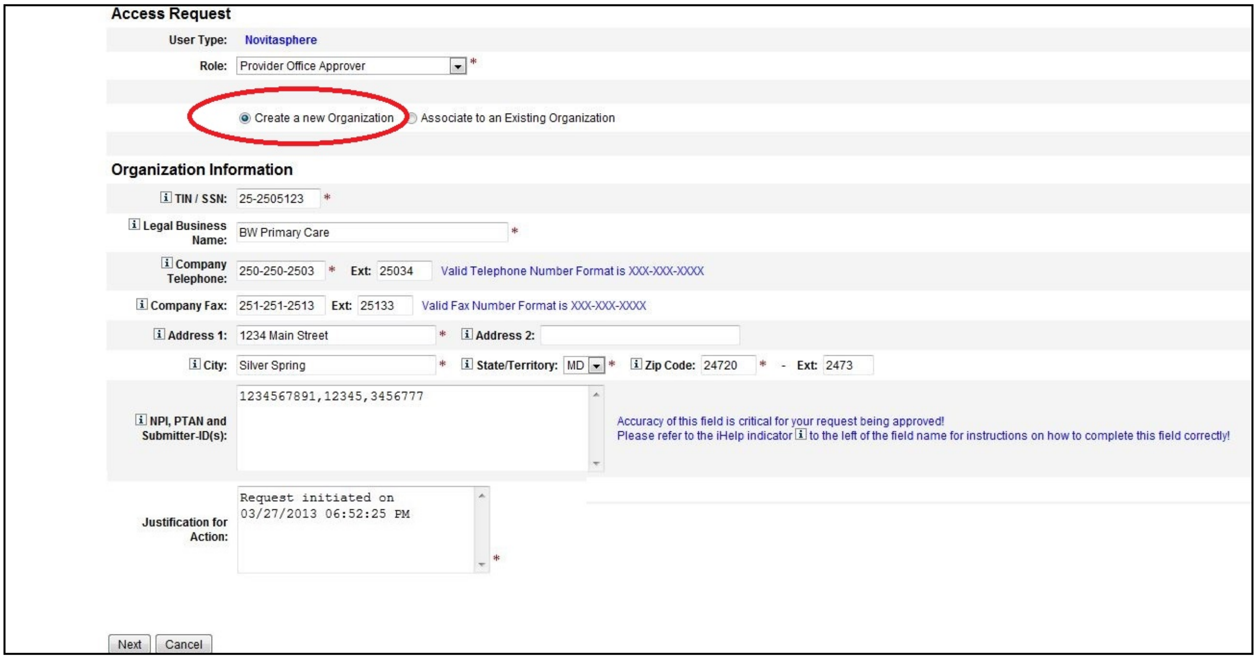
User Type: Novitasphere

Role: Select Role *

Justification for Action: *

Figure 13: Access Request - Select the Role

Action: Select the *Create a new Organization* radio button.



Access Request

User Type: Novitasphere

Role: Provider Office Approver *

● Create a new Organization ○ Associate to an Existing Organization

Organization Information

TIN / SSN: 25-2505123 *

Legal Business Name: BW Primary Care *

Company Telephone: 250-250-2503 * Ext: 25034 Valid Telephone Number Format is XXX-XXX-XXXX

Company Fax: 251-251-2513 Ext: 25133 Valid Fax Number Format is XXX-XXX-XXXX

Address 1: 1234 Main Street * Address 2:

City: Silver Spring * State/Territory: MD * Zip Code: 24720 * - Ext: 2473

NPI, PTAN and Submitter-ID(s): 1234567891,12345,3456777

Accuracy of this field is critical for your request being approved!
Please refer to the iHelp indicator to the left of the field name for instructions on how to complete this field correctly!

Justification for Action: Request initiated on 03/27/2013 06:52:25 PM *

Figure 14: Access Request – Create a New Organization

Action: Enter the required data in the **Organization Information** area.

Action: Enter the reason for the request in the *Justification for Action* field. Select the ***Next*** button to continue with the registration.

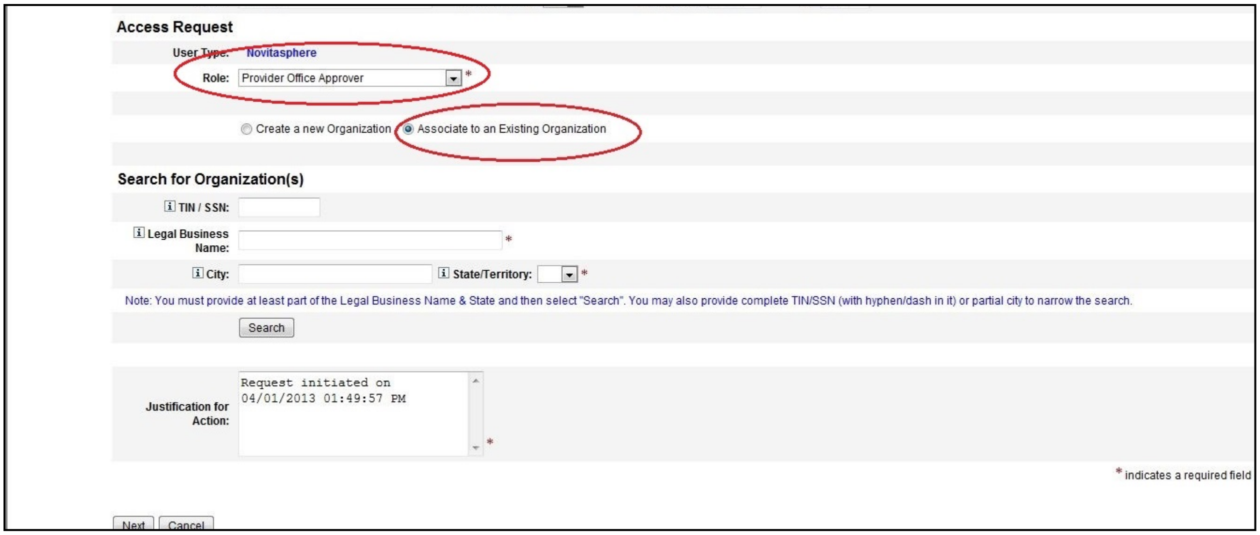
Provider Office Approver Associates to an Existing Organization

After the organization has been created and approved, another Provider Office Approver will be able to register as an approver of the existing organization.

The ***Access Request*** section of the **New User Registration** screen will prompt the user for the information needed by the CMS application based on the role selected.

Action: In the ***Access Request*** section, select the Provider Office Approver role from the *Role* drop-down list.

Action: Select the *Associate to an Existing Organization* radio button.



Access Request

User Type: Novitasphere

Role: Provider Office Approver *

○ Create a new Organization ● Associate to an Existing Organization

Search for Organization(s)

TIN / SSN:

Legal Business Name: *

City: State/Territory: *

Note: You must provide at least part of the Legal Business Name & State and then select "Search". You may also provide complete TIN/SSN (with hyphen/dash in it) or partial city to narrow the search.

Search

Justification for Action: Request initiated on 04/01/2013 01:49:57 PM *

* indicates a required field

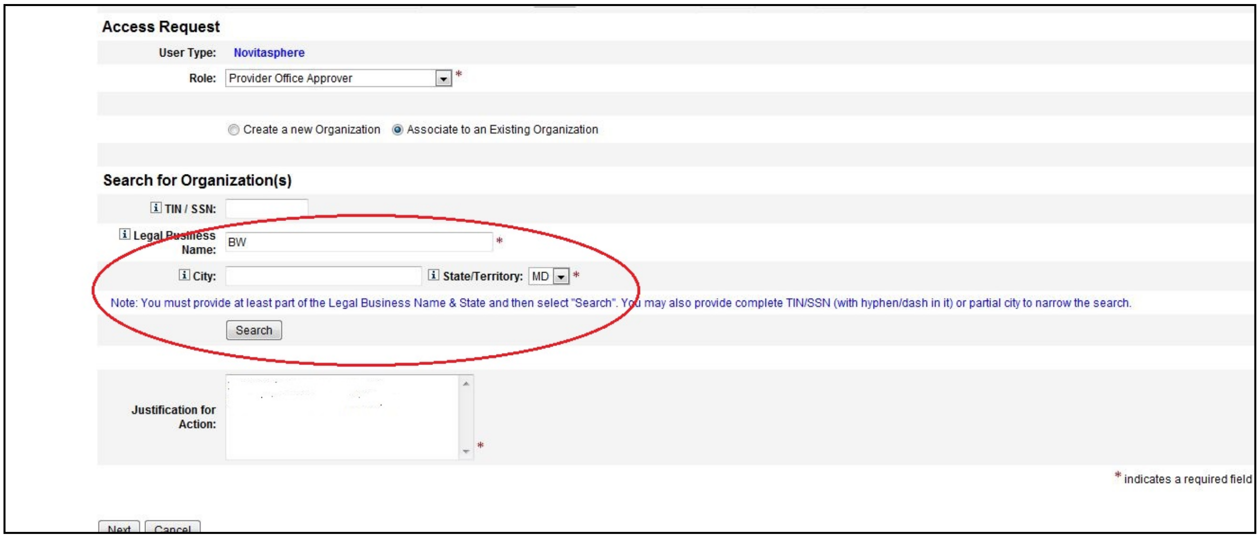
Next Cancel

Figure 15: Access Request – Select Role and Associate to an Existing Organization

Action: In the **Search for the Organization(s)** section, enter at least part of the Legal Business Name in the *Legal Business Name* field and select the state or territory from the *State/Territory* drop-down list.

Note: Required search fields are indicated with an asterisk (*). Provide as much of the required information in the search field for better search results.

Action: Select the ***Search*** button.



Access Request

User Type: Novitasphere

Role: Provider Office Approver *

○ Create a new Organization ● Associate to an Existing Organization

Search for Organization(s)

TIN / SSN:

Legal Business Name: BW *

City: State/Territory: MD *

Note: You must provide at least part of the Legal Business Name & State and then select "Search". You may also provide complete TIN/SSN (with hyphen/dash in it) or partial city to narrow the search.

Search

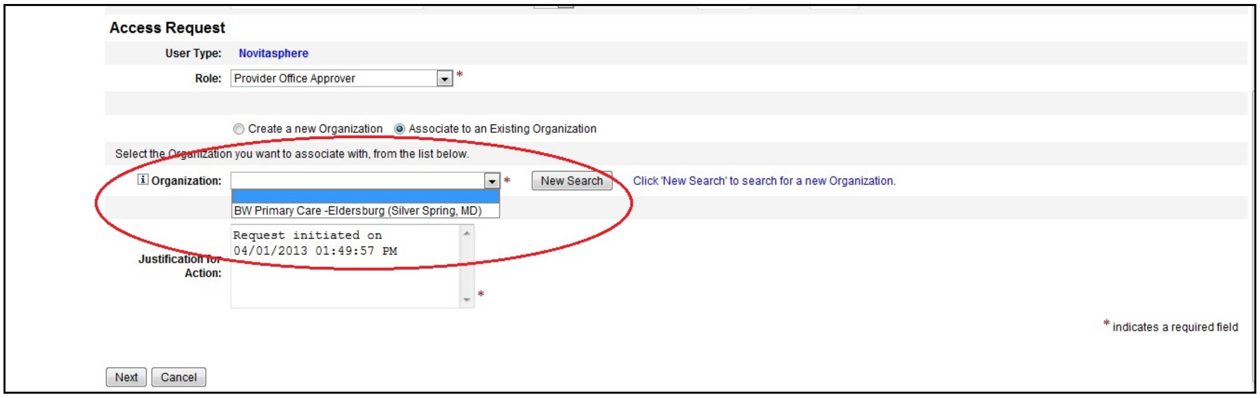
Justification for Action: *

* indicates a required field

Next Cancel

Figure 16: Search for the Organization

Action: Select the organization from the *Organization* drop-down list.



Access Request

User Type: Novitasphere

Role: Provider Office Approver *

○ Create a new Organization ● Associate to an Existing Organization

Select the Organization you want to associate with, from the list below.

Organization: *

BW Primary Care -Eldersburg (Silver Spring, MD)

Click 'New Search' to search for a new Organization.

Justification for Action: Request initiated on 04/01/2013 01:49:57 PM *

* indicates a required field

Figure 17: Select the Organization

Action: Enter the reason for the request in the *Justification for Action* field. Select the ***Next*** button to continue with the registration.

7.0 Using IACS

Once a user is approved for a CMS application, the user will return to the IACS application to perform the following functions:

- "Forgot Your Password?" self-service recovery
- "Forgot Your User ID?" self-service recovery
- Change password, at least every 60 days
- Re-enable an account disabled following 60 days of inactivity.
- Add new application or role
- Remove role
- Modify user and professional contact information
- Complete the mandatory Annual Certification

7.1 IACS Login

To log in to IACS, you will need to take the following actions:

Action: Navigate to https://applications.cms.hhs.gov.

Note: Alternatively, users may navigate to http://www.cms.gov/iacs and select the link for My Profile.

Action: Read the contents of the **CMS Applications Portal WARNING/REMINDER** screen, and agree by selecting the ***Enter CMS Applications Portal*** button.

The **CMS Applications Portal Introduction** screen will display, as illustrated in Figure 1.

Action: Select the Account Management hyperlink in the menu bar toward the top of the screen.

The screen will refresh and display the **Account Management** screen, as illustrated in Figure 2.

Action: Select the My Profile hyperlink on the **Account Management** screen.

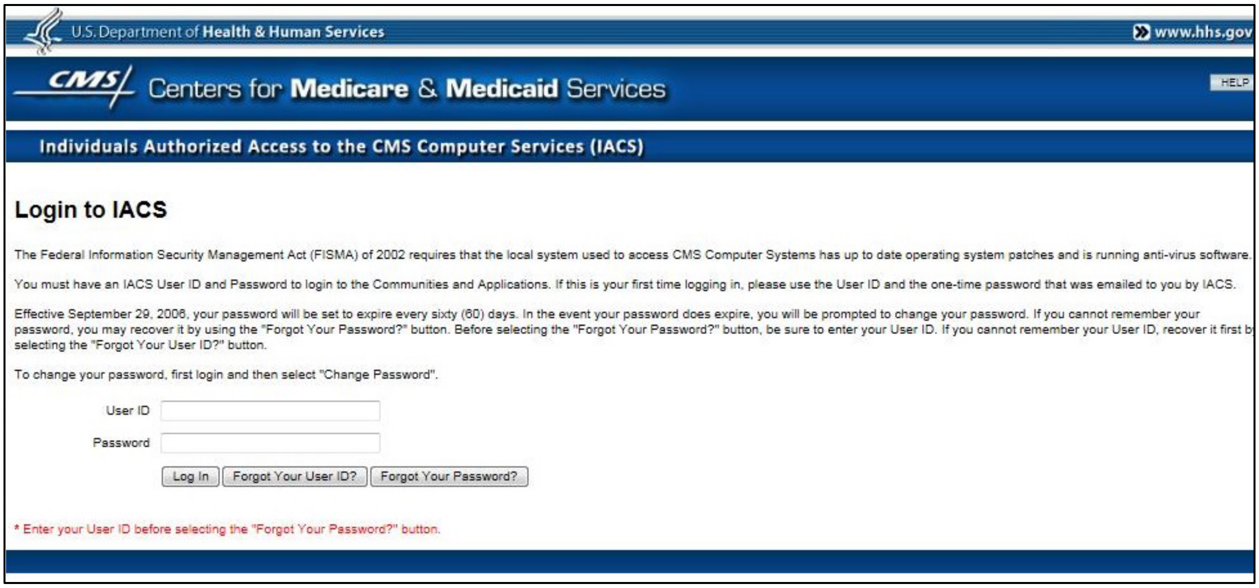
The **Terms and Conditions** screen will display.

All the ***Terms and Conditions*** on the screen should be read. This includes the Privacy Act Statement and the Rules of Behavior. The user can select the ***Print*** icon to the right of the text if he wants to print this information.

To accept the **Terms and Conditions,** the user must select the ***I Accept the above Terms and Conditions*** check box followed by the ***I Accept*** button.

If the user selects the ***I Decline*** button, a small window will appear with a message asking him to confirm his decision to decline. If the user confirms his decline, his IACS session will be cancelled and a screen indicating this will be displayed.

After accepting the **Terms and Conditions**, the **Login to IACS** screen will be displayed, as illustrated in Figure 18.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Login to IACS

The Federal Information Security Management Act (FISMA) of 2002 requires that the local system used to access CMS Computer Systems has up to date operating system patches and is running anti-virus software.

You must have an IACS User ID and Password to login to the Communities and Applications. If this is your first time logging in, please use the User ID and the one-time password that was emailed to you by IACS.

Effective September 29, 2006, your password will be set to expire every sixty (60) days. In the event your password does expire, you will be prompted to change your password. If you cannot remember your password, you may recover it by using the "Forgot Your Password?" button. Before selecting the "Forgot Your Password?" button, be sure to enter your User ID. If you cannot remember your User ID, recover it first b selecting the "Forgot Your User ID?" button.

To change your password, first login and then select "Change Password".

User ID

Password

* Enter your User ID before selecting the "Forgot Your Password?" button.

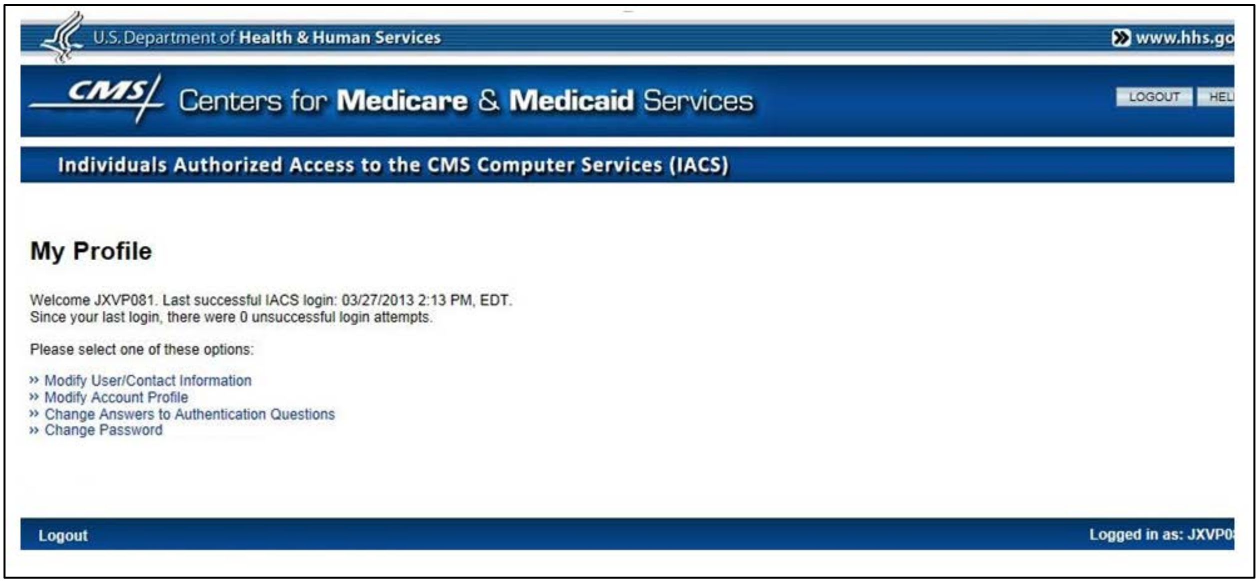
Figure 18: Login to IACS Screen

Action: Enter your new ***User ID***.

Action: Enter your *Password.*

Action: Select the ***Log In*** button*.*

The system will display the **My Profile** screen, as illustrated in Figure 19. Refer to Section 7.2 for further information.


U.S. Department of Health & Human Services
www.hhs.go
CMS Centers for Medicare & Medicaid Services
LOGOUT
HEL
Individuals Authorized Access to the CMS Computer Services (IACS)
Logout
Logged in as: JXVP0

My Profile

Welcome JXVP081. Last successful IACS login: 03/27/2013 2:13 PM, EDT.
Since your last login, there were 0 unsuccessful login attempts.

Please select one of these options:

» Modify User/Contact Information
» Modify Account Profile
» Change Answers to Authentication Questions
» Change Password

Figure 19: My Profile Screen: MA/MA-PD/PDP/CC Application Users

Action: Select the hyperlink for the function to work.

> **Note:** The first time the user logs in to IACS, he will be prompted to enter the User ID and the initial password pattern will be sent to the e-mail account on record. The user will be prompted to change the password to create a new password. After the password has been changed successfully, the system will display the **My Profile** screen.

7.2 My Profile Screen

The **My Profile** screen is the main IACS menu. The user will select one of the hyperlinks below to navigate to the IACS application. The hyperlinks will be displayed based on the user's role(s). Fields are editable based on each application's requirements.

The following hyperlink is available for all application users except COB, CSR, HETS UI, and HPG.

- Modify User/Contact Information
    - Modify select fields, including E-mail address

The following hyperlinks are available to all registered IACS users:

- Modify Account Profile
    - View details pertaining to the user's IACS Access Profile
    - Request Access/Remove Access to CMS applications integrated with IACS
    - Modify User's profile
- Change Answers to Authentication Questions
- Change Password

- Certify Account profile (Certification due on mm/dd/yyyy)

The following hyperlinks are available to users with approver roles:

- Pending Approvals
  - Approve/Reject/Defer New User Registration or modification requests
- Manage users under my authority
  - Search and view users
  - Specific to applications
    - Disassociate a user from the Security Official Organization
    - Remove Organization Number
    - Manage Contracts
    - Remove Call Centers, Submitter ID
- Pending Certification
  - Approve/Reject/Defer Pending Certification requests.

The following hyperlinks are available to users with help desk roles who will be able to perform the following functions:

- Manage users under my authority
  - Search and view users
  - Disable a user's account
  - Reset Password
  - Unlock a user's account
  - View archived users
- User Lookup
  - Search for any user's Help Desk contact information

The following hyperlinks are application specific:

- Search and View (Only) Pending Approvals (PQRS/eRx, PS&R/STAR, HPG and HETS UI)
  - The supporting Help Desks for these applications will be able to search pending requests.
- PQRS/eRx User Report
  - The PQRI Help Desk will be able to create user reports and export the report to an .xls file.

- Search and Modify DMEPOS User Profiles
    - The CBIC Tier 2 user will be able to search and perform the following actions for a selected DMEPOS user:
        - Disassociate from the role
        - Disassociate from the PTAN
        - Convert a BAO to AO, removing the existing AO from the DMEPOS application

8.0 Managing User IDs & Passwords

The IACS password must conform to the following CMS Password Policy:

- The password must be changed at least every 60 days.
- The password must be eight characters long.
- The password must start with an alphabetical character.
- The password must contain at least one number.
- The password must contain at least one lower case letter.
- The password must contain at least one upper case letter.
- The password must not contain the User ID.
- The password must not contain four consecutive characters from any of the previous six passwords.
- The password must be different from the previous six passwords.

In addition:

- The password must not contain any of the following reserved words or number combinations: 1234, PASSWORD, WELCOME, CMS, HCFA, SYSTEM, MEDICARE, MEDICAID, TEMP, LETMEIN, GOD, SEX, MONEY, QUEST, F20ASYA, RAVENS, REDSKIN, ORIOLES, BULLETS, CAPITOL, MARYLAND, TERPS, DOCTOR, 567890, 12345678, ROOT, BOSSMAN, JANUARY, FEBRUARY, MARCH, APRIL, MAY, JUNE, JULY, AUGUST, SEPTEMBER, OCTOBER, NOVEMBER, DECEMBER, SSA, FIREWALL, CITIC, ADMIN, UNISYS, PWD, SECURITY, 76543210, 43210, 098765, IRAQ, OIS, TMG, INTERNET, INTRANET, EXTRANET, ATT, LOCKHEED

8.1 Change Password

A user’s password can be changed from the **My Profile** screen. Follow the steps below to change the password:

1. Log in to IACS using the User ID and password.
2. On the **My Profile** screen, select the Change Password hyperlink.

3. To change your password, enter your Current password, a new password and re-enter the new password again to confirm the new password.
4. Select the ***Change Password*** button to complete the Change Password process.

   Note: Users will not be allowed to change the password more than once a day.

8.2 Change Password - Password Expiration

The user's password must be changed at least once every 60 days. When the user logs in after the password expiration, IACS will prompt the user to change his password by displaying the **Change Password** screen. Once the user changes the password successfully, the **My Profile** screen will be displayed.

Note: Should the user log in to any of the applications that he has access to with the expired password, the user will be redirected to the **CMS Portal** Page allowing him to change his password.

8.3 Forgot Your Password?

Follow the steps below to change the password from the **Login to IACS** screen:

1. On the **Login to IACS** screen, enter the User ID and then select the ***Forgot Your Password?*** button.
2. Enter the SSN and the E-mail address and select the ***Next*** button.
3. When prompted, answer the Authentication Questions and select the ***Next*** button.
4. On the **Change Password** screen, enter a new password.
5. Enter the new password again and select the ***Change Password*** button.
6. On the **Change Password Results** screen, select the ***OK*** button.

   Note: Users will not be allowed to change the password more than once a day.

8.4 Forgot Your User ID?

The user needs to follow the steps below to retrieve his User ID from the **Login to IACS** screen:

1. From the **Login to IACS** screen, select the ***Forgot Your User ID?*** button.
2. When prompted, enter the First Name, Last Name, Date of Birth, SSN, and E-mail.
3. The User ID will be sent to the E-mail on record.

Note: Refer to Section 7.1 for Login instructions.

Alternatively, the user can also use the **Account Management** screen to retrieve the User ID as follows:

1. Navigate to https://applications.cms.hhs.gov.
2. Select the Account Management hyperlink in the menu bar toward the top of the screen.

3. Select the Forgot your User ID? hyperlink.
4. When prompted, enter the First Name, Last Name, Date of Birth, SSN, and E-mail.

8.5 Re-Activate Account

CMS requires inactive accounts to be disabled. The account will be considered inactive if the user has not logged in to IACS for 60 days. The user's account will be disabled and the user will be unable to access any application. Below are the steps the user should take to re-activate the account:

1. Navigate to https://applications.cms.hhs.gov. Alternatively, users may navigate to http://www.cms.gov/iacs and select the link for My Profile.
2. Select the Account Management hyperlink in the center of the screen or in the menu bar toward the top of the screen.
3. Select the My Profile hyperlink on the **Account Management** screen.
4. Accept the Terms and Conditions.
5. Log in using the User ID and password.
6. When prompted, answer the Security Questions and Authentication Questions.
7. Change the password.

If the user is not prompted to answer the Security Questions and Authentication Questions, then he must contact the application Help Desk.

8.6 Locked Account

If the user has not been able to log in after three consecutive attempts, the IACS user account will be locked. The system will automatically unlock the user after 60 minutes.

If the user does not want to wait for the system to unlock the account, the user can use the ***Forgot your Password*?** feature. Once the user correctly responds to the Security Questions and Authentication Questions, the user will be prompted to create a new password.

The user can also contact the Help Desk for assistance. When the Help Desk unlocks the account, the user can log in with his current User ID and password. If the Help Desk unlocks and resets the user's password, IACS will send the user an initial password pattern. The user must log in to IACS with the User ID and the initial password pattern. The user will be prompted to change the password. Refer to Section 18.0 for additional Help Desk contact information.

9.0 Modify User/Contact Information

IACS provides the user with the option to modify user information and/or professional contact information provided during IACS registration. Use the Modify User/Contact Information hyperlink to update the following information:

- E-mail address (requires approval)
- Professional credentials

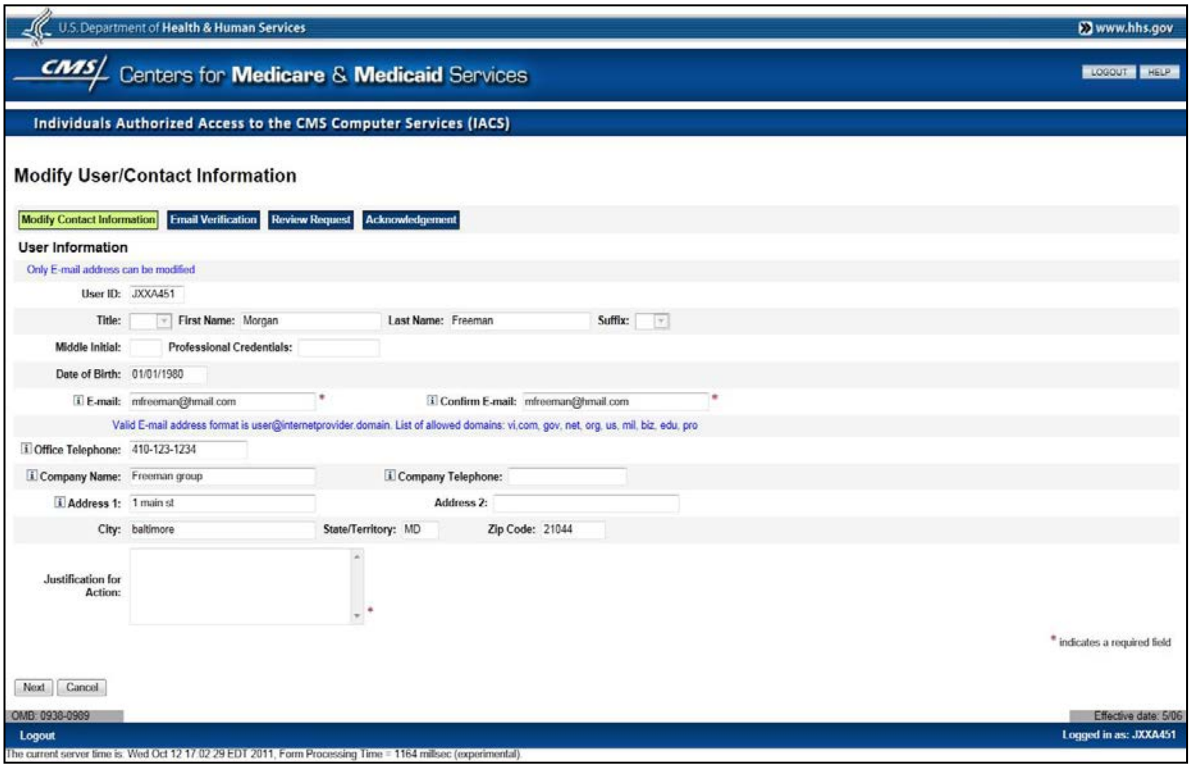
- Professional contact information, company name, address and phone numbers

Notes:

- Users will not be able to update their First Name, Last Name, SSN, and Date of Birth information using Modify User/Contact Information. Users will need to contact the Help Desk to update this information.
- MA/MA-PD/PDP/CC Application users will be allowed to modify only the E-mail address.
- The Modify User/Contact Information hyperlink will not be displayed for the following applications: COB, CSR, HETS UI, and HPG.
- Any applications not listed above will be allowed to modify the contact information and the E-mail address at the same time. All changes will take place once the request has been approved. If the E-mail change request has been rejected, none of the contact information requested changes will take place.

9.1 Modify User/Contact Information – Change E-mail

This section describes the change E-mail process. When the user selects the Modify User/Contact Information hyperlink, the **Modify User/Contact Information** screen will display, as illustrated in Figure 20.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
Modify Contact Information
Email Verification
Review Request
Acknowledgement
Next
Cancel
Logout

Modify User/Contact Information

User Information

Only E-mail address can be modified

User ID: JXXA451

Title: First Name: Morgan Last Name: Freeman Suffix:

Middle Initial: Professional Credentials:

Date of Birth: 01/01/1980

E-mail: mfreeman@hmail.com * Confirm E-mail: mfreeman@hmail.com *

Valid E-mail address format is user@internetprovider.domain. List of allowed domains: vi,com, gov, net, org, us, mil, biz, edu, pro

Office Telephone: 410-123-1234

Company Name: Freeman group Company Telephone:

Address 1: 1 main st Address 2:

City: baltimore State/Territory: MD Zip Code: 21044

Justification for Action: *

* indicates a required field

OMB: 0938-0989 Effective date: 5/06

Logged in as: JXXA451

The current server time is: Wed Oct 12 17:02:29 EDT 2011, Form Processing Time = 1164 millsec (experimental).

Figure 20: Modify User/Contact Information Screen

Action: Modify the E-mail address and other information on the **User Information** screen, as needed.

When the user enters an E-mail address and has selected another field, the screen will refresh. The C*onfirm E-mail* field will be displayed. The user must re-enter the E-mail address to confirm the change.

Action: Select the ***Next*** button after making changes.

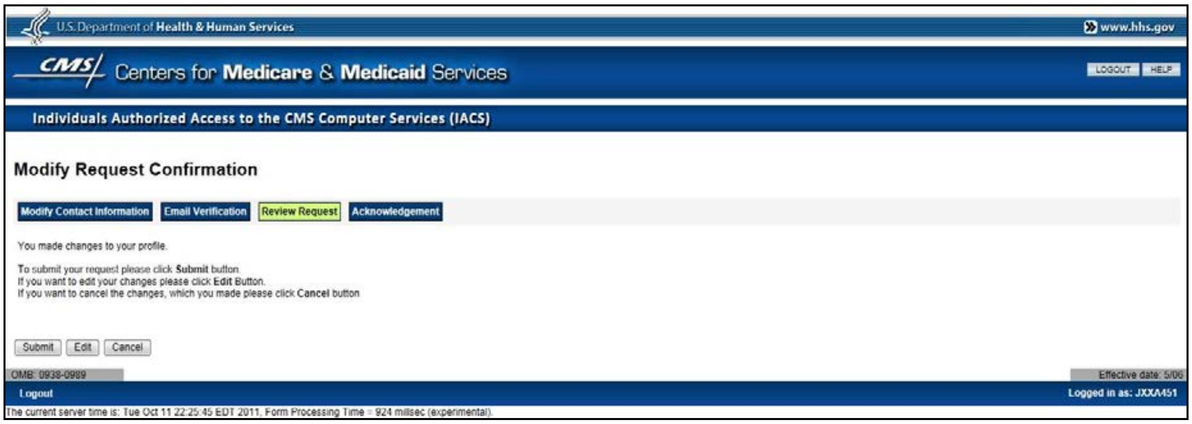
Note: If the ***Cancel*** button is selected during the modification process, no changes will be made and the user will be returned to the **My Profile** screen.

When the ***Next*** button is selected, the system validates the data that has been entered. The E-mail address is validated to verify that it does not already exist for another IACS account.

Once the E-mail information is successfully validated, the **E-mail Address Verification** screen will display, as illustrated in Figure 5. The user will be sent an E-mail that confirms IACS has received the user's request and provides him with a Verification Code. The user must enter the *Verification Code* on the **E-mail Address Verification** screen, within 30 minutes from the time the Verification Code is generated. For more information regarding the E-mail address verification process, review the process in Section 6.1.

When the user enters the correct verification code and selects the ***Next*** button on the **E-mail Address Verification** screen, the system will display the **Modify Request Confirmation** screen, as illustrated in Figure 21.

Note: If the user needs to make any changes to the modification request, he should use the ***Edit*** button.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
Modify Request Confirmation
Modify Contact Information
Email Verification
Review Request
Acknowledgement
Submit
Edit
Cancel
Logout

You made changes to your profile.

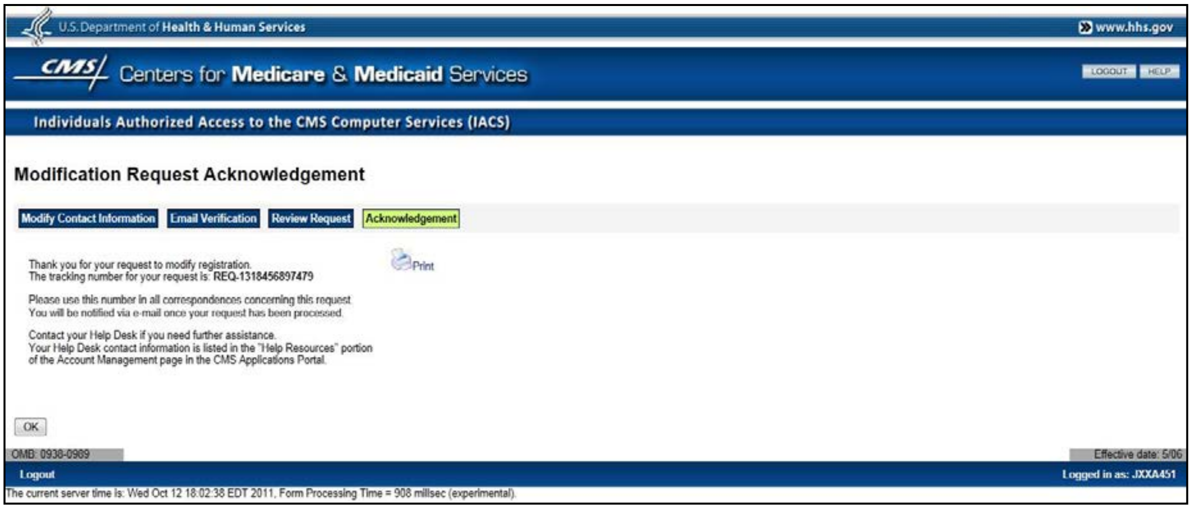
To submit your request please click **Submit** button.
If you want to edit your changes please click **Edit** Button.
If you want to cancel the changes, which you made please click **Cancel** button

OMB: 0938-0989
Effective date: 5/06
Logged in as: JXXA451
The current server time is: Tue Oct 11 22:25:45 EDT 2011, Form Processing Time = 924 millsec (experimental).

Figure 21: Modify Request Confirmation Screen

Action: Select the ***Submit*** button to submit the modification request.

When the user selects the **Submit** button, a **Modification Request Acknowledgement** screen will display, as illustrated in Figure 22.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
Modify Contact Information
Email Verification
Review Request
Acknowledgement
Print
OK
Logout

Modification Request Acknowledgement

Thank you for your request to modify registration.
The tracking number for your request is: **REQ-1318456897479**

Please use this number in all correspondences concerning this request
You will be notified via e-mail once your request has been processed.

Contact your Help Desk if you need further assistance.
Your Help Desk contact information is listed in the "Help Resources" portion of the Account Management page in the CMS Applications Portal.

OMB: 0938-0989

Effective date: 5/06

Logged in as: JXXA451

The current server time is: Wed Oct 12 18:02:38 EDT 2011, Form Processing Time = 908 millsec (experimental).

Figure 22: Modification Request Acknowledgement Screen

The **Modification Request Acknowledgement** screen indicates that the request has been successfully submitted and the request tracking number has been assigned. This tracking number should be recorded and used if there are any questions about the status of the request.

The information contained on the screen can be printed by selecting the ***Print*** icon.

Action: Select the ***OK*** button to complete the modification request.

Notes:

- Contact information that does not require approval will take effect once the ***OK*** button is selected.
- E-mail modification requests require approval. When contact information changes are made with an E-mail change request, the contact information does not get updated until the E-mail request has been approved. Should the modification request be rejected, none of the requested changes will be made to the user's contact information.

The **Modification Request Acknowledgement** screen will close and the system will return to the **My Profile** screen. This screen indicates that the change request has been successfully submitted.

The user will be sent an E-mail with a request tracking number confirming that IACS has received the request. If the confirmation E-mail notification is not received within 24 hours after the user modifies the profile, the user will need to contact the Help Desk. For Help Desk contact information, see Section 18.0.

10.0 Modify Account Profile

The following sections describe the **Modify Account Profile** feature and the most common actions available to modify a user’s profile. Depending on the application, an existing user can perform the following actions:

- View user’s access profile
- Add applications
- Add and remove contracts (MA/MA-PD/PDP/CC)
- Disassociate from the current role
- Add a role
- Modify report access (MA/MA-PD/PDP/CC)
- Modify profile, some common options are to associate and/or disassociate with other organizations within an application or modify specific application attributes
- Modify 2nd factor notification method (PQRS/eRx)

Note: A user cannot be their own approver, for example, IACS would not allow the same person to be the Approver and the End User for the same organization within the same application.

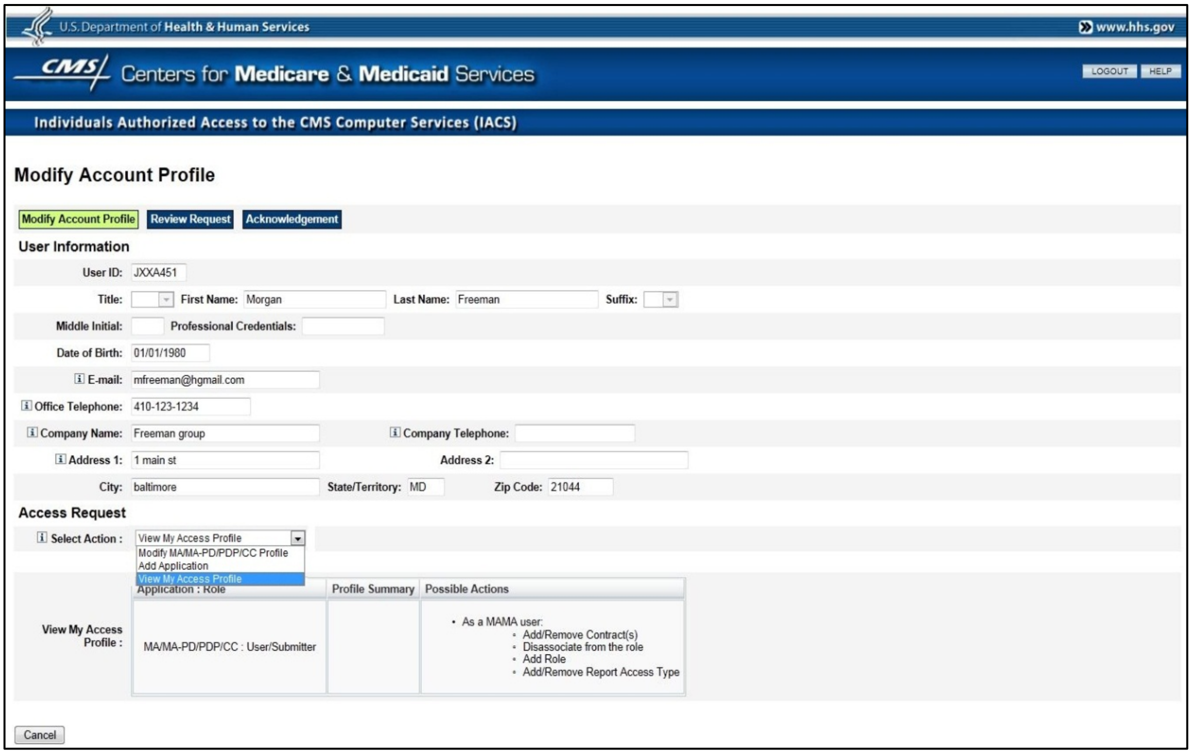
10.1 View User’s Access Profile

When the Modify Account Profile hyperlink is selected, the **Modify Account Profile** screen will display the information in the user’s account profile that is specific to his role(s) within the application(s).

At the top of the screen, the ***User Information*** section displays the user’s information.

In the ***Access Request*** area of this screen, the approved access information will be displayed in the ***View My Access Profile*** table, as illustrated in Figure 23. If the user has a role in more than one application, then each application will be displayed in a separate row in the table.

The *Select Action* field provides a drop-down list from which the user can select the desired action. The actions for this example are illustrated in Figure 23*.*


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
Modify Account Profile
Review Request
Acknowledgement
Cancel

Modify Account Profile

User Information

User ID:	JXXA451						
Title:		First Name:	Morgan	Last Name:	Freeman	Suffix:	
Middle Initial:		Professional Credentials:					
Date of Birth:	01/01/1980						
E-mail:	mfreeman@hgmail.com						
Office Telephone:	410-123-1234						
Company Name:	Freeman group	Company Telephone:					
Address 1:	1 main st	Address 2:					
City:	baltimore	State/Territory:	MD	Zip Code:	21044		

Access Request

Select Action : View My Access Profile

- Modify MA/MA-PD/PDP/CC Profile
- Add Application
- View My Access Profile

View My Access Profile :

Application : Role	Profile Summary	Possible Actions
MA/MA-PD/PDP/CC : User/Submitter		• As a MAMA user: ▪ Add/Remove Contract(s) ▪ Disassociate from the role ▪ Add Role ▪ Add/Remove Report Access Type

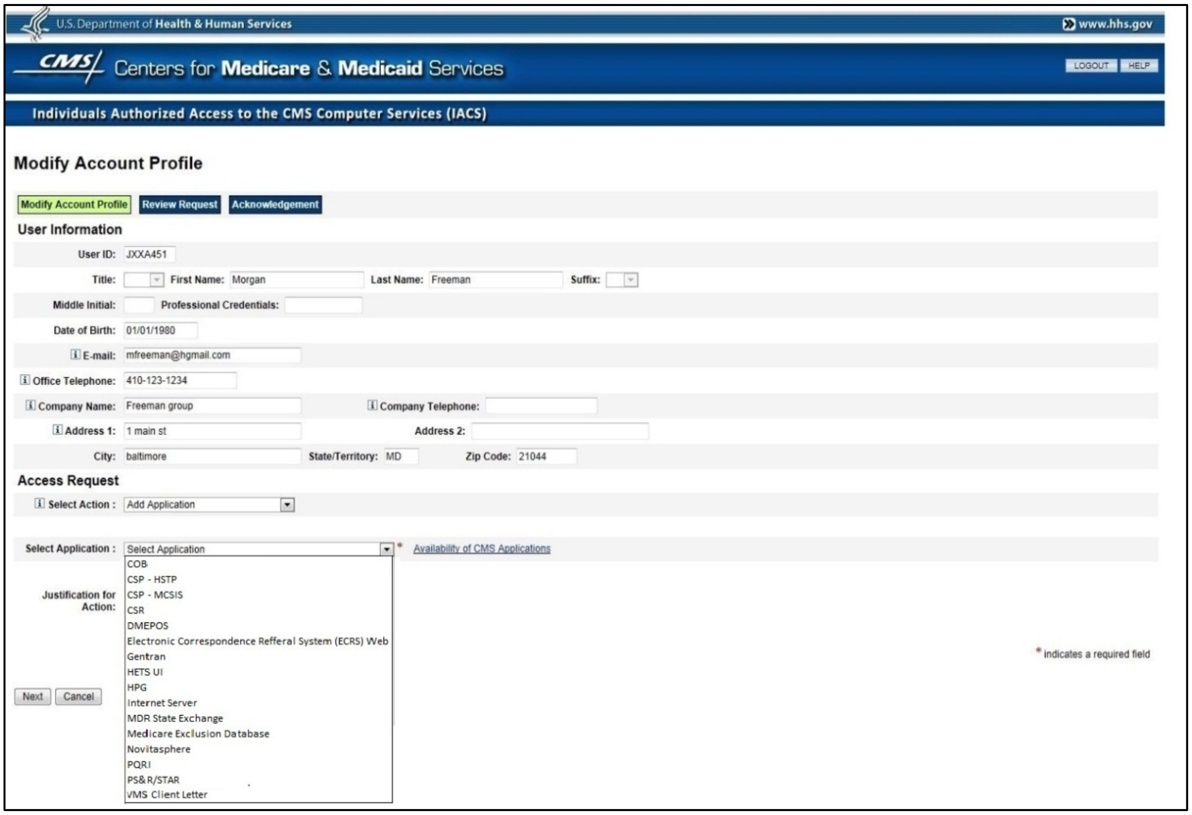
Figure 23: Modify Account Profile Screen: Access Request Area – Select Action Drop-Down List

10.2 Add Application

If the user selects the action ***Add Application***, the screen will refresh the ***Access Request*** section to allow the user to select an application. The ***Access Request*** section is similar to the one shown in Figure 24. The user will be able to add applications integrated with IACS that are contained in the *Select Application* drop-down list, as illustrated in Figure 24.

The following rules need to be followed when requesting access to roles in other applications:

- Depending on the application being selected, the user may request to have one or more roles for a CMS application.
- The user cannot be an Approver and a User for the same application.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
Modify Account Profile
Modify Account Profile
Review Request
Acknowledgement
User Information
Access Request
Availability of CMS Applications
COB
CSP - HSTP
CSP - MCSIS
CSR
DMEPOS
Electronic Correspondence Refferal System (ECRS) Web
Gentran
HETS UI
HPG
Internet Server
MDR State Exchange
Medicare Exclusion Database
Novitasphere
PQRI
PS&R/STAR
VMS Client Letter
Next
Cancel

User ID: JXXA451

Title: First Name: Morgan Last Name: Freeman Suffix:

Middle Initial: Professional Credentials:

Date of Birth: 01/01/1980

E-mail: mfreeman@hgmail.com

Office Telephone: 410-123-1234

Company Name: Freeman group Company Telephone:

Address 1: 1 main st Address 2:

City: baltimore State/Territory: MD Zip Code: 21044

Select Action : Add Application

Select Application : Select Application *

Justification for Action:

* indicates a required field

Figure 24: Modify Account Profile Screen: Access Request Area – Select Application Drop-Down List

Action: Select the desired application from the *Select Application* drop-down list.

Action: Select the role from the *Role* drop-down list.

Action: Enter a justification statement in the *Justification for Action* field. This field must include the reason for requesting this action.

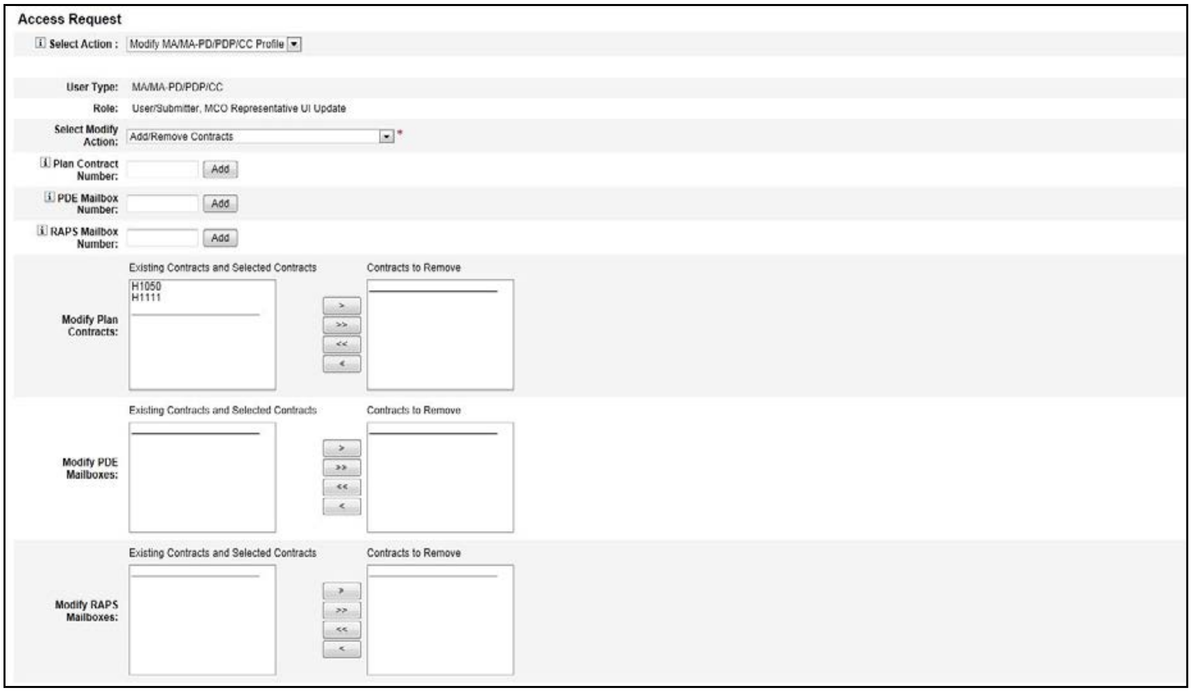
Action: Select the ***Next*** button after entering the justification statement.

The system will display the **Modify Request Confirmation** screen, as illustrated in Figure 21.

For further information on completing the **Modify Account Profile** process, follow the instructions included within Section 10.0.

10.3 MA/MA-PD/PDP/CC - Add and Remove Contracts

If the user selects the action ***Modify Profile***, then selects the option ***Add/Remove Contracts***, the screen will refresh to a screen in which the ***Access Request*** area is similar to the one shown in Figure 25.



Access Request

Select Action : Modify MA/MA-PD/PDP/CC Profile

User Type: MA/MA-PD/PDP/CC

Role: User/Submitter, MCO Representative UI Update

Select Modify Action: Add/Remove Contracts *

Plan Contract Number:

PDE Mailbox Number:

RAPS Mailbox Number:

Modify Plan Contracts: Existing Contracts and Selected Contracts: H1050, H1111 — Contracts to Remove:

Modify PDE Mailboxes: Existing Contracts and Selected Contracts — Contracts to Remove

Modify RAPS Mailboxes: Existing Contracts and Selected Contracts — Contracts to Remove

Figure 25: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC User/Submitter Add or Remove Contracts

If the user wants to add a contract number to his current list of contract numbers, then the user should follow these steps:

Action: Enter the contract number in the appropriate *Plan Contract Number, PDE Mailbox,* or *RAPS Mailbox* field.

Action: Select the applicable ***Add*** button.

The newly added contract will be displayed in the appropriate text box. Repeat the actions above to add another contract number.

If the user wants to remove a contract number from his current list of contract numbers, then the user should follow these steps:

Action: In the *Modify Plan Contracts* or *Modify RAPS Mailboxes* fields, select the items that need to be removed from the *Existing Contracts* or the *Selected Contracts* column.

Action: Select the **>** button to move the selected item to the *Contracts to Remove* column.

The direction buttons will move the selected items from one column to another. Select the button with the single arrow to move selected items from one column to the other. Select the button with the double arrow to move the complete list from one column to the other.

After making modifications, the user should do the following:

Action: Enter a justification statement in the *Justification for Action* field. This field must include the reason for requesting this action.

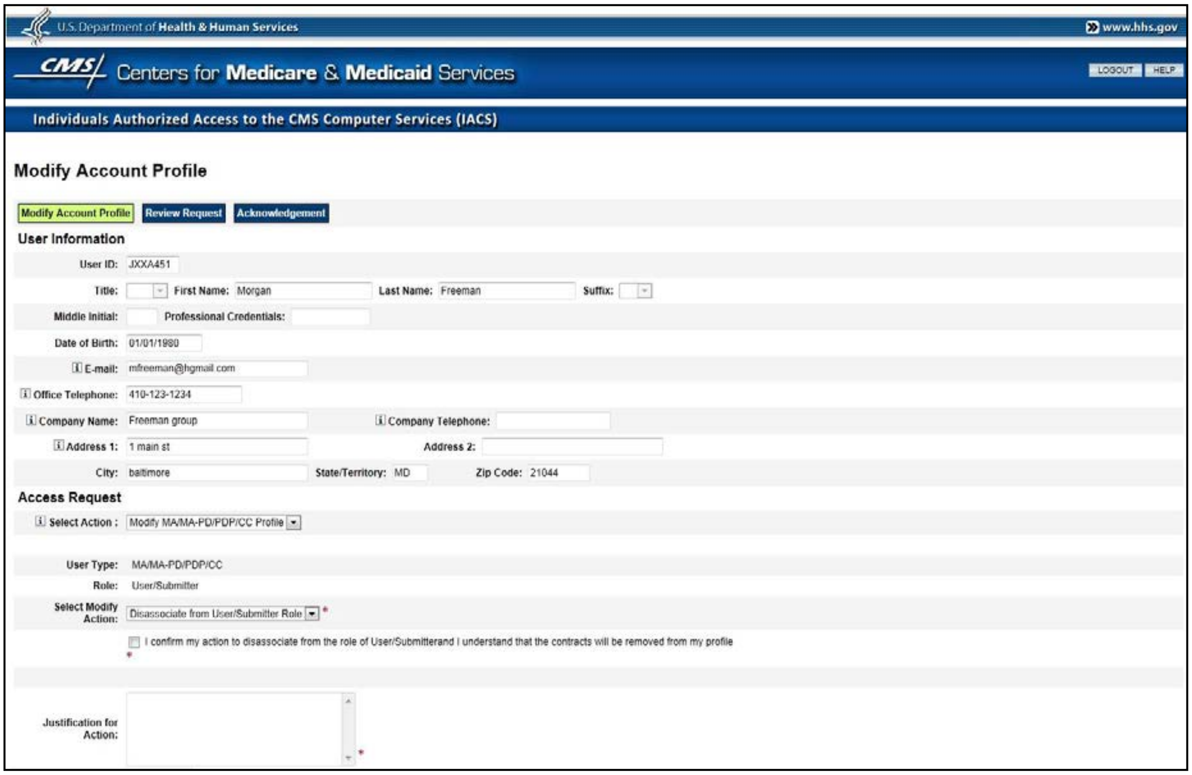
Action: Select the ***Next*** button after entering the justification statement.

The system will display the **Modify Request Confirmation** screen, as illustrated in Figure 21.

For further information on completing the **Modify Account Profile** process, follow the instructions included within Section 10.0.

10.4 Disassociate from Current Role

For applications that allow users to disassociate from a role, the *Select Action* drop-down list on the **Modify Account Profile** screen will contain the option to disassociate from that role. If the user selects this action, the screen will refresh and a confirmation message and check box will appear in the ***Access Request*** area, as illustrated in Figure 26.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
Modify Account Profile
Review Request
Acknowledgement

Modify Account Profile

User Information

User ID:	JXXA451						
Title:		First Name:	Morgan	Last Name:	Freeman	Suffix:	
Middle Initial:		Professional Credentials:					
Date of Birth:	01/01/1980						
E-mail:	mfreeman@hgmail com						
Office Telephone:	410-123-1234						
Company Name:	Freeman group			Company Telephone:			
Address 1:	1 main st			Address 2:			
City:	baltimore	State/Territory:	MD	Zip Code:	21044		

Access Request

Select Action : Modify MA/MA-PD/PDP/CC Profile

User Type: MA/MA-PD/PDP/CC

Role: User/Submitter

Select Modify Action: Disassociate from User/Submitter Role *

□ I confirm my action to disassociate from the role of User/Submitterand I understand that the contracts will be removed from my profile *

Justification for Action: *

Figure 26: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC User/Submitter Disassociate from Role

Notes:

- The message text will read, *"I confirm my action to disassociate from the role of < Role Name > and I understand that the < Contract Numbers> will be removed from my profile."*
- If the user has two MA/MA-PD/PDP/CC Application roles in his profile, the contracts in his profile will not be removed until he disassociates from both roles.

If the user decides to disassociate from his current role, then he should do the following:

Action: Select the Confirmation check box to confirm disassociation from the current role.

Action: Enter a justification statement for the request in the *Justification for Action* field. This field must include the reason for requesting this action.

Action: Select the ***Next*** button after entering the justification statement.

The system will display the **Modify Request Confirmation** screen, as illustrated in Figure 21.

For further information on completing the **Modify Account Profile** process, follow the instructions included within Section 10.0.

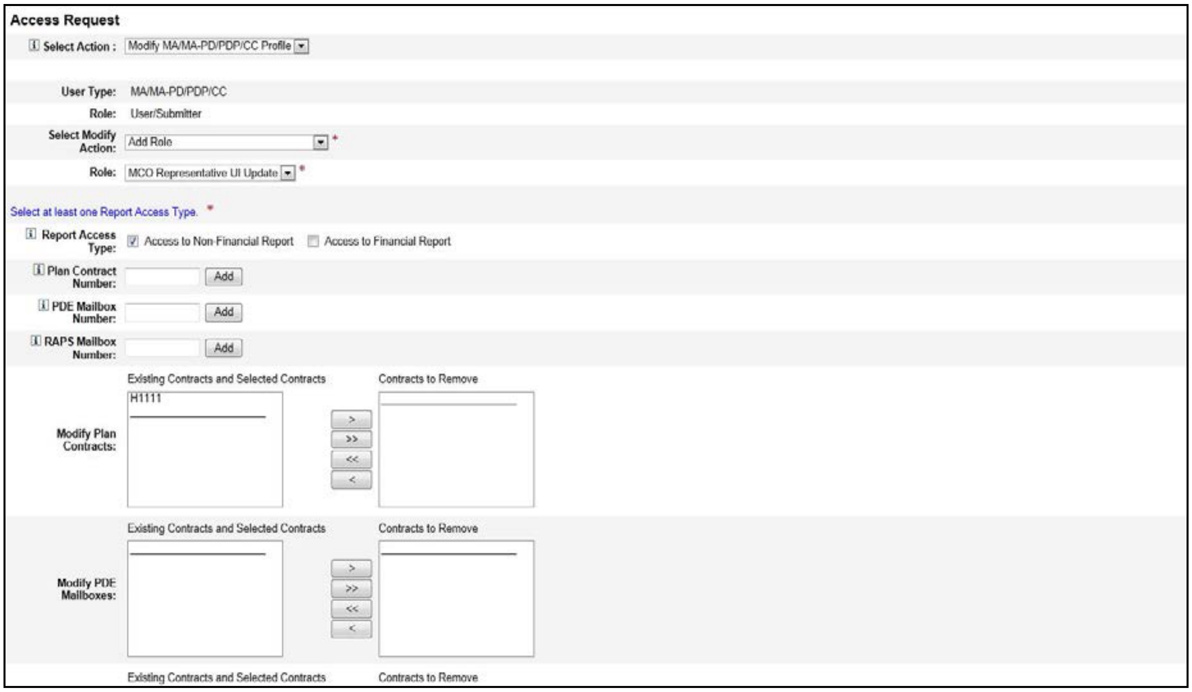
Notes:

- Users of following applications will not be able to disassociate from their current role: COB, CSR, HETS UI, and HPG.
- Authorizers, EPOCs and Approvers within the MA/MA-PD/PDP/CC Application will not be able to disassociate from their current role. Authorizers, EPOCs and Approvers will not be able to register for another MA/MA-PD/PDP/CC role until they disassociate from the current role. To disassociate from a role, a Service Request (SR) must be submitted to IACS Administration to remove the role from the user's account. A role can only be removed for an EPOC without any contracts. Therefore, the EPOC, should first use the **Modify Account Profile** feature to remove all contracts and then submit the SR. Refer to Frequently Asked Questions, Question 30 for further information.
- A MA/MA-PD/PDP/CC user who has a pending modification for add role, add contract, or modify report access type will not be allowed to disassociate from that role. IACS will display a message informing the user that the modification request is pending and the user will not be allowed to disassociate from that role.

10.5 Add Role

If the user selects the action ***Modify Profile,*** then selects the option *Add Role*, the screen will refresh and the ***Access Request*** area will include the following items, as illustrated in Figure 27.

- *Role* drop-down list: User can select a role from the role dropdown
- *Report Access Type* check boxes: User can modify the selection of access to non-financial and financial reports
- Contract selection fields: User can Add/Remove contracts



Access Request

Select Action : Modify MA/MA-PD/PDP/CC Profile

User Type: MA/MA-PD/PDP/CC

Role: User/Submitter

Select Modify Action: Add Role *

Role: MCO Representative UI Update *

Select at least one Report Access Type. *

Report Access Type: ☑ Access to Non-Financial Report ☐ Access to Financial Report

Plan Contract Number:

PDE Mailbox Number:

RAPS Mailbox Number:

Modify Plan Contracts:

Existing Contracts and Selected Contracts	Contracts to Remove
H1111	

Modify PDE Mailboxes:

Existing Contracts and Selected Contracts	Contracts to Remove

Existing Contracts and Selected Contracts Contracts to Remove

Figure 27: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC Add Role

Action: Select the available role from the *Role* drop-down list.

> **Note:** If the user has two roles existing in his profile, then the *Add Role* option will not be displayed in the *Select Modify Action* drop-down list.

Action: Modify the *Report Access Type* selection, if needed**.**

Action: Add contracts or mailboxes, as needed. Enter data into the appropriate fields and select the ***Add*** button.

Action: Remove contracts or mailboxes, as needed. Select data from the *Existing Contracts and Selected Contracts* column, then select the **>** or **>>** button to move the data to the *Contract to Remove* column. Refer to Section 10.3 for further information.

After making modifications, the user should do the following:

Action: Enter a justification statement for the request in the *Justification for Action* field. This field must include the reason for requesting this action.

Action: Select the ***Next*** button.

The system will display the **Modify Request Confirmation** screen, as illustrated in Figure 21.

For further information on completing the **Modify Account Profile** process, follow the instructions included within Section 10.0.

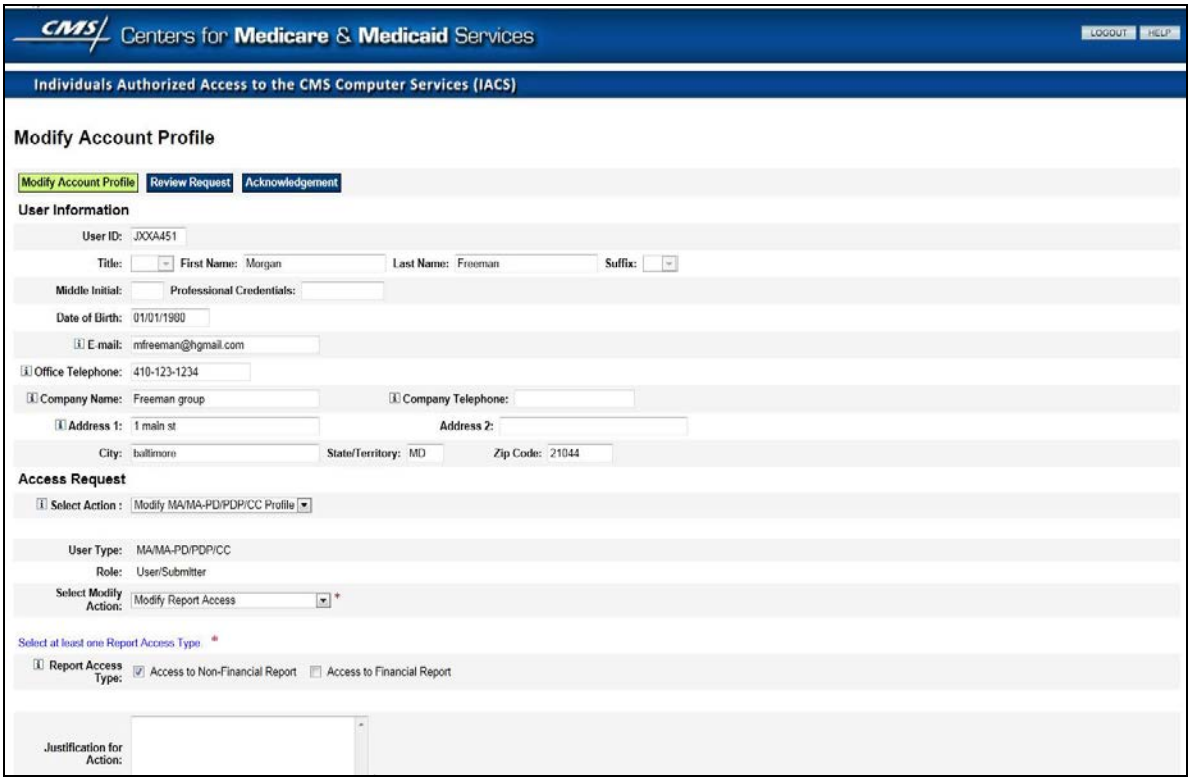
Notes:

- Users for the following applications will not be able to add a role within the same application: COB, HETS UI.
- Only the MA/MA-PD/PDP/CC roles listed in Table 1 will be able to request an additional role within the application**.**
- All PQRS/eRx Users will be able to request a new role within the PQRS/eRx Application for an organization that is different from their current organization.
- The PQRS/eRx User will be able to request one or more of the following roles within an organization:
  - EHR Submitter
  - End User
  - PQRS Submitter
  - PQRS Representative
- The PS&R/STAR User will be able to request one or more of the following roles within an FI/Carrier/MAC organization. The roles will be assigned upon appropriate approval.
  - PS&R User
  - PS&R Admin
  - STAR User 1 – STAR User 8
- The PS&R/STAR User will be able to request one or more of the following roles within a Provider organization. The roles will be assigned upon appropriate approval.
  - PS&R User
  - PS&R Admin
- The PS&R/STAR System Maintainer will be able to request one or more roles. The roles will be assigned upon appropriate approval.
  - PS&R User
  - PS&R Admin
  - STAR User 1 – STAR User 8

10.6 Modify Report Access

The ***Modify Report Access*** action is available to the MA/MA-PD/PDP/CC users as referenced in Table 1.

If the user selects the action ***Modify Profile,*** then selects the option *Modify Report Access,* the screen will refresh and the *Report Access Type* check boxes will be displayed, as illustrated in Figure 28.


CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
Modify Account Profile
Review Request
Acknowledgement

Modify Account Profile

User Information

User ID: JXXA451

Title: First Name: Morgan Last Name: Freeman Suffix:

Middle Initial: Professional Credentials:

Date of Birth: 01/01/1980

E-mail: mfreeman@hgmail.com

Office Telephone: 410-123-1234

Company Name: Freeman group Company Telephone:

Address 1: 1 main st Address 2:

City: baltimore State/Territory: MD Zip Code: 21044

Access Request

Select Action : Modify MA/MA-PD/PDP/CC Profile

User Type: MA/MA-PD/PDP/CC

Role: User/Submitter

Select Modify Action: Modify Report Access *

Select at least one Report Access Type *

Report Access Type: ☑ Access to Non-Financial Report □ Access to Financial Report

Justification for Action:

Figure 28: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC Modify Report Access

Action: Select the desired *Report Access Type*.

Note: At least one *Report Access Type* should be selected.

After making modifications, the user should do the following:

Action: Enter a justification statement for the request in the *Justification for Action* field. This field must include the reason for requesting this action.

Action: Select the ***Next*** button.

The system will display the **Modify Request Confirmation** screen, as illustrated in Figure 21.

For further information on completing the **Modify Account Profile** process, follow the instructions included within Section 10.0.

10.7 Modify Account Profile – Other Application Modifications

MA/MA-PD/PDP/CC

- The **Modify Account Profile** feature does not have an option to change the State/Territory for Access attribute. If a user has the MA State/Territory User, SHIP End User, or SPAP End User role and needs to change the *State/Territory for Access* assignment, he can do this in two steps by using the **Modify Account Profile** option. First, the user will need to disassociate from the current role(s). Then, the user will need to use the *Add Role* option to select the appropriate roles and *State/Territory for Access*.
- Only the user with the roles listed in Table 1 can request an additional role within the MA/MA-PD/PDP/CC Application.
- **Modify Report Access** option will not be applicable for MA/MA-PD/PDP/CC users who do not have access to Gentran mailboxes.

HPG

- Submitter ID can only be modified by the IACS Administrators using the IACS Admin Console. The MCARE Help Desk will have to open an IACS Trouble Ticket requesting the IACS Administrator to modify the HPG User's Submitter ID.

PQRS/eRx

- A user registered as a Security Official may modify his NPI, PTAN, and organization details except for the organization TIN/SSN and the Legal Business Name.
- A user registered for the following roles will be able to modify his current selection of 2nd factor passcode notification method using the drop-down list, labeled as *Preferred 2nd Factor Notification Method*:
    - EHR Submitter
    - HIE User
    - PQRS Submitter User
    - Individual Practitioner with 2-Factor Authentication
- The *2nd Factor Notification Method* options are:
    - Email
    - SMS / Mobile (Text message)
    - Interactive Voice Response Number (IVR)
- A user registered as a Security Official or a Backup Security Official will be able to modify his current selection of 2-Factor Authentication Approver role.
- A user registered as an Individual Practitioner will have the option to modify his current selection of 2-Factor Authentication role.

PS&R/STAR

- A user registered as a PS&R Security Official or PS&R/STAR Security Official may modify his organization details except for the organization TIN/SSN and the Legal Business Name.
- A user registered as a PS&R Security Official may modify *CMS Certification Numbers* (CCN) associated with his organization.

11.0 Completing the Annual Certification to Keep Your IACS Account Active

Users registered through IACS for CMS applications are required to annually certify their continued need for access to CMS systems. IACS enforces the Annual Certification requirement for all applications supported by IACS.

The certification due date corresponds to the anniversary of the User's IACS User ID creation date. The certification process is initiated with an E-mail notification to the user providing him with instructions for completing the certification.

11.1 E-mail Notifications

A user will receive an advisory E-mail 45 days prior to his Annual Certification due date. The user will continue to receive E-mails once a week from the initial 45 day E-mail until 15 days prior to his Certification Date. Then, beginning 15 days before his Certification Date, the user will receive an E-mail every day informing him of how many days he has remaining to complete the Certification Request.

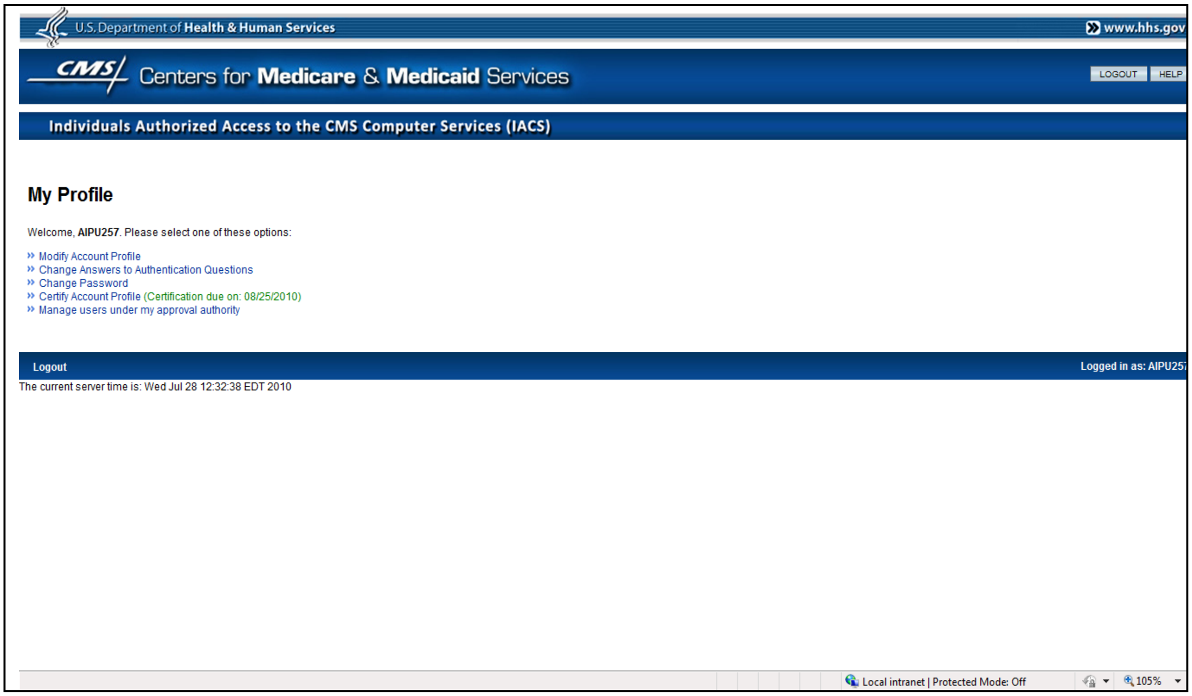
If the Certification Request is not submitted prior to midnight on the Certification Date, his IACS account will be archived. An E-mail will be sent informing the user that his account has been archived. Should he attempt to login to IACS after being archived, a message will appear that the account could not be found.

The Annual Certification actions for a user with no assigned roles will be slightly different. The E-mail notification will advise the user of the situation and provide instructions on how to submit the request to add a role in order to maintain the account. The modification request will need to be approved before the user can submit the Annual Certification request. Should the user take no action, the account will be archived after the certification due date.

Note: Once the user's account has been archived, he will be required to go through New User Registration to establish a new account.

11.2 Certify Account Profile

The **My Profile** screen will have a Certify Account Profile hyperlink as shown in Figure 29. When the user selects this hyperlink, he will be presented with the **Terms and Conditions**. After accepting the **Terms and Conditions**, the User will continue with the Annual Certification process.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

My Profile

Welcome, **AIPU257**. Please select one of these options:

- Modify Account Profile
- Change Answers to Authentication Questions
- Change Password
- Certify Account Profile (Certification due on: 08/25/2010)
- Manage users under my approval authority

Logout
Logged in as: AIPU257

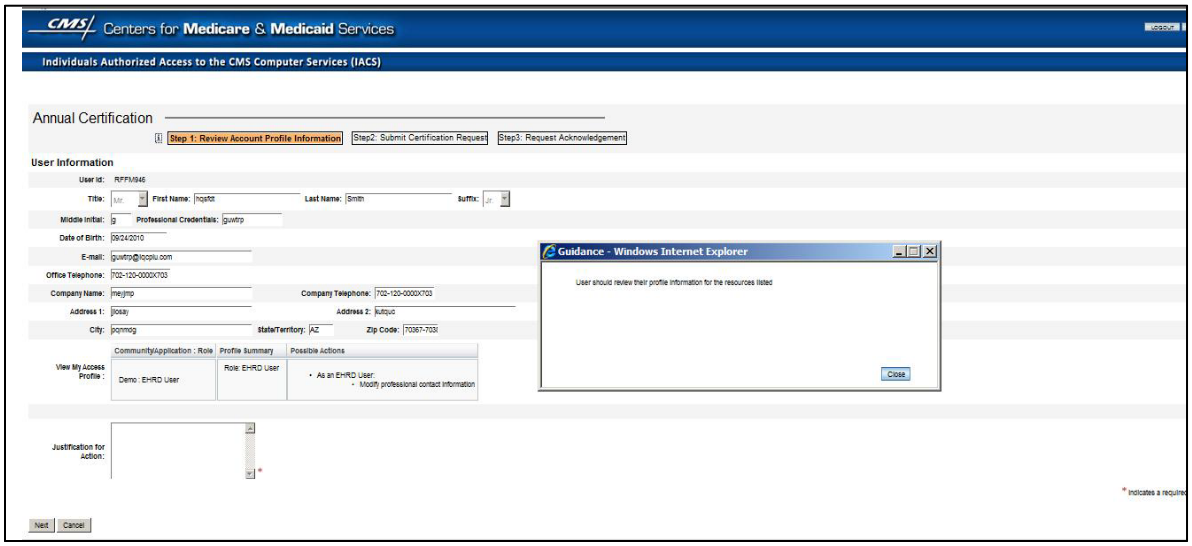
The current server time is: Wed Jul 28 12:32:38 EDT 2010

Local intranet | Protected Mode: Off
105%

Figure 29: My Profile Screen: Certify Account Profile Hyperlink

The Annual Certification process will be a three-step process**.**

Step 1: Review Account Profile Information screen will display showing the user’s profile, as illustrated in Figure 30.



CMS Centers for Medicare & Medicaid Services
LOGOUT
Individuals Authorized Access to the CMS Computer Services (IACS)

Annual Certification

Step 1: Review Account Profile Information | Step2: Submit Certification Request | Step3: Request Acknowledgement

User Information

User Id: RFFM946

Title: Mr. First Name: hqsfdt Last Name: Smith Suffix: Jr.

Middle Initial: g Professional Credentials: guwtrp

Date of Birth: 09/24/2010

E-mail: guwtrp@lqcplu.com

Office Telephone: 702-120-0000X703

Company Name: meyjmp Company Telephone: 702-120-0000X703

Address 1: jlosay Address 2: kutquc

City: pqnmdg State/Territory: AZ Zip Code: 70367-703

View My Access Profile :

Community/Application : Role	Profile Summary	Possible Actions
Demo : EHRD User	Role: EHRD User	• As an EHRD User: • Modify professional contact information

Justification for Action: *

Guidance - Windows Internet Explorer

User should review their profile information for the resources listed

* Indicates a required

Figure 30: Annual Certification: Review Account Profile Screen

Action: Review and select the ***Next*** button to certify.

When the user selects the ***Next*** button, the system will display the **Annual Certification - Step 2: Submit Certification Request** screen.

Note: If a user has no roles, contracts, call centers or required attributes for the application assigned to the account, IACS will display a message at the top of the screen describing the problem and the action to take to maintain the account. Should the user take no action, the account will be archived. The user must select the ***Cancel*** button to return to the **My Profile** screen.

Action: Select the ***Submit*** button on the **Annual Certification - Step 2: Submit Certification Request** screen to submit the request for re-certification.

The system will display the **Annual Certification - Step 3: Certification Request Acknowledgement** screen.

The **Annual Certification - Step 3: Certification Request Acknowledgement** screen indicates that the certification request has been successfully submitted and the request tracking number has been assigned.

Action: Select the ***OK*** button on **the Annual Certification – Step 3: Certification Request Acknowledgement** screen.

The **Annual Certification – Step 3: Certification Request Acknowledgement** screen will close and the system will return to the **My Profile** screen. The user will be sent an E-mail confirming that IACS has received his certification request.

When the user submits the Certification Request, it is routed to appropriate Approvers or EPOCs. If multiple approvals are required, the request will be routed to all corresponding approvers. The user's Approver(s) will have a minimum of 30 days to approve his request for Annual Certification. During that time, the user's Approver will receive reminder E-mails as described above. If the user's Annual Certification date is reached (or a minimum of 30 days after submission, whichever is later) and the Approver has taken no action, it will be treated the same as a rejected request and the user's account will be archived.

12.0 Approve Pending Request

This section describes how an Approver reviews and takes action on an IACS request requiring the Approver's attention. The following are the actions that an Approver may take:

- Approve/Reject/Defer requests for New User Registration and/or modifying existing user profiles.
- Search Pending Requests for New User Registration, Modify Profile, and/or Annual Certification.
- Approve/Reject/Defer requests for Annual Certification.

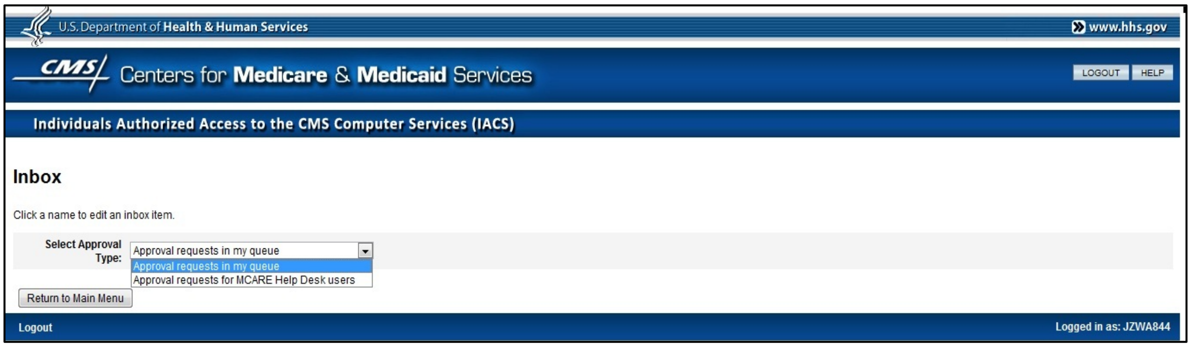
Approval hierarchy for an application is determined by the needs of the business. An application may elect to have the Help Desk role approve certain Approver or End User roles. Refer to Appendix A for the listing of applications and the role approval hierarchy.

12.1 Pending Approvals

To take an action on pending access requests, the user must first log in to IACS using his IACS User ID and password. The **My Profile** screen will display after a successful login, as illustrated in Figure 37.

Action: Select the Pending Approvals hyperlink on the **My Profile** screen.

Some applications have a common or shared Inbox accessed by all the Helpdesk users of the application to process pending requests. The Inbox selection screen will display, as illustrated in Figure 31. The Helpdesk user will select the appropriate Inbox from the approval type drop-down list. After the Helpdesk user has approved or rejected the request, the request will be removed from the shared Inbox.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Inbox

Click a name to edit an inbox item.

Select Approval Type: Approval requests in my queue

- Approval requests in my queue
- Approval requests for MCARE Help Desk users

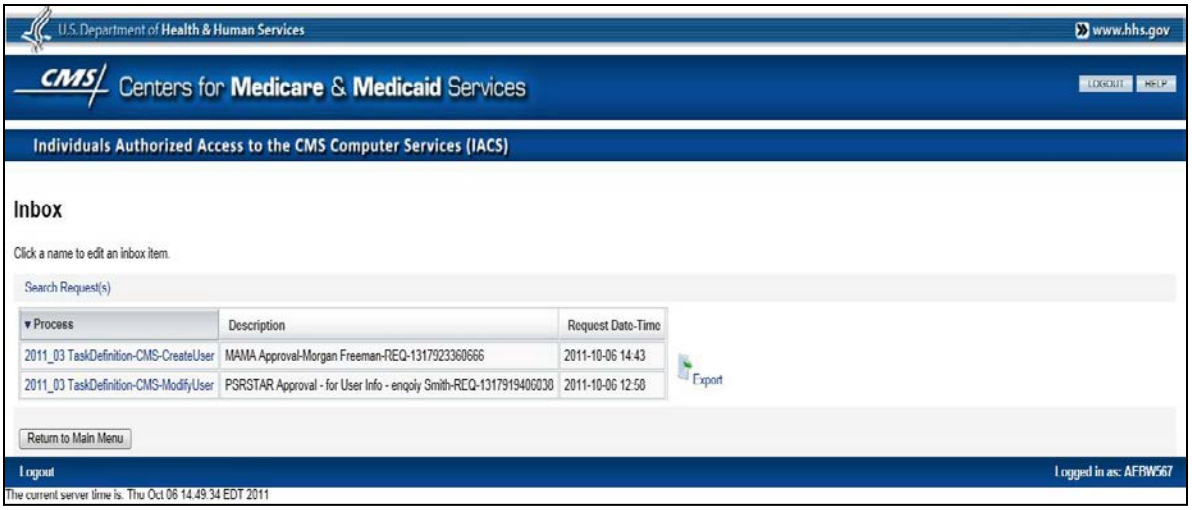
Return to Main Menu
Logout

Logged in as: JZWA844

Figure 31: Inbox Selection

Action: Select the appropriate *Select Approval Type* to access the **Inbox** screen.

The Approver's **Inbox** screen will display, as illustrated in Figure 32. The pending approval requests for New User Registration and account profile modification will be displayed as hyperlinks in a table, as illustrated in Figure 31. The Approver can also search for requests by selecting the Search Request hyperlink. Section 12.1.2 provides details on the search function.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Inbox

Click a name to edit an inbox item.

Search Request(s)

▾ Process	Description	Request Date-Time
2011_03 TaskDefinition-CMS-CreateUser	MAMA Approval-Morgan Freeman-REQ-1317923360666	2011-10-06 14:43
2011_03 TaskDefinition-CMS-ModifyUser	PSRSTAR Approval - for User Info - enqoiy Smith-REQ-1317919406038	2011-10-06 12:58

Export
Return to Main Menu
Logout

Logged in as: AFRW567

The current server time is: Thu Oct 06 14.49.34 EDT 2011

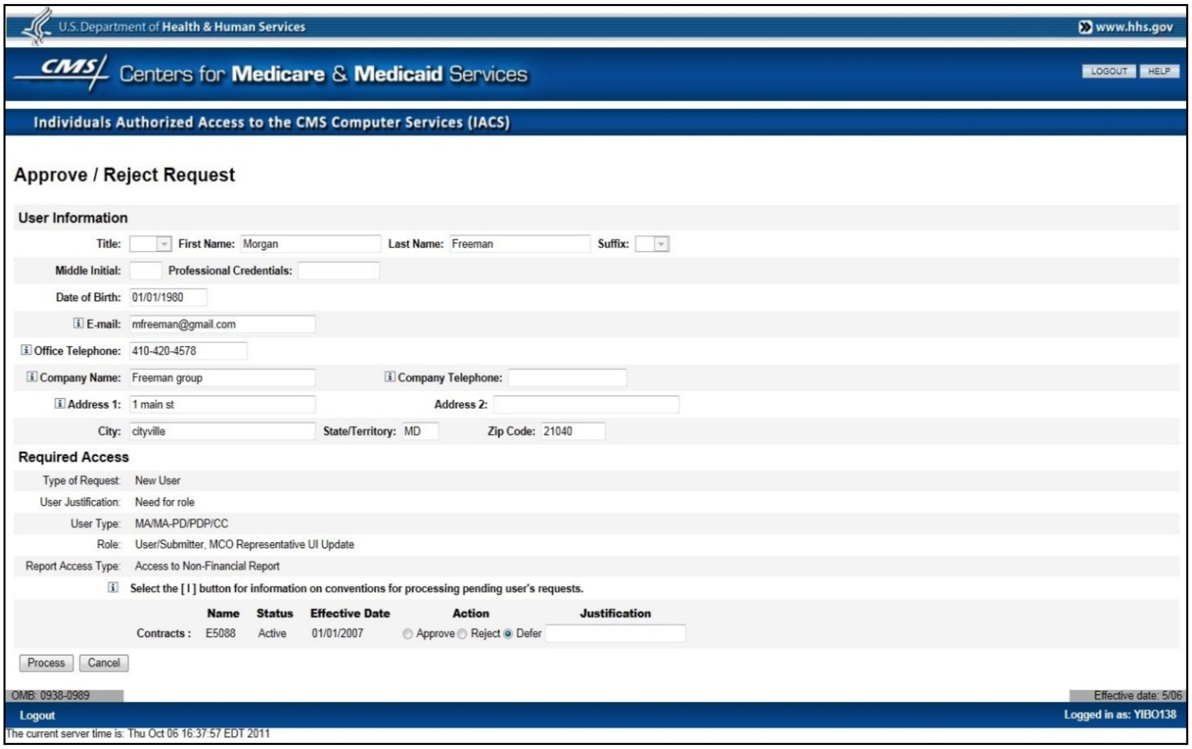
Figure 32: Approver Inbox Screen

Action: Select the hyperlink of the pending approval request to work on from the *Process* column.

> **Note:** The MA/MA-PD/PDP/CC Application screens will be used to illustrate the search function and other Approver functions. Approvers for the PQRS/eRx Application should refer to Section 12.1.1 for additional information.

When the Approver has selected the *Pending Approval* request to work on, the **Approve / Reject Request** screen will display, as illustrated in Figure 33.

The ***User Information*** and ***Required Access*** areas of the screen will display information specific to the user and his access request. At the bottom of the screen, the type of request is identified and the contracts to be approved for access are displayed. The *Action* column defaults to the *Defer* radio button for all individual items in the request.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Approve / Reject Request

User Information

Title: Suffix:
First Name: Morgan
Last Name: Freeman
Middle Initial:
Professional Credentials:
Date of Birth: 01/01/1980
E-mail: mfreeman@gmail.com
Office Telephone: 410-420-4578
Company Name: Freeman group
Company Telephone:
Address 1: 1 main st
Address 2:
City: cityville
State/Territory: MD
Zip Code: 21040

Required Access

Type of Request: New User
User Justification: Need for role
User Type: MA/MA-PD/PDP/CC
Role: User/Submitter, MCO Representative UI Update
Report Access Type: Access to Non-Financial Report

Select the [I] button for information on conventions for processing pending user's requests.

	Name	Status	Effective Date	Action	Justification
Contracts :	E5088	Active	01/01/2007	○ Approve ○ Reject ● Defer	

OMB: 0938-0989
Effective date: 5/06
Logged in as: YIBO138
The current server time is: Thu Oct 06 16:37:57 EDT 2011

Figure 33: Approve/Reject Request Screen: Required Access Area – Grouped Pending Items

Action: Review the requestor's ***User Information*** and ***Required Access*** section.

Action: Determine the action to be taken for each individual item.

> **Note:** The Approver's action (Approve / Reject / Defer) taken on the individual item (*Contracts*) will be applicable to all the MA/MA-PD/PDP/CC Application roles in the user's profile.

Action: Select the appropriate *Action* radio button for each item.

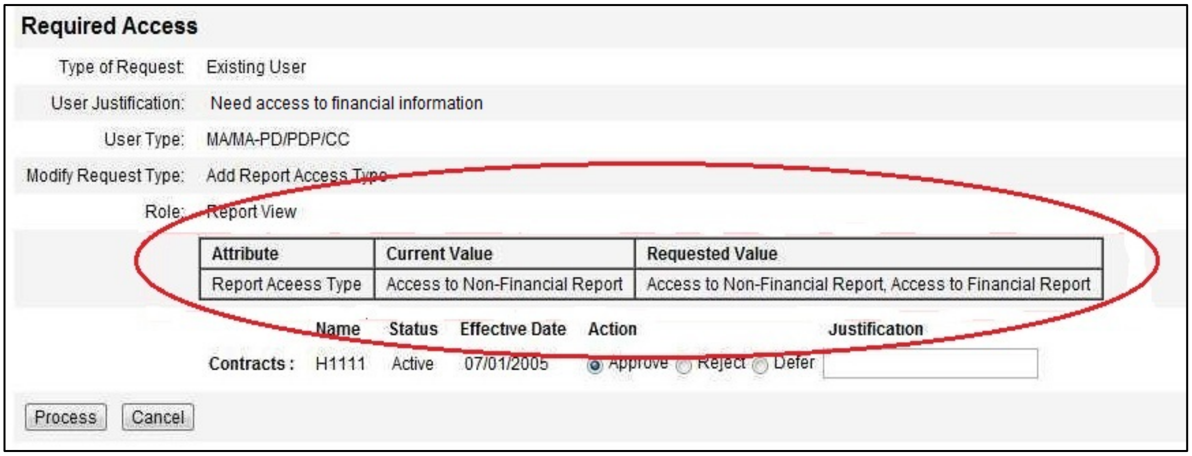
- If you select ***Approve***, the system will assign the default text 'Approved' as the justification. You may overwrite this if necessary.

- If you select ***Reject***, you must provide a justification reason. The justification you enter will be forwarded to the user in a rejection E-mail notification.

- If you select ***Defer***, no justification is required and the request will remain in pending status until it is approved or rejected by an authorized Approver or until it expires.

Note: The Approver has 12 days from the request date to approve / reject the request. After 12 days, the request will expire and the user will be required to re-submit his request. The timeout frame for the requests differs from one application to another; refer to Appendix B for the request timeout days by role type.

Note: For modification requests that require approval, the ***Requested Access*** section will display the attributes to be modified, with the current value and the requested value. Figure 34 illustrates a user's request to modify the *Report Access Type*. The user's current access type, Access to Non-Financial Report, is shown in the *Current Value* column. The user has requested access to Non-Financial and Financial Reports, as shown in the *Requested Value* column.



Required Access

Type of Request: Existing User

User Justification: Need access to financial information

User Type: MA/MA-PD/PDP/CC

Modify Request Type: Add Report Access Type

Role: Report View

Attribute	Current Value	Requested Value
Report Aceess Type	Access to Non-Financial Report	Access to Non-Financial Report, Access to Financial Report

	Name	Status	Effective Date	Action	Justification
Contracts :	H1111	Active	07/01/2005	● Approve ○ Reject ○ Defer	

Figure 34: Modification Request Required Access Section

Action: Select the ***Process*** button at the bottom of the screen when you are done.

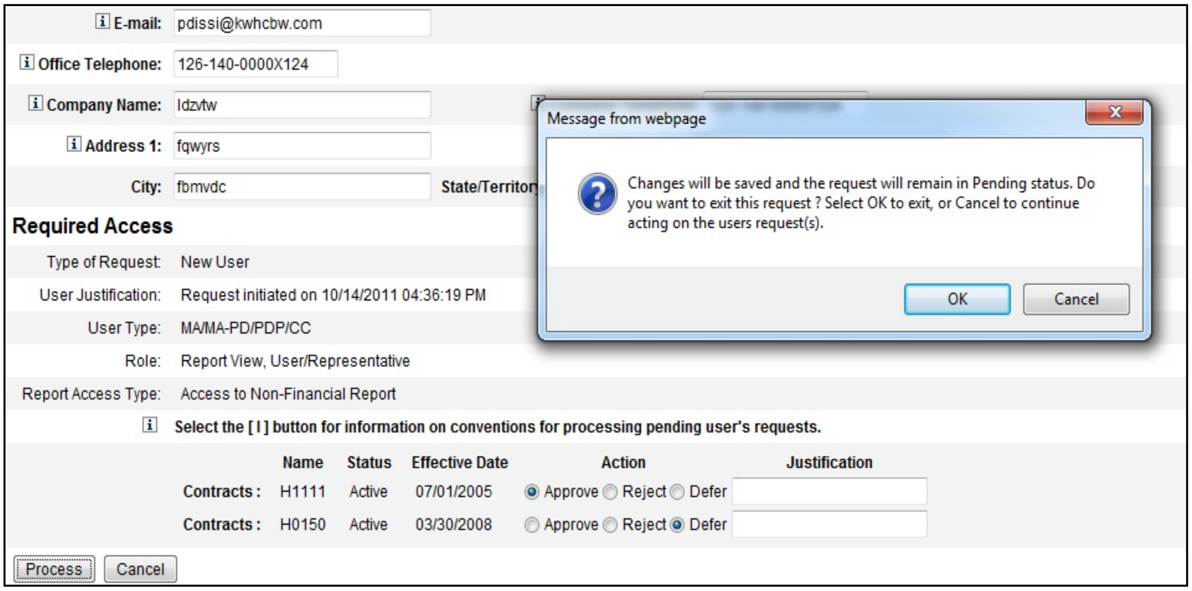
Note: If the ***Cancel*** button is selected at any point during the approval process, a warning message will be displayed to confirm the action. The user selects the ***OK*** button to cancel the request and return to the **Inbox** screen or ***Cancel*** to continue with the approval process.

When the user selects the ***Process*** button, the system will verify the action that has been taken for the items in the pending request.

If the user approves or rejects all items, IACS will:

1. Return to the **Inbox** screen if the user has additional pending approvals awaiting his action, or
2. Return to the **My Profile** screen if the user has no more pending approvals awaiting his action, or
3. Return to the **Search criteria for pending request(s)** screen if the pending request was selected from **the Search criteria for pending request(s)** screen.

If the user defers one or more items while approving or rejecting the other items in the request, IACS will display the message illustrated in Figure 35.



E-mail:	pdissi@kwhcbw.com
Office Telephone:	126-140-0000X124
Company Name:	Idzvtw
Address 1:	fqwyrs
City:	fbmvdc

State/Territor

Message from webpage

Changes will be saved and the request will remain in Pending status. Do you want to exit this request ? Select OK to exit, or Cancel to continue acting on the users request(s).

OK Cancel

Required Access

Type of Request:	New User
User Justification:	Request initiated on 10/14/2011 04:36:19 PM
User Type:	MA/MA-PD/PDP/CC
Role:	Report View, User/Representative
Report Access Type:	Access to Non-Financial Report

Select the [I] button for information on conventions for processing pending user's requests.

	Name	Status	Effective Date	Action	Justification
Contracts :	H1111	Active	07/01/2005	● Approve ○ Reject ○ Defer	
Contracts :	H0150	Active	03/30/2008	○ Approve ○ Reject ● Defer	

Process Cancel

Figure 35: Confirm Action Dialogue box with Deferred Items

Action: When this message appears, read the text in the dialogue box and determine the correct action.

Action: Select the ***OK*** button to confirm your action.

Action: Select the ***Cancel*** button to remain on the **Approve / Reject Request** screen.

When the user selects the ***OK*** button, IACS will:

1. Return to the **Inbox** screen if the user has additional pending approvals awaiting his action, or
2. Return to the **My Profile** screen if the user has no more pending approvals awaiting his action.

Note: If there is more than one Approver associated with the request, then the pending request will be routed to all corresponding Approvers.

12.1.1 PQRS/eRx PECOS Verification

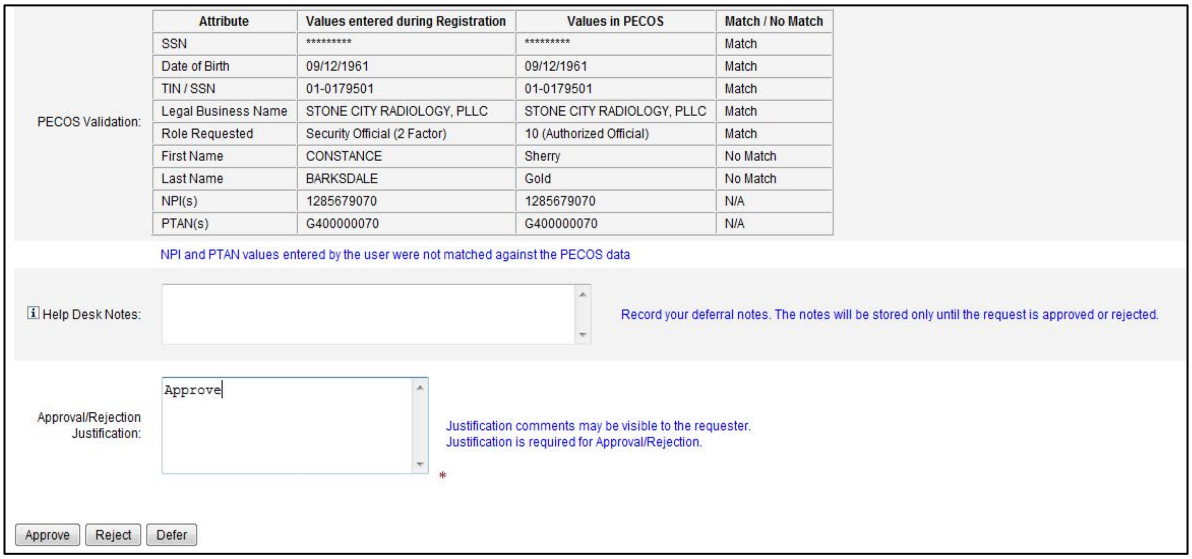
This section describes the **Approve / Reject Request** screen for those registering for the following roles:

- Security Official (SO)
- Backup Security Official (BSO)
- PQRS Submitter not associated with an organization
- PQRS Representative not associated with an organization

The **Approve / Reject Request** screen will display the values provided by the requestor, the values in PECOS, and the results *Match* or *No Match*.

The **Approve / Reject Request** screen with the validation table will be displayed, as illustrated in Figure 36. This figure represents the Security Official (SO) and Backup Security Official (BSO) approval. The validation table will display the values and the comparison results for *TIN/SSN, Date of Birth, Legal Business Name, Role Requested, First Name,* and *Last Name*. The *NPI(s)* and *PTAN(s)* will be displayed, but not matched.

The **Approve / Reject Request** screen for the PQRS Submitter and PQRS Representative approval will display the values and the comparison results for *TIN/SSN*, *Date of Birth*, *First Name, Last Name, NPI(s),* and *PTAN(s).*



PECOS Validation:

Attribute	Values entered during Registration	Values in PECOS	Match / No Match
SSN	*********	*********	Match
Date of Birth	09/12/1961	09/12/1961	Match
TIN / SSN	01-0179501	01-0179501	Match
Legal Business Name	STONE CITY RADIOLOGY, PLLC	STONE CITY RADIOLOGY, PLLC	Match
Role Requested	Security Official (2 Factor)	10 (Authorized Official)	Match
First Name	CONSTANCE	Sherry	No Match
Last Name	BARKSDALE	Gold	No Match
NPI(s)	1285679070	1285679070	N/A
PTAN(s)	G400000070	G400000070	N/A

NPI and PTAN values entered by the user were not matched against the PECOS data

Help Desk Notes:

Record your deferral notes. The notes will be stored only until the request is approved or rejected.

Approval/Rejection Justification: Approve

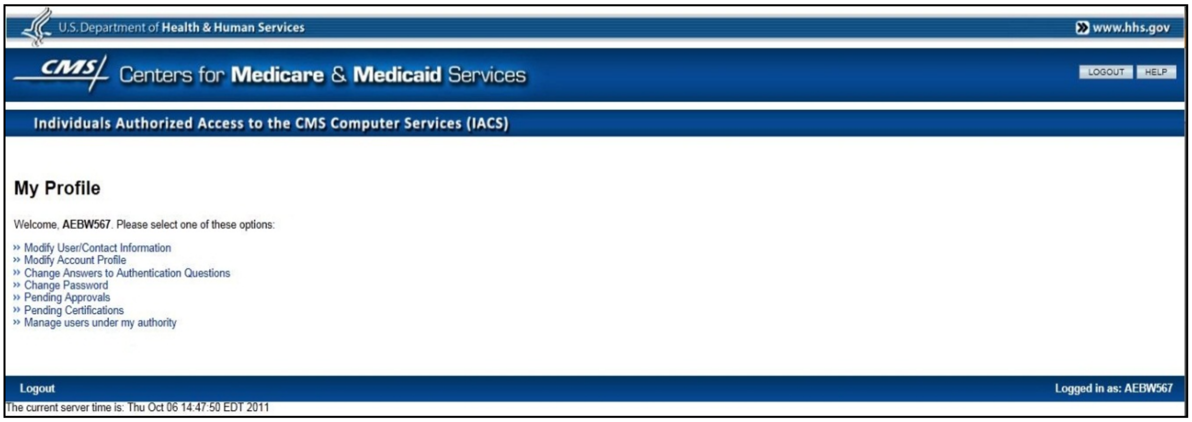
Justification comments may be visible to the requester.
Justification is required for Approval/Rejection.

Figure 36: Approve / Reject Request Screen with PECOS Validation

Note: The PQRI Helpdesk will be able to record notes in the *Help Desk Notes* field during the approval process. The notes will be viewable and editable by all PQRI Helpdesk users while the request is pending action. Once the request is approved or rejected, the request will be removed from the queue along with the notes. The *Help Desk Notes* field will be associated with the request and accepts up to 1,000 characters.

12.1.2 Search Pending Requests

This section details the **Search Request** function used to search for a specific request by providing the search criteria.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

My Profile

Welcome, **AEBW567**. Please select one of these options:

- » Modify User/Contact Information
- » Modify Account Profile
- » Change Answers to Authentication Questions
- » Change Password
- » Pending Approvals
- » Pending Certifications
- » Manage users under my authority

Logout

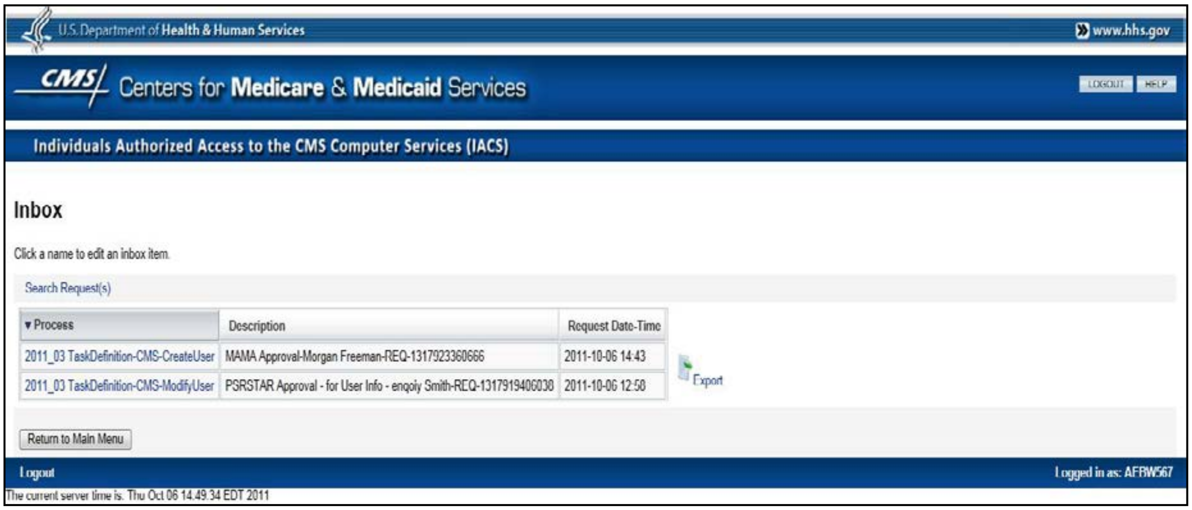
Logged in as: AEBW567

The current server time is: Thu Oct 06 14:47:50 EDT 2011

Figure 37: My Profile Screen

Action: Select the Pending Approvals hyperlink on the **My Profile** screen.

The Approver's **Inbox** screen will display, as illustrated in Figure 38. The **Inbox** screen allows the user to search for pending requests by selecting the Search Request(s) hyperlink or selecting the pending request from the Inbox table.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
Export
Return to Main Menu

Inbox

Click a name to edit an inbox item.

Search Request(s)

▾ Process	Description	Request Date-Time
2011_03 TaskDefinition-CMS-CreateUser	MAMA Approval-Morgan Freeman-REQ-1317923360666	2011-10-06 14:43
2011_03 TaskDefinition-CMS-ModifyUser	PSRSTAR Approval - for User Info - enqoiy Smith-REQ-1317919406038	2011-10-06 12:58

Logout

Logged in as: AEBW567

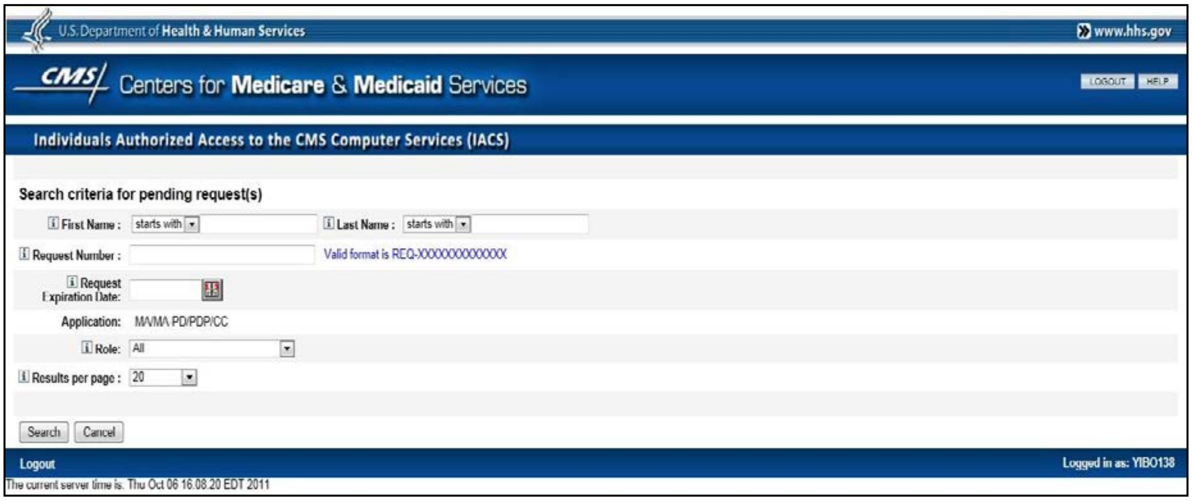
The current server time is. Thu Oct 06 14.49.34 EDT 2011

Figure 38: Approver Inbox Screen: Search Request(s) Hyperlink

Action: Select the Search Request(s) hyperlink.

The **Search criteria for pending request(s)** screen with multiple search criteria options will display, as illustrated in Figure 39.

Note: This function is currently only available for the Bundled Payments EFT, CMS Administration – Physician Value, CPC, CSP-HSTP, CSP-MCSIS, ECRS, esMD, Gentran, Internet Server, MACPro, MA/MA-PD/PDP/CC, MED, MDR, MyCGS, Novitasphere, PS&R/STAR, PV/PQRS Registration System, The SPOT, and VMS Client Letter applications.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Search criteria for pending request(s)

First Name : starts with ▾ Last Name : starts with ▾

Request Number : Valid format is REQ-XXXXXXXXXXXXX

Request Expiration Date:

Application: MA/MA PD/PDP/CC

Role: All ▾

Results per page : 20 ▾

Logged in as: YIBO138

The current server time is: Thu Oct 06 16.08.20 EDT 2011

Figure 39: Search Criteria for Pending Request(s) Screen

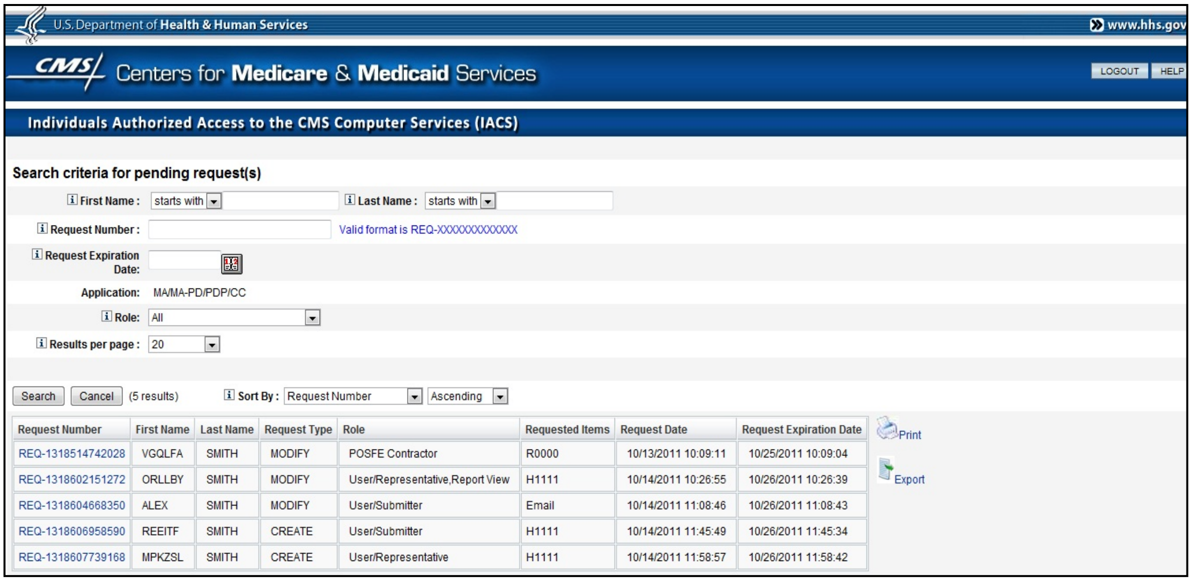
Action: Select the desired search criteria by entering the appropriate data in the search fields or selecting from the available drop-down lists.

Notes:

- Approvers can search pending requests by First Name, Last Name, Request Number, Request Expiration Date, and Role.
- In addition to the search criteria mentioned above, PS&R/STAR Helpdesks can search the pending registration request(s) by *TIN/SSN* and/or *Legal Business Name* of the organization. The *Legal Business Name* field will accept a partial entry of the organization name. The *TIN/SSN* field requires the data to be entered in full.

Action: Select the ***Search*** button to execute the search.

The screen will refresh and the search results will display at the bottom of the screen, as illustrated in Figure 40.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Search criteria for pending request(s)

First Name :	starts with
Last Name :	starts with
Request Number :	Valid format is REQ-XXXXXXXXXXXXX
Request Expiration Date:	
Application:	MA/MA-PD/PDP/CC
Role:	All
Results per page :	20

Search Cancel (5 results) Sort By : Request Number Ascending

Request Number	First Name	Last Name	Request Type	Role	Requested Items	Request Date	Request Expiration Date
REQ-1318514742028	VGQLFA	SMITH	MODIFY	POSFE Contractor	R0000	10/13/2011 10:09:11	10/25/2011 10:09:04
REQ-1318602151272	ORLLBY	SMITH	MODIFY	User/Representative,Report View	H1111	10/14/2011 10:26:55	10/26/2011 10:26:39
REQ-1318604668350	ALEX	SMITH	MODIFY	User/Submitter	Email	10/14/2011 11:08:46	10/26/2011 11:08:43
REQ-1318606958590	REEITF	SMITH	CREATE	User/Submitter	H1111	10/14/2011 11:45:49	10/26/2011 11:45:34
REQ-1318607739168	MPKZSL	SMITH	CREATE	User/Representative	H1111	10/14/2011 11:58:57	10/26/2011 11:58:42

Figure 40: Search Criteria for Pending Request(s) Screen: Search Results

Action: Select the hyperlink of the pending approval request to work on from the *Request Number* column.

When the Approver has selected a Pending Approval request to work on, the **Approve / Reject Request** screen will display which will allow the Approver to make a decision on the pending request. The approval process is explained in detail in Section 12.1.

Note: The Approvers of Bundled Payments EFT, CMS Administration – Physician Value, CPC, CSP-HSTP, CSP-MCSIS, ECRS, esMD, Gentran, Internet Server, MACPro, MA/MA-PD/PDP/CC, MED, MDR, MyCGS, Novitasphere, PS&R/STAR, PV/PQRS Registration System, The SPOT, and VMS Client Letter applications can also search for Pending Certification Requests by selecting the Pending Certifications hyperlink from the **My Profile** screen and selecting the Search Request(s) hyperlink from the Approver **Inbox** screen as explained above.

12.2 Search and View (Only) Pending Approvals

The Search and View (only) Pending Approvals hyperlink is available to the PQRI Help Desk, PS&R/STAR Help Desk, and MCARE Help Desk to search pending requests by the request tracking number.

Enter the complete request number in the *Enter Tracking Number* field and select the ***Search*** button. The Helpdesk can only view the request.

12.3 Annual Certification Approval

12.3.1 Approver E-mail Notifications

An Approver will receive an E-mail informing him that a user under his authority has submitted a request for certification and the request is awaiting his review. This E-mail will be sent to the

Approver as soon as the user (under the Approver's authority) has submitted the request for re-certification.

The Approver will receive a reminder E-mail 5 days after the submission of the request for re-certification and then every day thereafter until the day the certification request is approved or rejected by the Approver or until the certification request expires. Approvers will always have at least 30 days to approve or reject a certification request.

The Authorizer will receive a notification E-mail when an Approver under his authority fails to perform the annual certification. E-mails will be sent to the Authorizers 14 days, 7 days, and one day before the certification due date unless the Approver submits the certification. This E-mail is sent to Authorizers when an Approver has dependent users under their authority.

12.3.2 Approve/Reject/Defer Requests for Annual Certification

The Approver will be able to approve, reject, or defer a pending request for IACS Annual Certification.

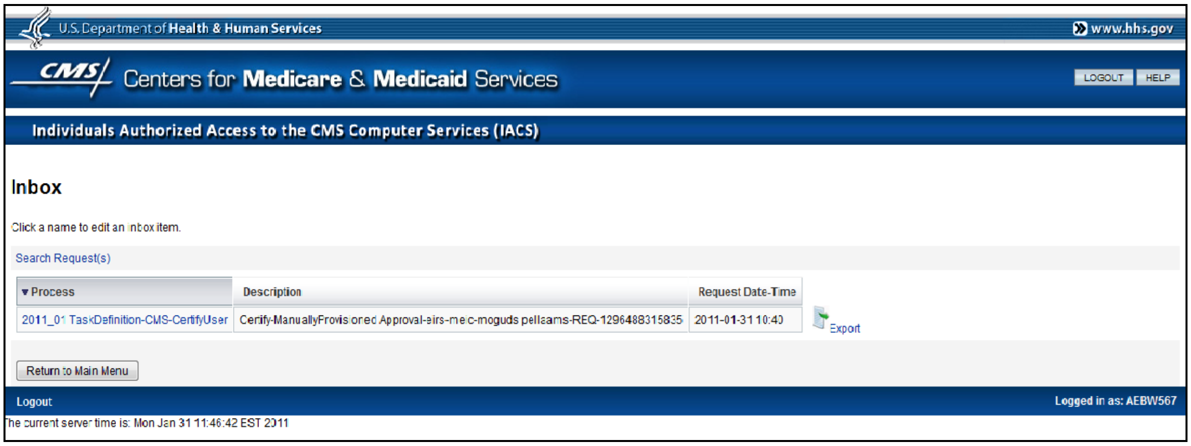
When the user submits the Certification Request, it is routed to the appropriate Approvers or EPOCs, or all of them, if his request requires multiple Approvers. The user's Approvers will have a minimum of 30 days to approve his request for Annual Certification. During that time, the user's Approver will receive reminder E-mails as described in Section 12.3.1.

The Certification Request from Helpdesk Users or Authorizers (Top of the Chain users) will be sent to the corresponding Business Owners who will open a Service Request (SR) to IACS Administration. The Service Request will provide the IACS Administrator with the approval/rejection decision of the Business Owner for the Top of the Chain users' certification request.

To take action on pending Certification Requests, the Approver must first log in to IACS using his IACS User ID and password. After a successful login, the **My Profile** screen will be displayed, as illustrated in Figure 37.

Action: Select the Pending Certifications hyperlink.

The Approver **Inbox** screen will display. The Approver's pending certification items will be displayed as hyperlinks in a table, as illustrated in Figure 41.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP

Individuals Authorized Access to the CMS Computer Services (IACS)

Inbox

Click a name to edit an inbox item.

Search Request(s)

▾ Process	Description	Request Date-Time
2011_01 TaskDefinition-CMS-CertifyUser	Certify-ManuallyProvisioned Approval-eirs-meic-moguds pellaams-REQ-1296488315835	2011-01-31 10:40

Export
Return to Main Menu
Logout

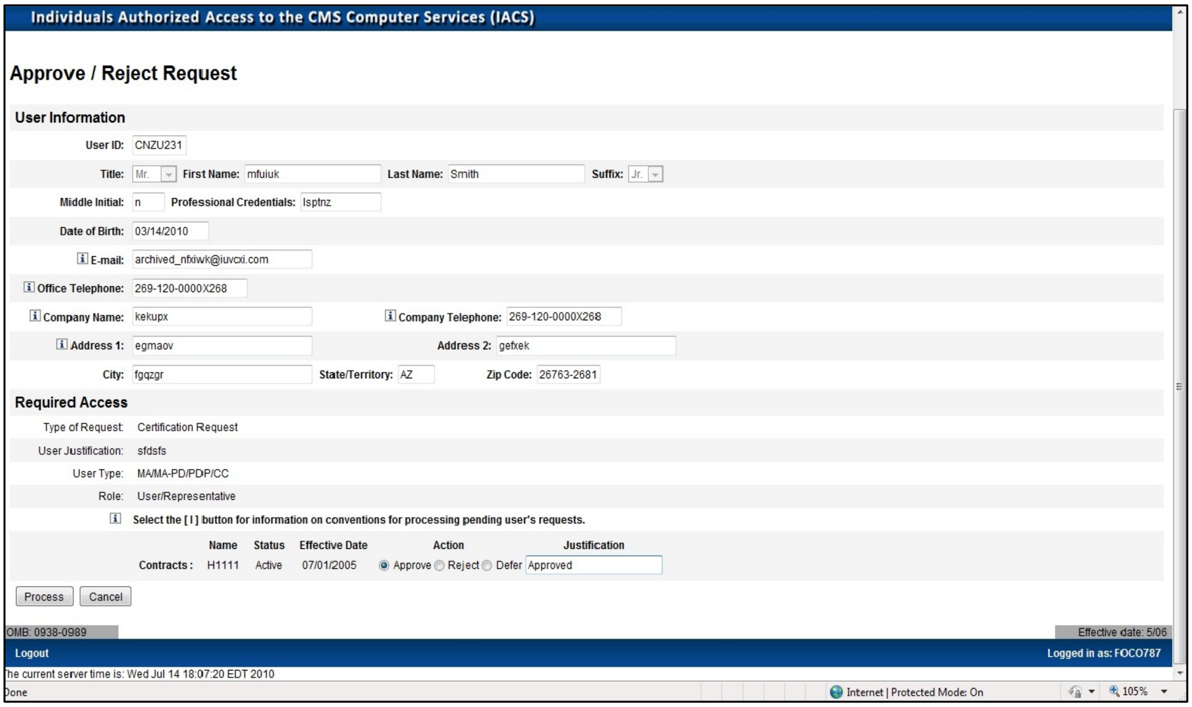
Logged in as: AEBW567

The current server time is: Mon Jan 31 11:46:42 EST 2011

Figure 41: Inbox Listing Pending Certification

Action: Select the hyperlink of the pending certification item to work on, as listed in the *Process* column**.**

The **Approve / Reject Request** screen will display, as shown below in Figure 42.


Individuals Authorized Access to the CMS Computer Services (IACS)

Approve / Reject Request

User Information

User ID:	CNZU231						
Title:	Mr.	First Name:	mfuiuk	Last Name:	Smith	Suffix:	Jr.
Middle Initial:	n	Professional Credentials:	lsptnz				
Date of Birth:	03/14/2010						
E-mail:	archived_nfxiwk@iuvcxi.com						
Office Telephone:	269-120-0000X268						
Company Name:	kekupx	Company Telephone:	269-120-0000X268				
Address 1:	egmaov	Address 2:	gefxek				
City:	fgqzgr	State/Territory:	AZ	Zip Code:	26763-2681		

Required Access

Type of Request:	Certification Request
User Justification:	sfdsfs
User Type:	MA/MA-PD/PDP/CC
Role:	User/Representative

Select the [I] button for information on conventions for processing pending user's requests.

	Name	Status	Effective Date	Action	Justification
Contracts :	H1111	Active	07/01/2005	● Approve ○ Reject ○ Defer	Approved

OMB: 0938-0989

Effective date: 5/06

Logged in as: FOCO787

The current server time is: Wed Jul 14 18:07:20 EDT 2010

Figure 42: Approve / Reject Request Screen: Certification Request

Action: Review the requestor's information.

Action: Select *Approve*, *Reject* or *Defer* from the *Action* column and enter a justification statement in the *Justification* field.

Action: When finished, select the ***Process*** button at the bottom of the screen.

Note: If the user's Annual Certification date is reached (or a minimum of 30 days after submission, whichever is later), and the Approver has taken no action, it will be treated as a rejected request.

13.0 Managing Users Under My Authority

13.1 Authorized Official, Security Official, EPOC – Search and Manage Users

The **Manage users under my authority** feature allows the Authorized Official (AO), Security Official (SO), External Point of Contact (EPOC), and Helpdesk users with approval capability to view users under their scope of responsibility. The **Manage users under my authority** screen allows the user to select the various search criteria to search the users under their authority. After the user selects the ***Search*** button, the records matching the search criteria will display. The ***Edit*** button will display for the applications and roles listed in Table 3.

Application	Role	Search and View Users under their authority	Edit
COB	COB Approver	COB User	Remove Organization
CSR	Authorizer, Approver	Approver, CSR User	Remove Call Centers
HPG	MCARE Help Desk	HPG User	Remove Submitter ID
MA/MA-PD/PDP/CC	Authorizer	EPOC	Remove Contract
MA/MA-PD/PDP/CC	EPOC	MA Submitter, MA Representative, PDP Submitter, PDP Representative, MMP User, NET Submitter, NET Representative, MCO Representative UI Update, Report View, POSFE Contractor	Remove Contract
PQRS/eRx	Security Official	End User, Backup Security Officials	Disassociate User
PS&R/STAR	Security Official	End User, Backup Security Officials	Disassociate User

Table 3: Manage Users Under My Authority - Roles with Edit Capabilities

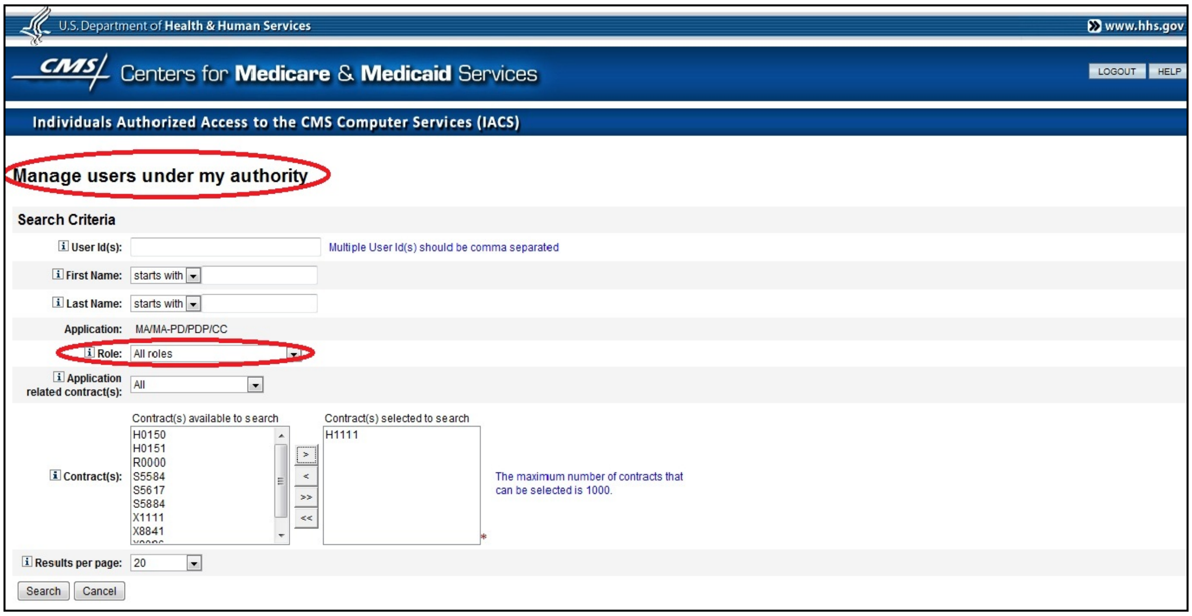
13.2 Manage Contracts

To manage users under the Approver's authorization, the Approver must first log in to IACS using his IACS User ID and password. The **My Profile** screen will display after a successful login, as illustrated in Figure 37.

The MA/MA-PD/PDP/CC Application screens will be used to illustrate the **Manage users under my authority** edit function.

Action: Select the Manage users under my authority hyperlink.

The **Manage users under my authority** screen will display, as illustrated in Figure 43. The appropriate search criteria will display based on the Approver's approval authority and the application.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

Search Criteria

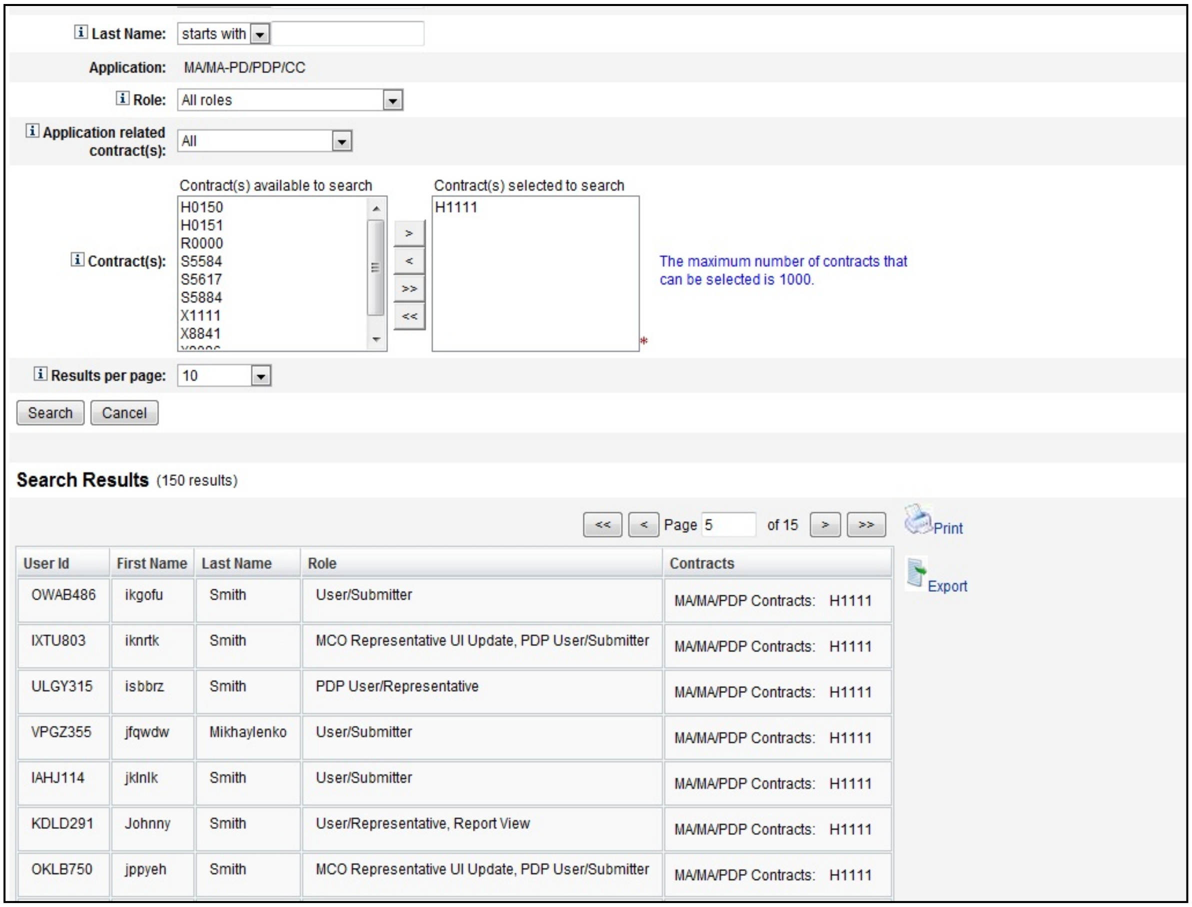
User Id(s):	Multiple User Id(s) should be comma separated
First Name:	starts with
Last Name:	starts with
Application:	MA/MA-PD/PDP/CC
Role:	All roles
Application related contract(s):	All
Contract(s):	Contract(s) available to search: H0150 H0151 R0000 S5584 S5617 S5884 X1111 X8841 Contract(s) selected to search: H1111 The maximum number of contracts that can be selected is 1000.
Results per page:	20

Figure 43: Manage user under my authority – Search Criteria

Action: Select the desired *Search Criteria* by entering the appropriate data in the search fields or by selecting from the available drop-down lists**.**

Action: Select the ***Search*** button to execute the search.

The screen will refresh and the search results will display in a table under the ***Search Criteria*** area, as illustrated in Figure 44.



Last Name: starts with

Application: MA/MA-PD/PDP/CC

Role: All roles

Application related contract(s): All

Contract(s):
Contract(s) available to search: H0150, H0151, R0000, S5584, S5617, S5884, X1111, X8841
Contract(s) selected to search: H1111 *

The maximum number of contracts that can be selected is 1000.

Results per page: 10

Search Results (150 results)

Page 5 of 15

User Id	First Name	Last Name	Role	Contracts
OWAB486	ikgofu	Smith	User/Submitter	MA/MA/PDP Contracts: H1111
IXTU803	iknrtk	Smith	MCO Representative UI Update, PDP User/Submitter	MA/MA/PDP Contracts: H1111
ULGY315	isbbrz	Smith	PDP User/Representative	MA/MA/PDP Contracts: H1111
VPGZ355	jfqwdw	Mikhaylenko	User/Submitter	MA/MA/PDP Contracts: H1111
IAHJ114	jklnlk	Smith	User/Submitter	MA/MA/PDP Contracts: H1111
KDLD291	Johnny	Smith	User/Representative, Report View	MA/MA/PDP Contracts: H1111
OKLB750	jppyeh	Smith	MCO Representative UI Update, PDP User/Submitter	MA/MA/PDP Contracts: H1111

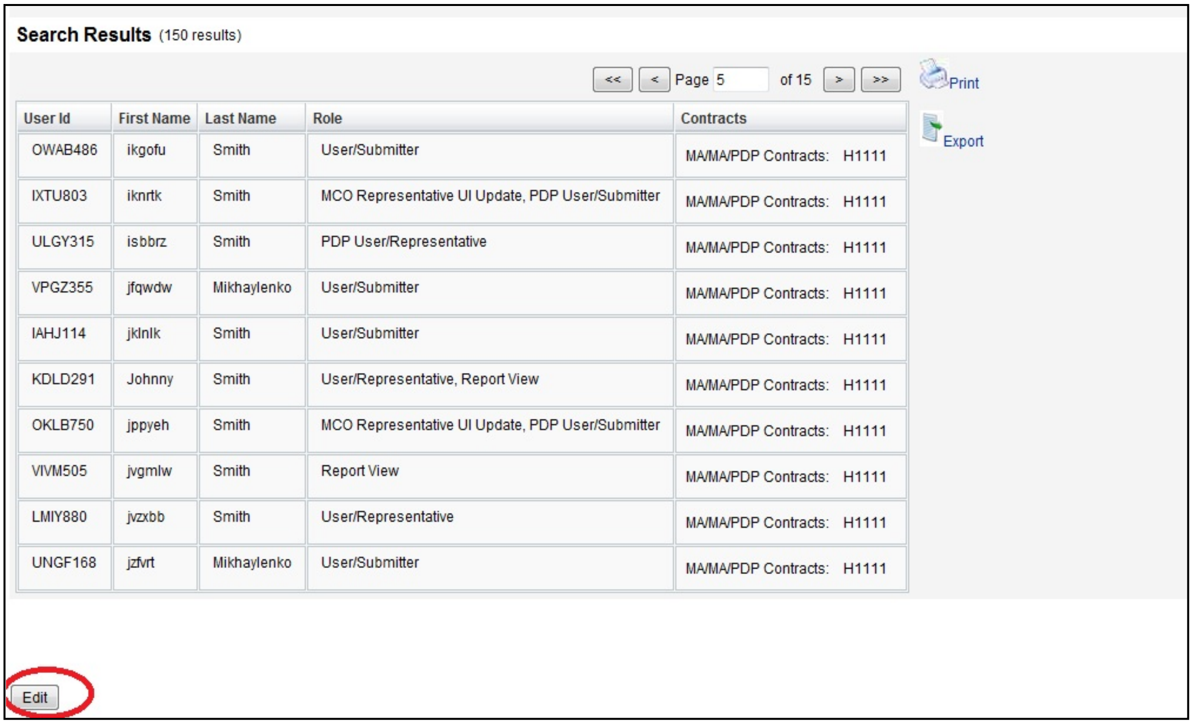
Figure 44: Manage users under my authority Screen – Search Results Area

Action: Scroll through the screens of the ***Search Results*** table until the appropriate user is found**.**

Action: Select the ***Print*** icon to print the information.

Action: Select the ***Export*** icon to export the information to an Excel file.

Note: **Manage users under my authority** function has a limitation in the number of records that can be displayed in the Search Results section. If the given search criteria for the search qualifies for 1,000 or more records, then the search results are not displayed; rather, a warning message stating that the search qualified for more than the allowable limit will be displayed. The Approver should narrow the search criteria and execute the search again.



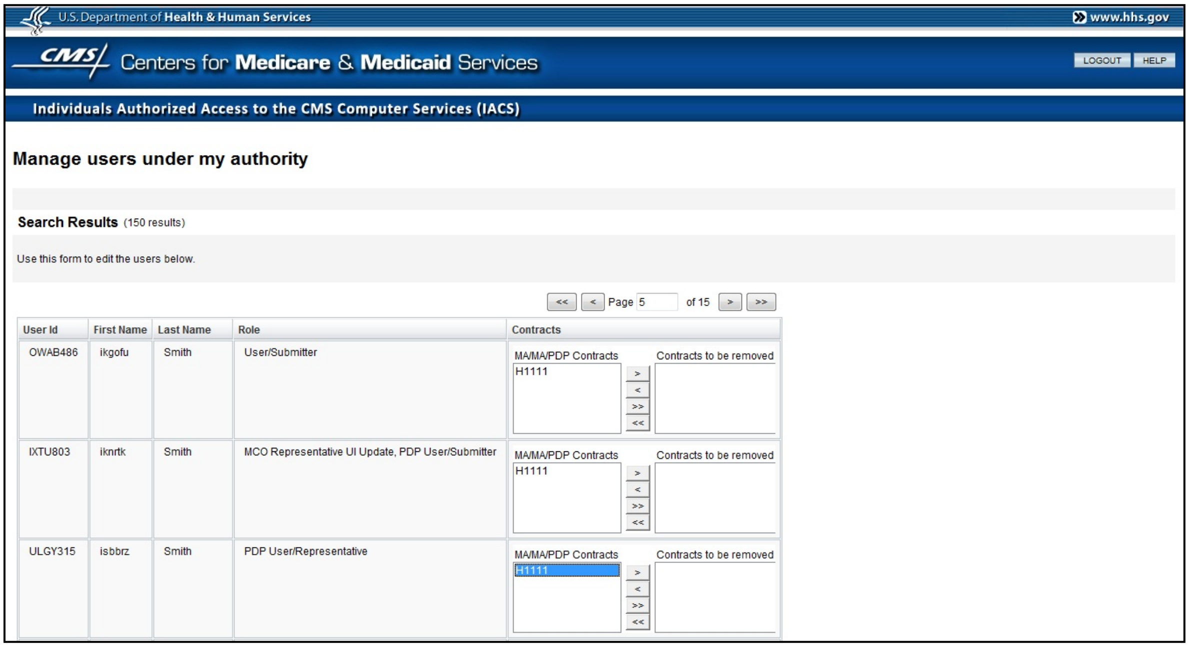
Search Results (150 results)

User Id	First Name	Last Name	Role	Contracts
OWAB486	ikgofu	Smith	User/Submitter	MA/MA/PDP Contracts: H1111
IXTU803	iknrtk	Smith	MCO Representative UI Update, PDP User/Submitter	MA/MA/PDP Contracts: H1111
ULGY315	isbbrz	Smith	PDP User/Representative	MA/MA/PDP Contracts: H1111
VPGZ355	jfqwdw	Mikhaylenko	User/Submitter	MA/MA/PDP Contracts: H1111
IAHJ114	jklnlk	Smith	User/Submitter	MA/MA/PDP Contracts: H1111
KDLD291	Johnny	Smith	User/Representative, Report View	MA/MA/PDP Contracts: H1111
OKLB750	jppyeh	Smith	MCO Representative UI Update, PDP User/Submitter	MA/MA/PDP Contracts: H1111
VIVM505	jvgmlw	Smith	Report View	MA/MA/PDP Contracts: H1111
LMIY880	jvzxbb	Smith	User/Representative	MA/MA/PDP Contracts: H1111
UNGF168	jzfvrt	Mikhaylenko	User/Submitter	MA/MA/PDP Contracts: H1111

Figure 45: Manage users under my authority Screen Search Results Area – Edit Button Selection

Action: Select the ***Edit*** button at the bottom of the screen, as illustrated in Figure 45.

The ***Search Results*** table will be converted into an editable format, as illustrated in Figure 46.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

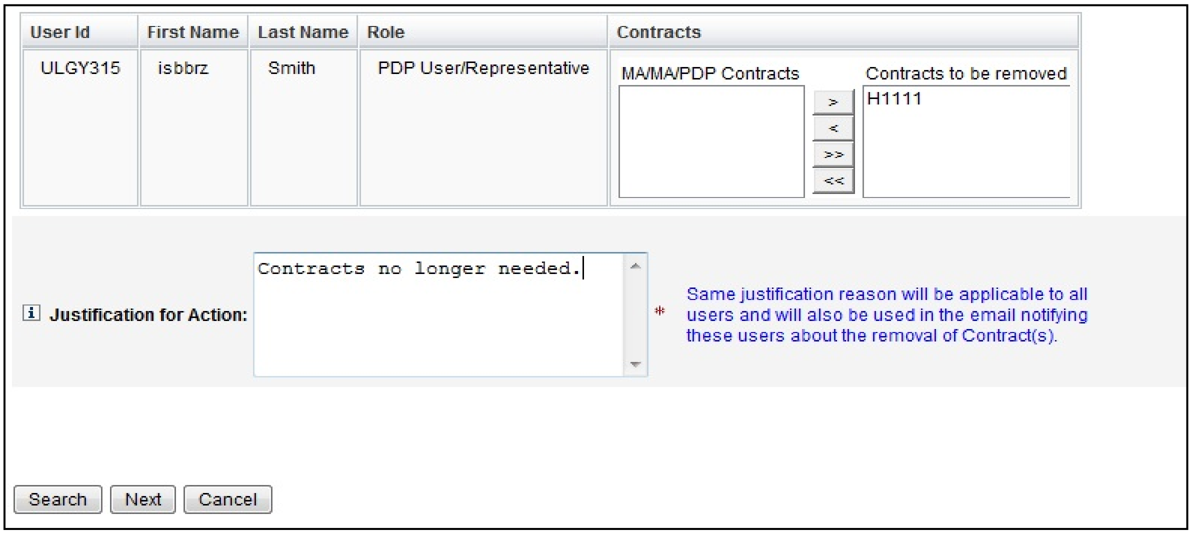
Search Results (150 results)

Use this form to edit the users below.

User Id	First Name	Last Name	Role	Contracts
OWAB486	ikgofu	Smith	User/Submitter	MA/MA/PDP Contracts: H1111 Contracts to be removed: > < >> <<
IXTU803	iknrtk	Smith	MCO Representative UI Update, PDP User/Submitter	MA/MA/PDP Contracts: H1111 Contracts to be removed: > < >> <<
ULGY315	isbbrz	Smith	PDP User/Representative	MA/MA/PDP Contracts: H1111 Contracts to be removed: > < >> <<

Figure 46: Manage users under my authority Screen: Search Results Area – Editable Search Results

Action: Edit the search results as desired.



User Id	First Name	Last Name	Role	Contracts
ULGY315	isbbrz	Smith	PDP User/Representative	MA/MA/PDP Contracts: Contracts to be removed: H1111

Justification for Action: Contracts no longer needed. *

Same justification reason will be applicable to all users and will also be used in the email notifying these users about the removal of Contract(s).

Figure 47: Manage users under my authority Screen: Search Results Area – Single Justification for Action

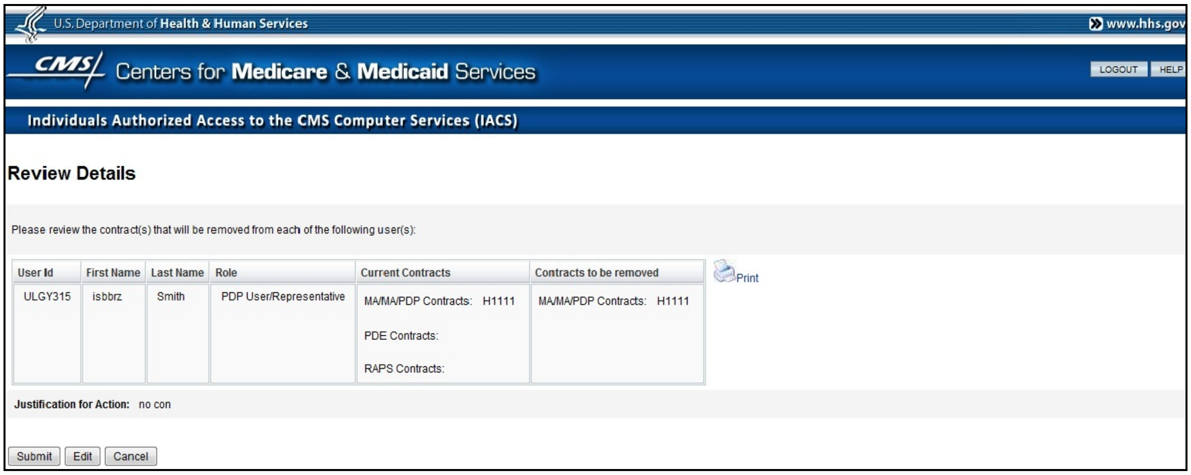
If the Approver wants to discard these search results and conduct a new search, select the ***Search*** button and the system will return to the **Manage users under my authority** - ***Search Criteria*** screen, as illustrated in Figure 43.

If the Approver wants to cancel the edits, select the ***Cancel*** button and the system will discard the changes and return to the **My Profile** screen, as illustrated in Figure 37.

Action: Enter the justification for the edits in the *Justification for Action* field, as illustrated in Figure 47.

Action: When finished, select the ***Next*** button.

The screen will refresh and the **Review Details** screen will be displayed, as illustrated in Figure 48.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Review Details

Please review the contract(s) that will be removed from each of the following user(s):

User Id	First Name	Last Name	Role	Current Contracts	Contracts to be removed
ULGY315	isbbrz	Smith	PDP User/Representative	MA/MA/PDP Contracts: H1111 PDE Contracts: RAPS Contracts:	MA/MA/PDP Contracts: H1111

Justification for Action: no con

Figure 48: Review Details Screen

Action: Review the details and when satisfied with the change select the ***Submit*** button. The screen will refresh and return to the **My Profile** screen, as illustrated in Figure 37.

If the Approver wants to make changes to the edits, select the ***Edit*** button and the system will return to the editable ***Search Results*** section, as illustrated in Figure 46.

If the Approver wants to cancel the edits, select the ***Cancel*** button and the system will discard the edits and return to the **My Profile** screen, as illustrated in Figure 37.

13.3 Help Desk Functions using Manage users under my authority

This section is applicable to users with help desk roles. These users will be able to perform standard help desk functions from the **Manage users under my authority** screen. The Helpdesk users will be able to:

- Search and List User Accounts
- View User Accounts
- Disable User Accounts
- Reset User Passwords
- Unlock User Accounts

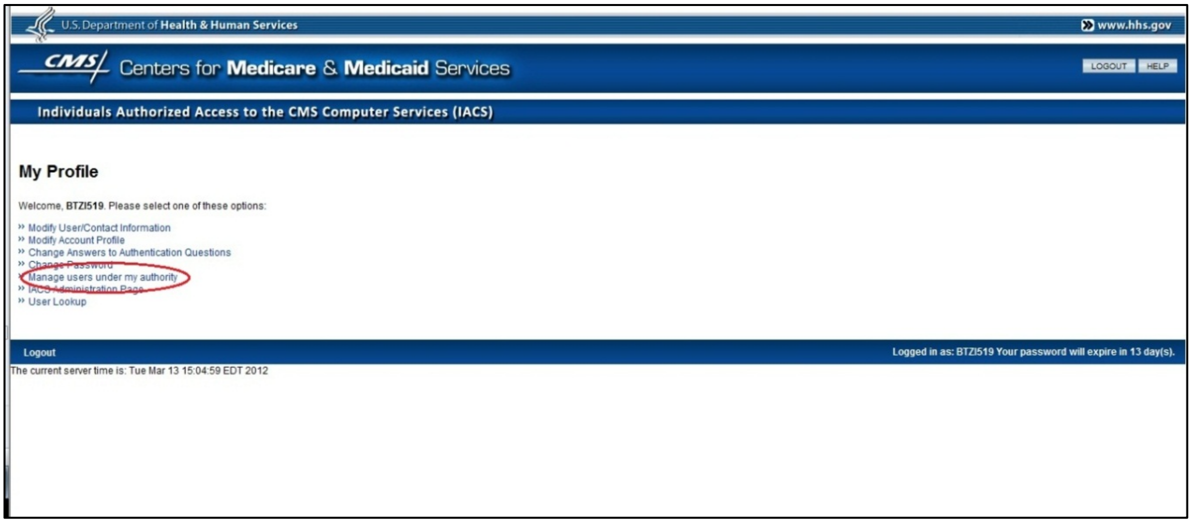
Table 4 lists the help desk roles with the capability to perform help desk functions.

Application	Help Desk Role	Supporting Help Desk
Bundled Payments EFT	Bundled Payments EFT Help Desk	Bundled Payments EFT Help Desk
CMS Administration – Physician Value	PV Admin Helpdesk Approver	PV Helpdesk
COB	COB Helpdesk	MAPD Help Desk
CPC	CPC Support	CPC Support

Application	Help Desk Role	Supporting Help Desk
CSP – MCSIS	MCSIS Help Desk User	MCSIS Help Desk
CSP – HSTP	HSTP Help Desk User	HSTP Help Desk
CSR	MAPD Helpdesk MAPD Helpdesk Admin	MAPD Help Desk
DMEPOS Bidding System (DBidS)	CBIC-Tier1 CBIC-Tier2	CBIC Help Desk
ECRS	ECRS HelpDesk	EDI Help Desk
esMD	esMD Help Desk	esMD Help Desk
GENTRAN	Gentran Helpdesk	IACS Administration
HETS UI	MCARE Help Desk	MCARE Help Desk
HPG	MCARE Help Desk	MCARE Help Desk
Internet Server	Internet Server Help Desk	IACS Administration
MA/MA-PD/PDP/CC	MAPD Helpdesk MAPD Helpdesk Admin	MAPD Help Desk
MACPro	MACPro Help Desk	MACPro Application Help Desk
MDR	Helpdesk	MAPD Help Desk
MyCGS	CSG Helpdesk	CGS DME JC Provider Call Center
MED	MED Help Desk User	EUS Help Desk
Novitasphere	Novitas Help Desk User	Novitasphere Help Desk
PQRS/eRx	PQRI Helpdesk	QualityNet Help Desk
PS&R/STAR	PS&R/STAR Helpdesk	EUS Help Desk
PV/PQRS Registration System	PV Helpdesk Approver	PV Helpdesk
The SPOT	FCSO Help Desk	FCSO Help Desk
VMS Client Letter	VMS Help Desk	VMS Help Desk

Table 4: Applications and Help Desk Roles Using Manage Users Under My Authority

To use the **Manage users under my authority** function, the Helpdesk user must first log in to IACS using his IACS User ID and password. The **My Profile** screen will display after a successful login. Figure 49 illustrates the **My Profile** screen after a successful login by an ECRS HelpDesk user.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
» Modify User/Contact Information
» Modify Account Profile
» Change Answers to Authentication Questions
» Change Password
» Manage users under my authority
» IACS Administration Page
» User Lookup
Logout

My Profile

Welcome, **BTZI519**. Please select one of these options:

Logged in as: BTZI519 Your password will expire in 13 day(s).

The current server time is: Tue Mar 13 15:04:59 EDT 2012

Figure 49: My Profile Screen

Action: Select the Manage users under my authority hyperlink.

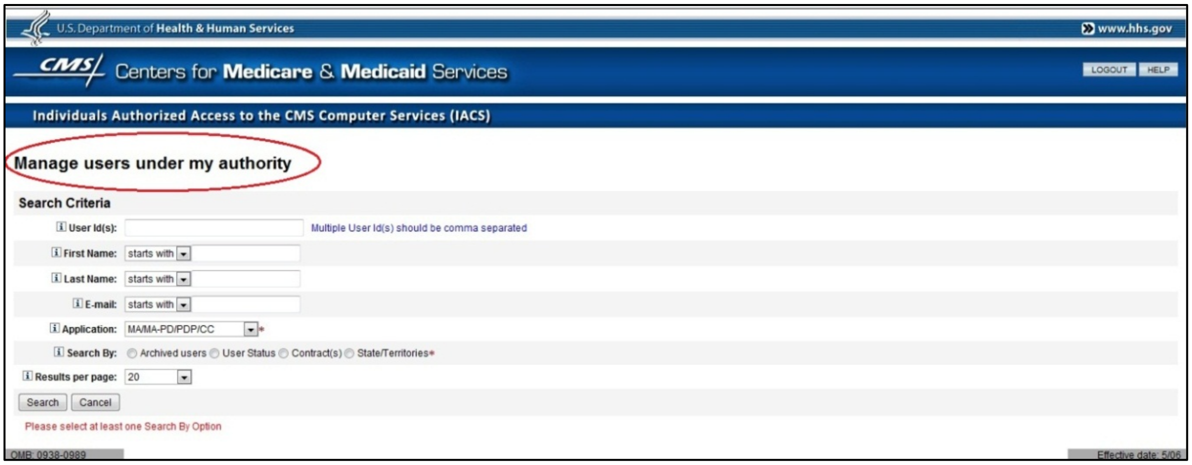
The **Manage users under my authority** screen will display multiple ***Search Criteria*** options. The search criteria options will be dependent on the application. For some applications, the *User Status* and *Role* selection will not display at the same time. Therefore, the Search Criteria will display the *Search By* field as a group of radio buttons. The Helpdesk will select one of the radio buttons to search.

Note: If the Helpdesk supports multiple CMS applications, the user will be required to first select the application from the *Application* drop-down list on the **Manage users under my authority** screen. The screen will refresh and display the appropriate search criteria options.

The following applications will display the *Search By* radio buttons for Archived users, User Status, and Roles: COB, DMEPOS Bidding System (DBidS), HETUS UI, HPG, and PQRS/eRx.

The MA/MA-PD/PDP/CC will display the *Search By* radio buttons for Archived users, User Status, Contracts, or State/Territories. Figure 50 displays the search options for MA/MA-PD/PDP/CC Helpdesks.

The following applications will display the User Status and Role selections as drop-down lists, as illustrated in Figure 51: Bundled Payments EFT, CMS Administration – Physician Value, CPC, CSP-MSCIS, CSP-HSTP, ECRS, esMD, Gentran, Internet Server, MACPro, MED, MDR, MyCGS, Novitasphere, PS&R/STAR, PV/PQRS Registration System, The SPOT, and VMS Client Letter.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP

Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

Search Criteria

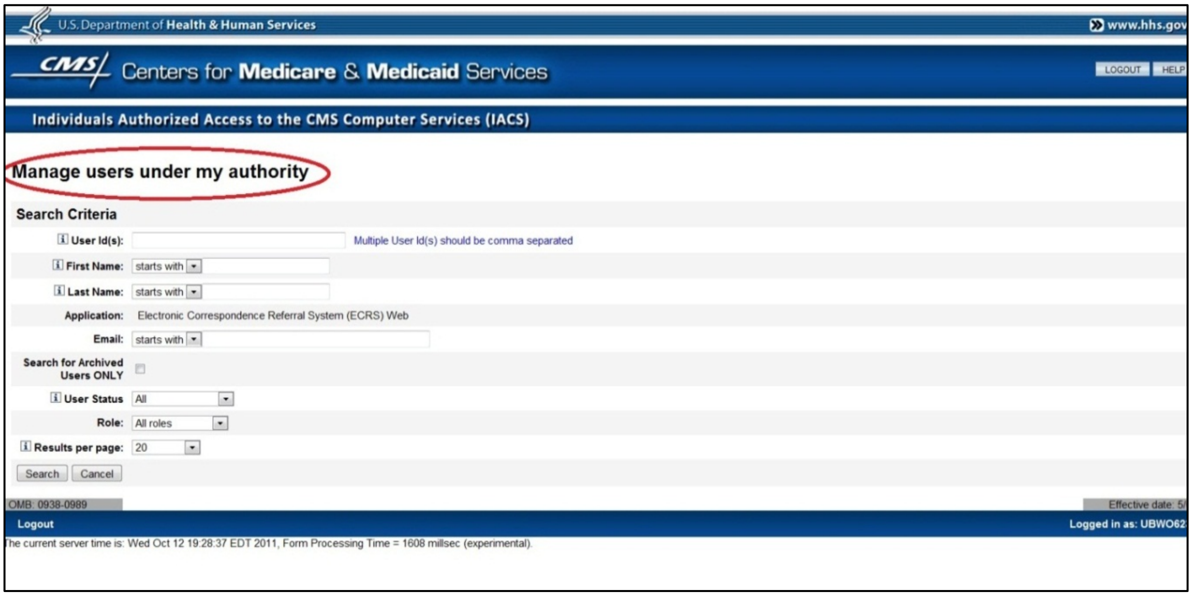
User Id(s): Multiple User Id(s) should be comma separated
First Name: starts with
Last Name: starts with
E-mail: starts with
Application: MA/MA-PD/PDP/CC *
Search By: ○ Archived users ○ User Status ○ Contract(s) ○ State/Territories*
Results per page: 20

Search Cancel

Please select at least one Search By Option

OMB: 0938-0989 Effective date: 5/06

Figure 50: Manage users under my authority Screen - MA/MA-PD/PDP/CC


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP

Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

Search Criteria

User Id(s): Multiple User Id(s) should be comma separated
First Name: starts with
Last Name: starts with
Application: Electronic Correspondence Referral System (ECRS) Web
Email: starts with
Search for Archived Users ONLY □
User Status All
Role: All roles
Results per page: 20

Search Cancel

OMB: 0938-0989 Effective date: 5/

Logout Logged in as: UBWO62

he current server time is: Wed Oct 12 19:28:37 EDT 2011, Form Processing Time = 1608 millsec (experimental).

Figure 51: Manage users under my authority Screen - ECRS

13.4 Searching for User Accounts

Helpdesks can view the users of their corresponding applications using the **Manage users under my authority** function, as illustrated in Figure 50 or Figure 51. The steps below will describe the **ECRS** Application. The Note section will provide additional information for applications with radio button options.

Action: Select the desired ***Search Criteria*** by entering the appropriate data in the search fields or selecting from the available drop-down lists**.**

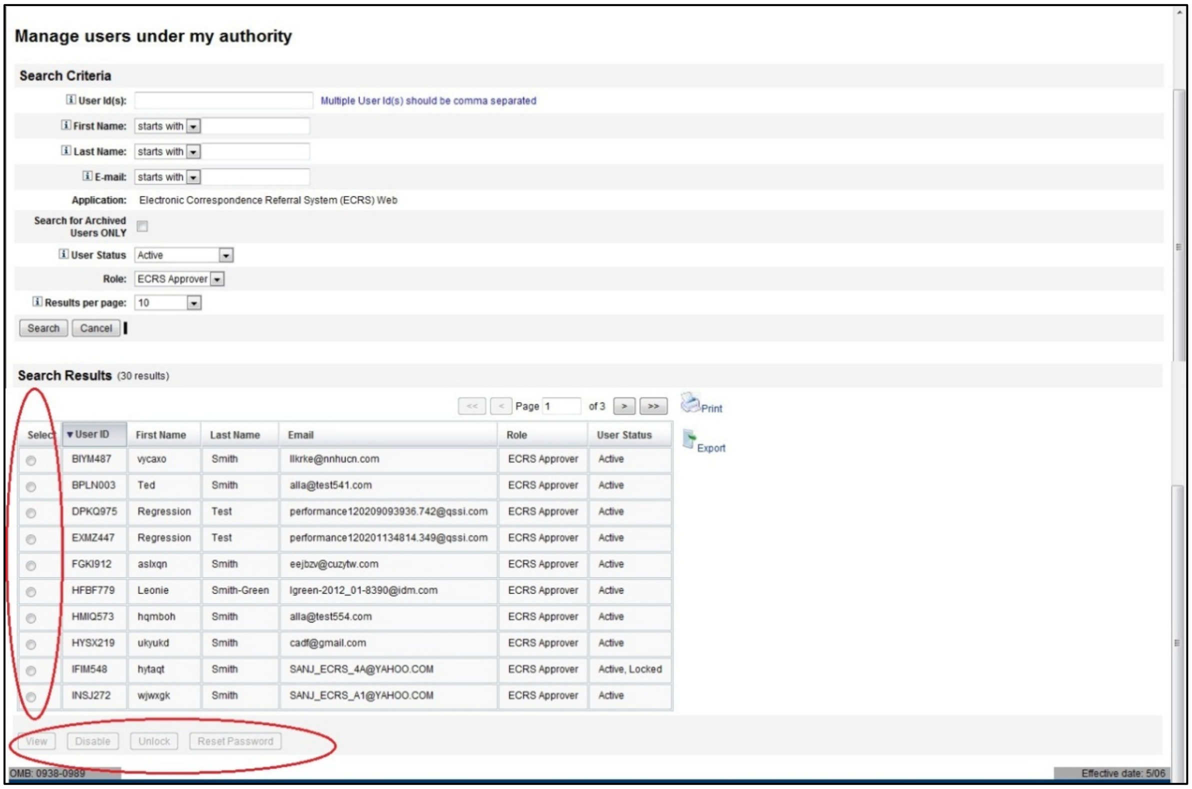
Notes:

- Helpdesks can search users by *User ID(s), First Name, Last Name*, *E-mail*, *User Status, Role, Archived Users,* and other specific application attributes.

- The *Search By* field is a collection of radio buttons that, when selected, refresh the screen and displays subsequent drop-down list choices to select. For instance, when the MAPD Helpdesk selects the *Contract(s)* radio button, the screen will refresh and the *Contract(s)* multi-select box will display.

Action: Select the ***Search*** button to execute the search.

The screen will refresh and the ***Search Results*** will display in a table under the ***Search Criteria*** area illustrated in Figure 52.



Manage users under my authority

Search Criteria

User Id(s):	Multiple User Id(s) should be comma separated
First Name:	starts with
Last Name:	starts with
E-mail:	starts with
Application:	Electronic Correspondence Referral System (ECRS) Web
Search for Archived Users ONLY	□
User Status	Active
Role:	ECRS Approver
Results per page:	10

Search Results (30 results)

Select	▾User ID	First Name	Last Name	Email	Role	User Status
○	BIYM487	vycaxo	Smith	llkrke@nnhucn.com	ECRS Approver	Active
○	BPLN003	Ted	Smith	alla@test541.com	ECRS Approver	Active
○	DPKQ975	Regression	Test	performance120209093936.742@qssi.com	ECRS Approver	Active
○	EXMZ447	Regression	Test	performance120201134814.349@qssi.com	ECRS Approver	Active
○	FGKI912	aslxqn	Smith	eejbzv@cuzytw.com	ECRS Approver	Active
○	HFBF779	Leonie	Smith-Green	lgreen-2012_01-8390@idm.com	ECRS Approver	Active
○	HMIQ573	hqmboh	Smith	alla@test554.com	ECRS Approver	Active
○	HYSX219	ukyukd	Smith	cadf@gmail.com	ECRS Approver	Active
○	IFIM548	hytaqt	Smith	SANJ_ECRS_4A@YAHOO.COM	ECRS Approver	Active, Locked
○	INSJ272	wjwxgk	Smith	SANJ_ECRS_A1@YAHOO.COM	ECRS Approver	Active

OMB: 0938-0989

Effective date: 5/06

Figure 52: Manage users under my authority Screen – Search Results

The ***Search Results*** will include a radio button to the left of each row of the user record and the following help desk function buttons will display at the bottom of the screen, as illustrated in Figure 52:

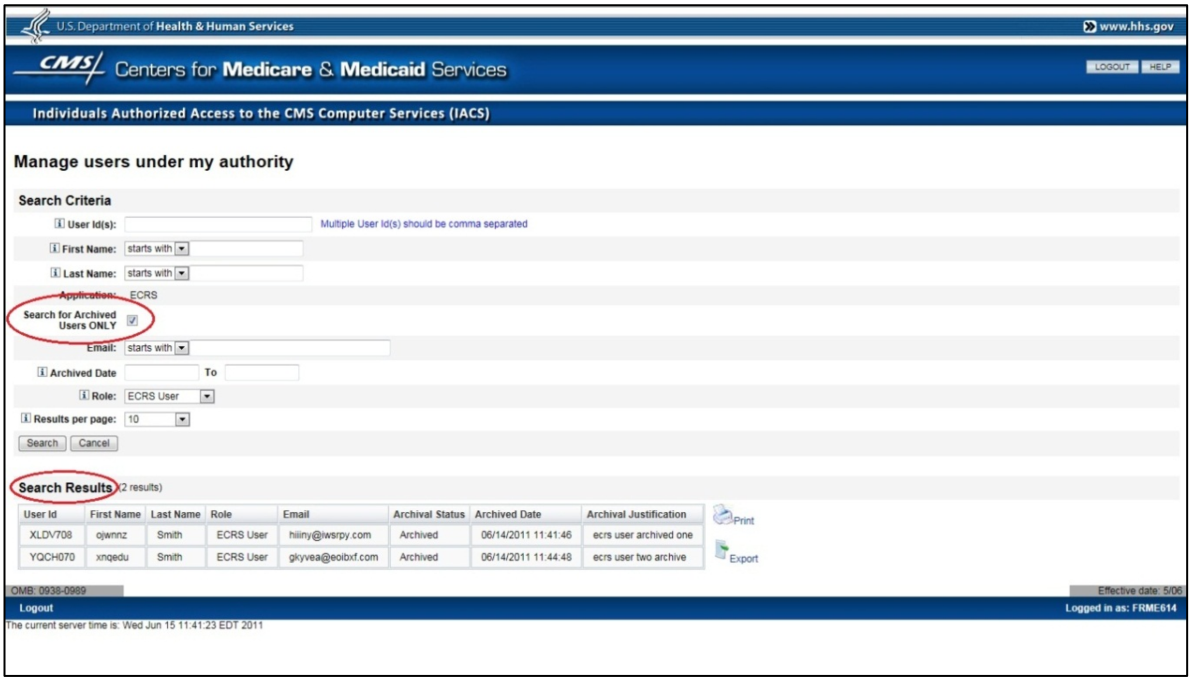
- View
- Disable
- Unlock
- Reset Password

Notes:

- The help desk function buttons will be inactive until the Helpdesk selects a user record. Once the radio button is selected, the appropriate help desk function buttons are enabled based on the user's status.
- If the system retrieves more than 1,000 records, a message will display informing the user to narrow the search.

Helpdesks can view archived users of their corresponding application(s) using the **Manage users under my authority** function, as illustrated in Figure 53.

Action: Select the *Search for Archived Users ONLY* check box in the **Manage users under my authority** screen.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

Search Criteria

User Id(s): Multiple User Id(s) should be comma separated

First Name: starts with

Last Name: starts with

Application: ECRS

Search for Archived Users ONLY ☑

Email: starts with

Archived Date To

Role: ECRS User

Results per page: 10

Search Results (2 results)

User Id	First Name	Last Name	Role	Email	Archival Status	Archived Date	Archival Justification
XLDV708	ojwnnz	Smith	ECRS User	hiiiny@iwsrpy.com	Archived	06/14/2011 11:41:46	ecrs user archived one
YQCH070	xnqedu	Smith	ECRS User	gkyvea@eoibxf.com	Archived	06/14/2011 11:44:48	ecrs user two archive

OMB: 0938-0989

Effective date: 5/06

Logged in as: FRME614

The current server time is: Wed Jun 15 11:41:23 EDT 2011

Figure 53: Manage users under my authority Screen – Search Results (Archived Users)

Action: Select the desired ***Search Criteria*** by entering the appropriate data in the search fields or select from the available drop-down lists**.**

Note: Helpdesk users can search archived users using *User ID(s), First Name, Last Name, E-mail, Archived Date,* and *Role*.

Action: Select the ***Search*** button to execute the search.

The screen will refresh and the ***Search Results*** will display in a table under the ***Search Criteria*** area, as illustrated in Figure 53.

Notes:

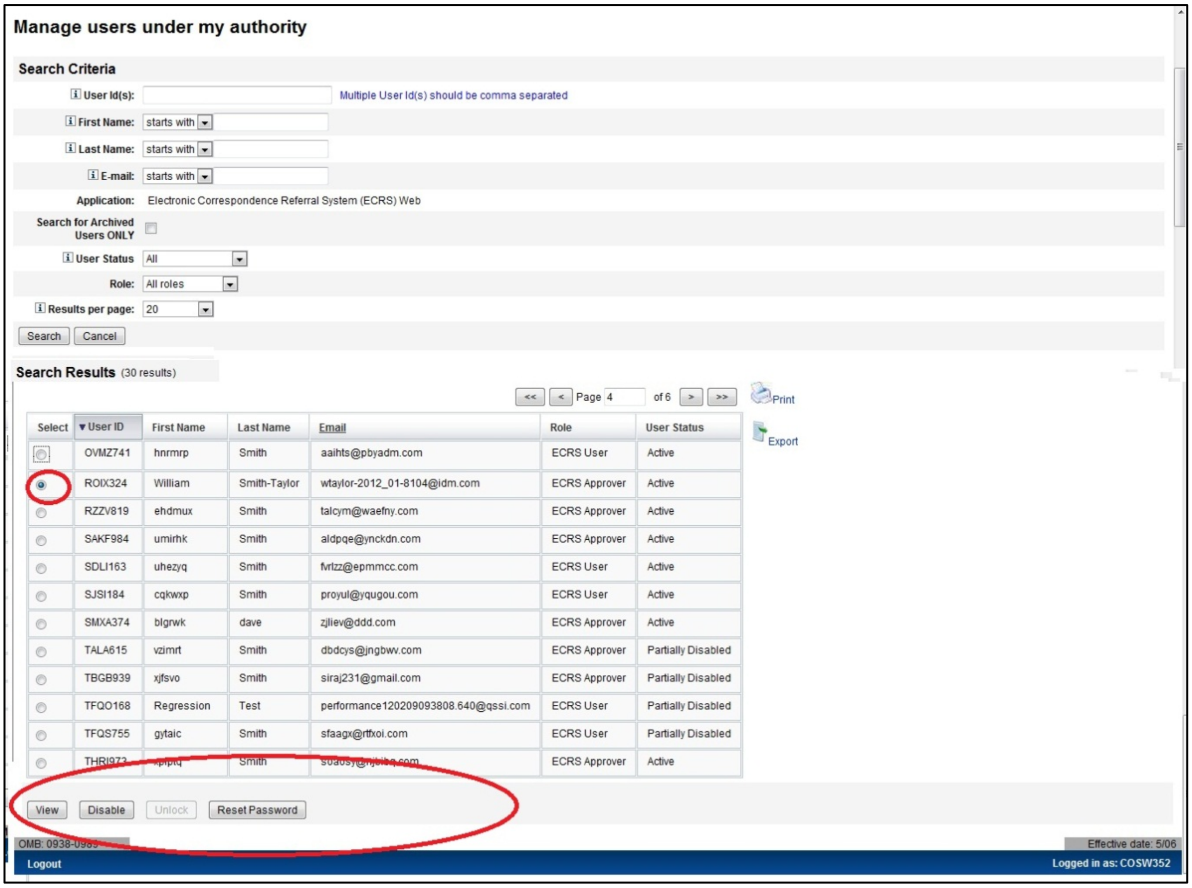
- If the ***Search*** button is selected and no search criteria has been selected, then the search results will include all users under the Helpdesk's scope of responsibility.
- The help desk function buttons are not shown when searching for archived users.

13.4.1 View User Account Information

The Helpdesk can view user account information (under their scope of responsibility) by using the **Manage users under my authority** view function to obtain user account information or identify user accounts requiring maintenance activities.

Action: Select the radio button shown to the left of a user record, as illustrated in Figure 54.

The ***Search Results*** area of the **Manage users under my authority** screen will refresh and the appropriate help desk function buttons will be enabled depending on the user's status.



Manage users under my authority

Search Criteria

User Id(s): Multiple User Id(s) should be comma separated
First Name: starts with
Last Name: starts with
E-mail: starts with
Application: Electronic Correspondence Referral System (ECRS) Web
Search for Archived Users ONLY □
User Status: All
Role: All roles
Results per page: 20

Search Results (30 results)

Page 4 of 6

Select	▼User ID	First Name	Last Name	Email	Role	User Status
○	OVMZ741	hnrmrp	Smith	aaihts@pbyadm.com	ECRS User	Active
●	ROIX324	William	Smith-Taylor	wtaylor-2012_01-8104@idm.com	ECRS Approver	Active
○	RZZV819	ehdmux	Smith	talcym@waefny.com	ECRS Approver	Active
○	SAKF984	umirhk	Smith	aldpqe@ynckdn.com	ECRS Approver	Active
○	SDLI163	uhezyq	Smith	fvrlzz@epmmcc.com	ECRS User	Active
○	SJSI184	cqkwxp	Smith	proyul@yqugou.com	ECRS User	Active
○	SMXA374	blgrwk	dave	zjliev@ddd.com	ECRS Approver	Active
○	TALA615	vzimrt	Smith	dbdcys@jngbwv.com	ECRS Approver	Partially Disabled
○	TBGB939	xjfsvo	Smith	siraj231@gmail.com	ECRS Approver	Partially Disabled
○	TFQO168	Regression	Test	performance120209093808.640@qssi.com	ECRS User	Partially Disabled
○	TFQS755	gytaic	Smith	sfaagx@rtfxoi.com	ECRS User	Partially Disabled
○	THRI973	xpiptq	Smith	soaosy@njbibq.com	ECRS Approver	Active

OMB: 0938-0989 Effective date: 5/06

Logged in as: COSW352

Figure 54: Manage users under my authority Screen – Help Desk Function Buttons Enabled

Action: Select the ***View*** button.

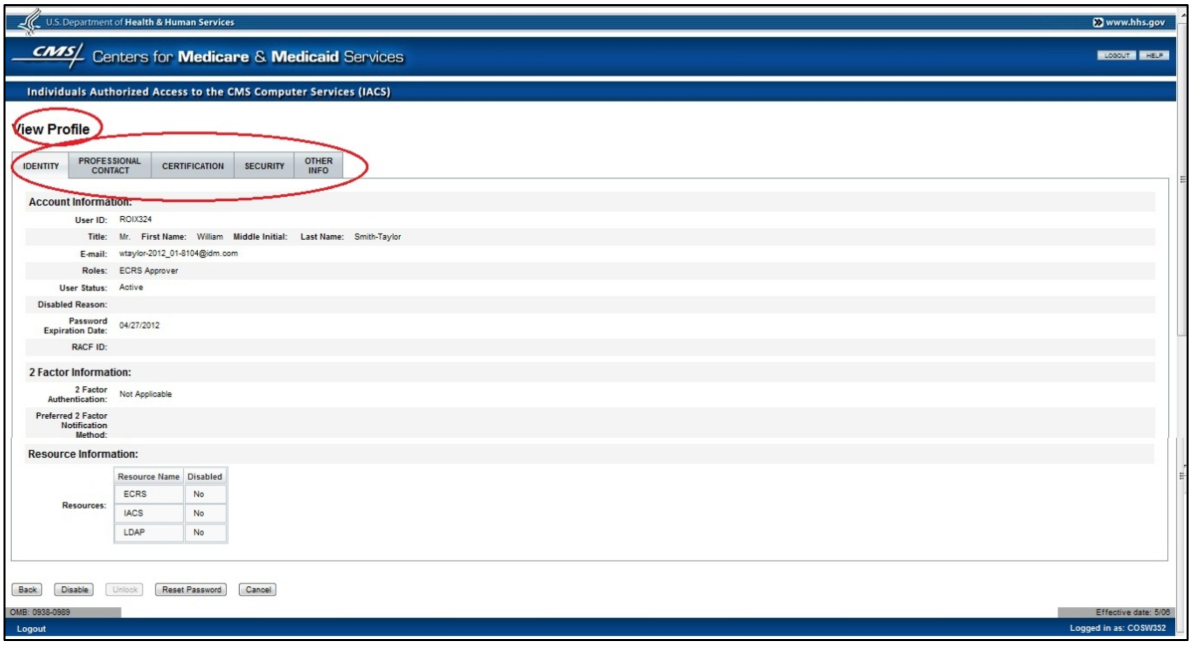
The **View Profile** screen, with the following navigation tabs, will display, as illustrated in Figure 55:

- Identity
- Professional Contact
- Certification
- Security
- Other Info

The Helpdesk will be able to choose any tab from the **View Profile** screen to view the appropriate user information. In addition, the **View Profile** screen provides the Helpdesk the ability to perform the standard help desk functions in every tab.

Once the ***View*** button is selected, the ***Identity*** tab will be the first tab displayed and this tab will include the user account information, as illustrated in Figure 55.

The illustrations below show how the Helpdesk could navigate through the various tabs on the **View Profile** screen and view the relevant account information in each tab.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)
View Profile
IDENTITY
PROFESSIONAL CONTACT
CERTIFICATION
SECURITY
OTHER INFO

Account Information:

User ID: ROIX324

Title: Mr. First Name: William Middle Initial: Last Name: Smith-Taylor

E-mail: wtaylor-2012_01-8104@idm.com

Roles: ECRS Approver

User Status: Active

Disabled Reason:

Password Expiration Date: 04/27/2012

RACF ID:

2 Factor Information:

2 Factor Authentication: Not Applicable

Preferred 2 Factor Notification Method:

Resource Information:

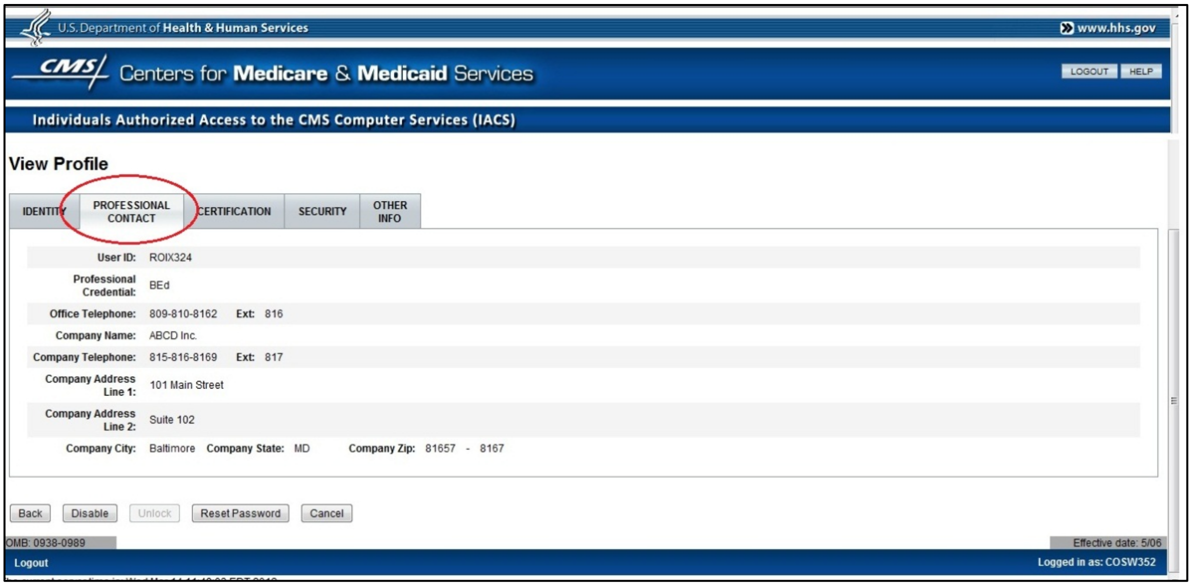
Resources:

Resource Name	Disabled
ECRS	No
IACS	No
LDAP	No

Figure 55: View Profile Screen – Identity Tab

Action: Select the ***Professional Contact*** tab.

The Professional Credentials and Company information will display, as illustrated in Figure 56.



User ID: ROIX324

Professional Credential: BEd

Office Telephone: 809-810-8162 Ext: 816

Company Name: ABCD Inc.

Company Telephone: 815-816-8169 Ext: 817

Company Address Line 1: 101 Main Street

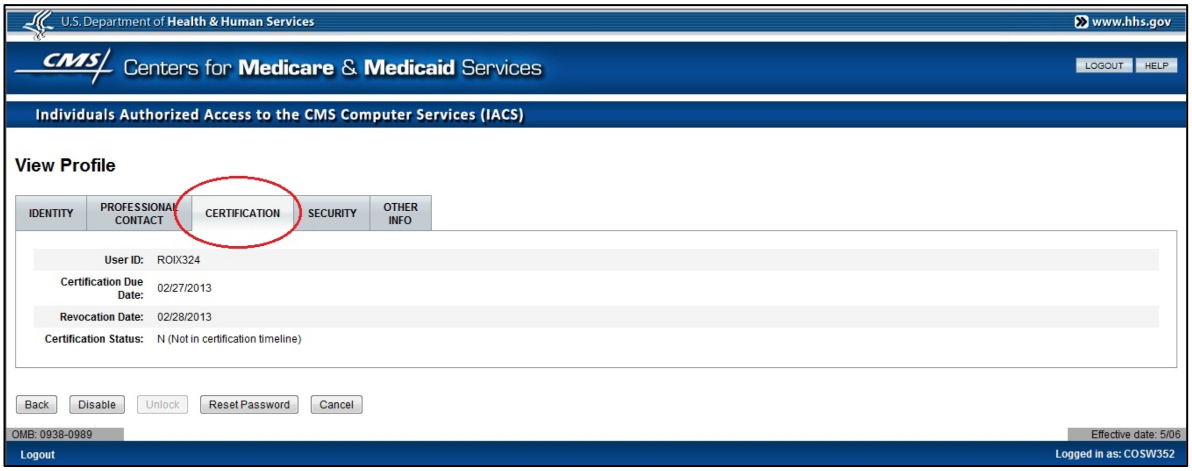
Company Address Line 2: Suite 102

Company City: Baltimore Company State: MD Company Zip: 81657 - 8167

Figure 56: View Profile Screen – Professional Contact Tab

Action: Select the ***Certification*** tab.

The user’s Certification information will display, as illustrated in Figure 57.



User ID: ROIX324

Certification Due Date: 02/27/2013

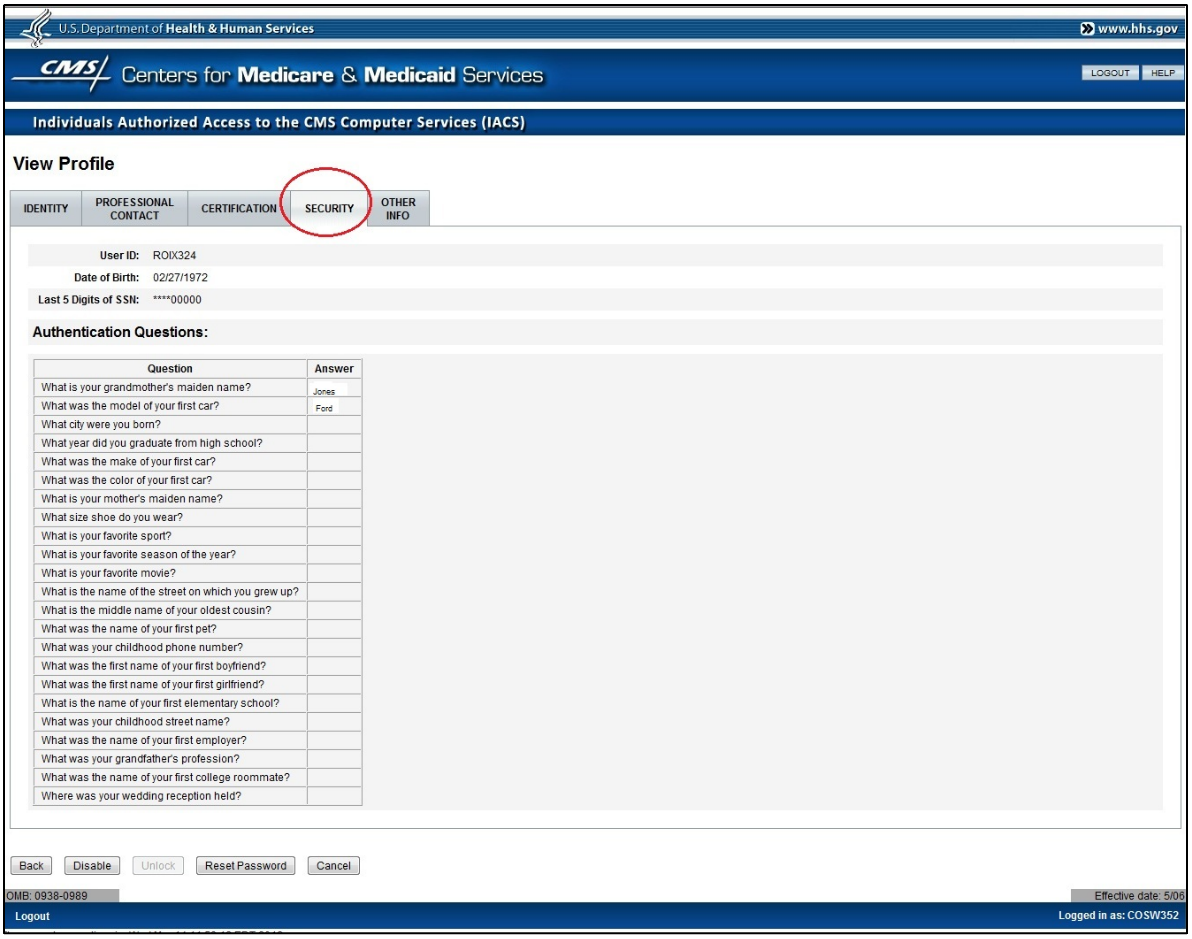
Revocation Date: 02/28/2013

Certification Status: N (Not in certification timeline)

Figure 57: View Profile Screen – Certification Tab

Action: Select the ***Security*** tab.

The user’s security information, authentication questions and answers will display, as illustrated in Figure 58.



View Profile

User ID: ROIX324

Date of Birth: 02/27/1972

Last 5 Digits of SSN: ****00000

Authentication Questions:

Question	Answer
What is your grandmother's maiden name?	Jones
What was the model of your first car?	Ford
What city were you born?	
What year did you graduate from high school?	
What was the make of your first car?	
What was the color of your first car?	
What is your mother's maiden name?	
What size shoe do you wear?	
What is your favorite sport?	
What is your favorite season of the year?	
What is your favorite movie?	
What is the name of the street on which you grew up?	
What is the middle name of your oldest cousin?	
What was the name of your first pet?	
What was your childhood phone number?	
What was the first name of your first boyfriend?	
What was the first name of your first girlfriend?	
What is the name of your first elementary school?	
What was your childhood street name?	
What was the name of your first employer?	
What was your grandfather's profession?	
What was the name of your first college roommate?	
Where was your wedding reception held?	

Figure 58: View Profile Screen – Security Tab

If the user selects the ***Back*** button, the user will be returned to the **Manage users under my authority – *Search Results*** screen.

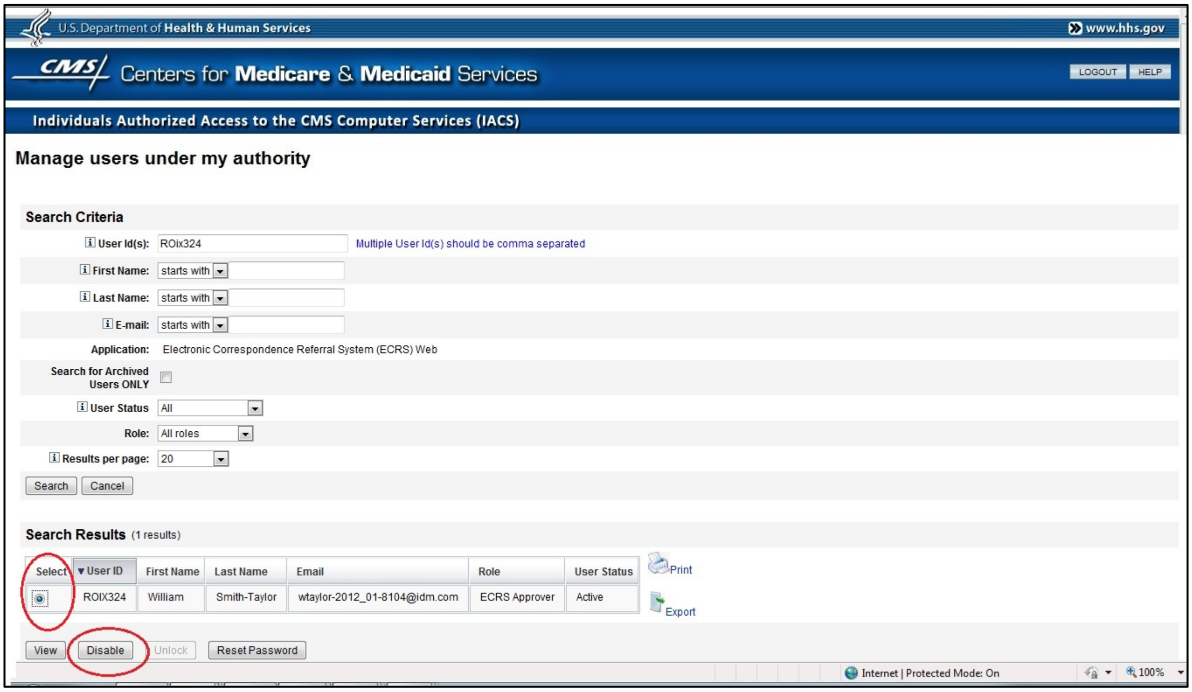
If the user selects the ***Cancel*** button, the user will be returned to the **My Profile** screen.

The ***Other Info*** tab on the **View Profile** screen will display application specific user information, for example, organization information. Specific information will not be applicable for all applications or for some roles within an application. For example, the ECRS Application does not have any application specific user information to be displayed. The PS&R/STAR Helpdesk will be able to view the organization information and CMS Certification Number (CCN), or Medicare Contractor ID, as appropriate. The MCARE Help Desk will be able to view the organization size for a HETS UI Security Official.

13.4.2 Disable User Account

Helpdesks can disable user accounts within their scope of responsibility by using the ***Disable*** button from the **Manage users under my authority – *Search Results*** screen.

Action: From the **Manage users under my authority** screen, select the user you want to disable by selecting the radio button to the left of the user account, as illustrated in Figure 59.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

Search Criteria

User Id(s):	ROix324	Multiple User Id(s) should be comma separated
First Name:	starts with	
Last Name:	starts with	
E-mail:	starts with	
Application:	Electronic Correspondence Referral System (ECRS) Web	
Search for Archived Users ONLY	□	
User Status	All	
Role:	All roles	
Results per page:	20	

Search Results (1 results)

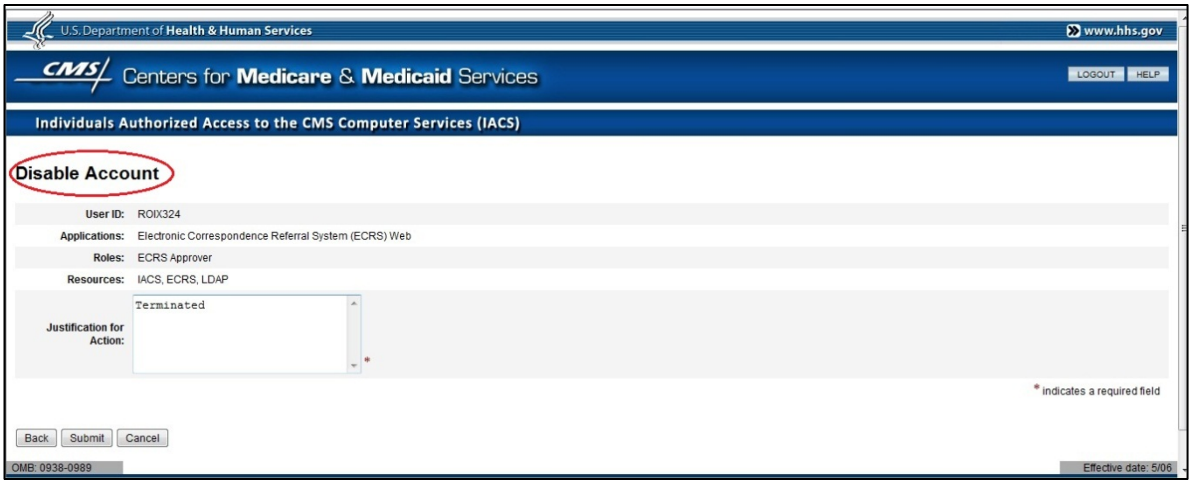
Select	User ID	First Name	Last Name	Email	Role	User Status
●	ROIX324	William	Smith-Taylor	wtaylor-2012_01-8104@idm.com	ECRS Approver	Active

Figure 59: Manage users under my authority Screen –Disable Option

Action: Select the ***Disable*** button.

The **Disable Account** screen will display, as illustrated in Figure 60.

Note: The ***Disable*** button will not be active when the user status is ‘Fully Disabled’.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Disable Account

User ID: ROIX324

Applications: Electronic Correspondence Referral System (ECRS) Web

Roles: ECRS Approver

Resources: IACS, ECRS, LDAP

Justification for Action: Terminated *

* indicates a required field

Back
Submit
Cancel
OMB: 0938-0989
Effective date: 5/06

Figure 60: Disable Account Screen

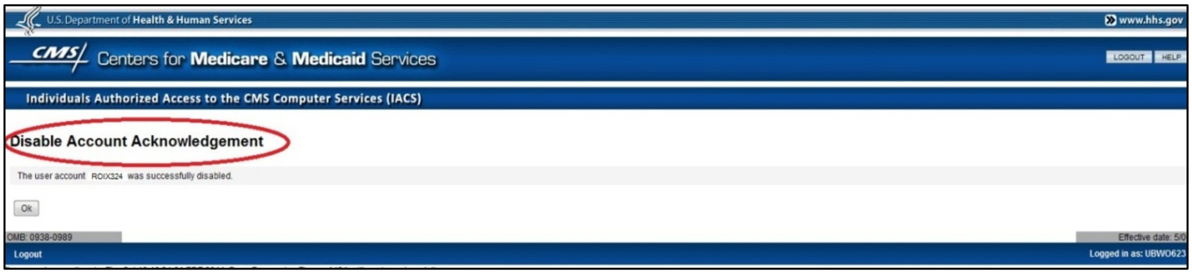
Action: Enter a justification statement in the *Justification for Action* field. This field must include the reason for disabling the user.

Action: Select the ***Submit*** button at the bottom of the screen.

The **Disable Account Acknowledgement** screen will display, as illustrated in Figure 61.

If the user selects the ***Back*** button, the user will be returned to the **Manage users under my authority – *Search Results*** screen.

If the user selects the ***Cancel*** button, the user will be returned to the **My Profile** screen.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Disable Account Acknowledgement

The user account ROIX324 was successfully disabled.

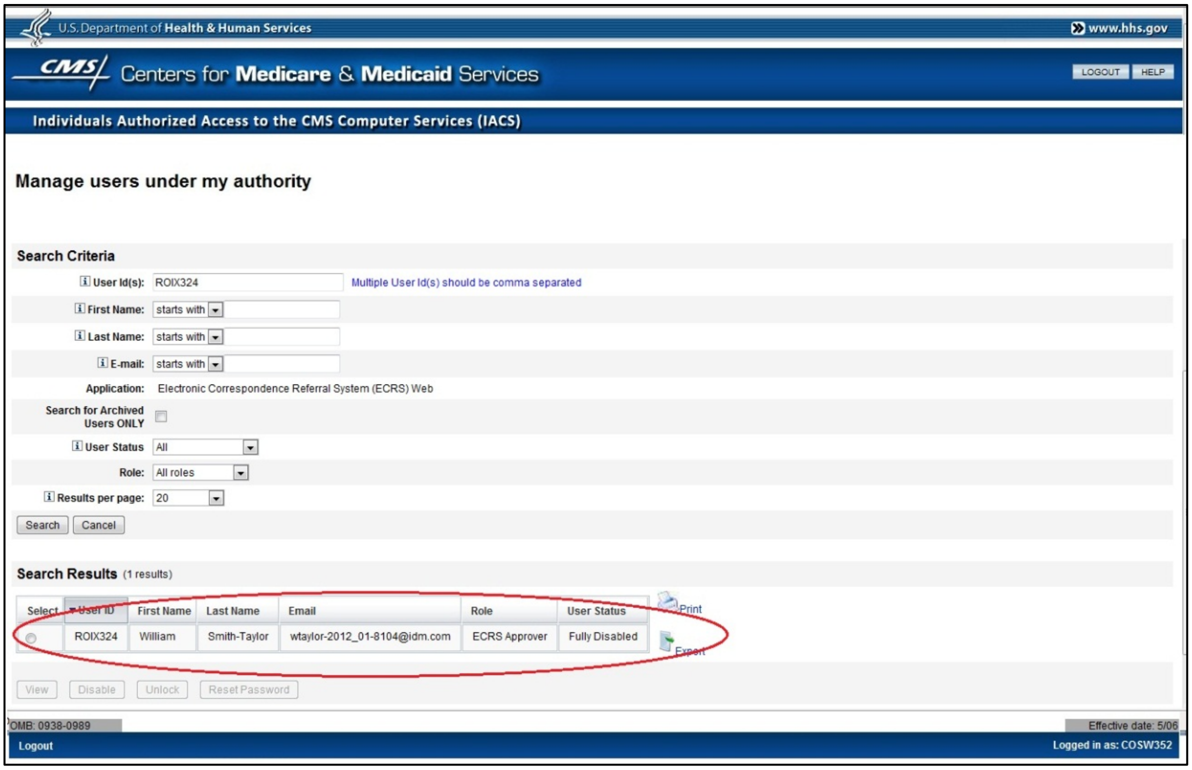
Ok
OMB: 0938-0989
Effective date: 5/0
Logout
Logged in as: UBWO623

Figure 61: Disable Account Acknowledgement Screen

The **Disable Account Acknowledgement** screen will display a message that the account was disabled successfully.

Action: Select the ***OK*** button at the bottom of the screen.

After the Helpdesk user selects ***OK***, the screen will refresh to the ***Search Results*** on the **Manage users under my authority** screen. The search results will display the user's status as 'Fully Disabled' under the *User Status* column, as illustrated in Figure 62.


U.S. Department of Health & Human Services
www.hhs.gov
CMS
Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

Search Criteria

User Id(s):	ROIX324 Multiple User Id(s) should be comma separated
First Name:	starts with
Last Name:	starts with
E-mail:	starts with
Application:	Electronic Correspondence Referral System (ECRS) Web
Search for Archived Users ONLY	□
User Status	All
Role:	All roles
Results per page:	20

Search Cancel

Search Results (1 results)

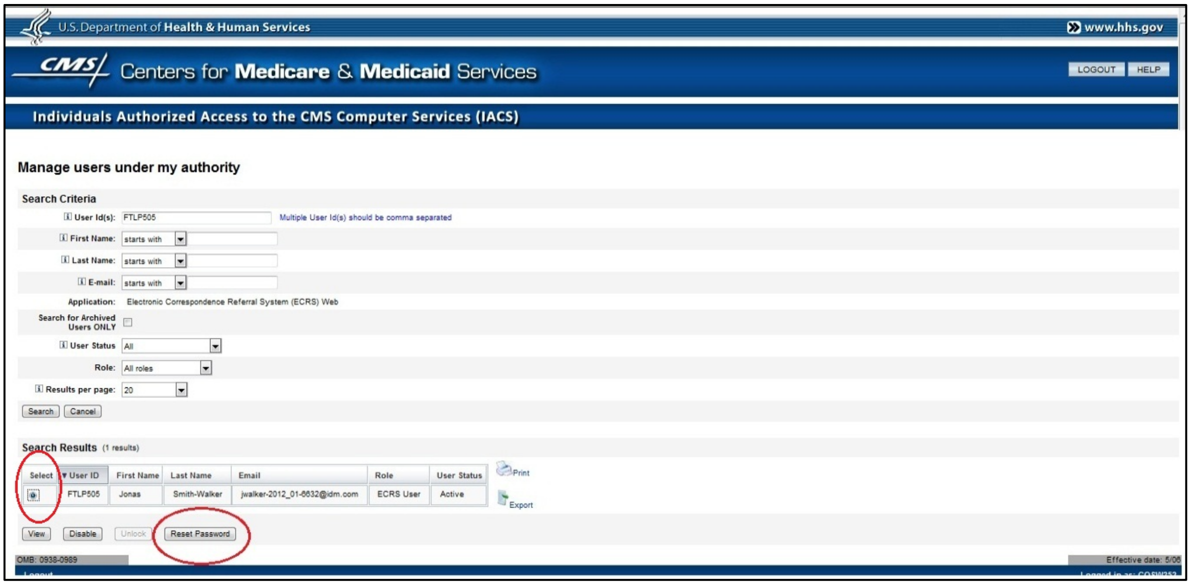
Select	User ID	First Name	Last Name	Email	Role	User Status
○	ROIX324	William	Smith-Taylor	wtaylor-2012_01-8104@idm.com	ECRS Approver	Fully Disabled

Figure 62: Manage users under my authority Screen – Shows User (Fully Disabled)

13.4.3 Reset User Password

Helpdesks can reset the password for user accounts within their scope of responsibility by using the ***Reset Password*** button from the **Manage users under my authority – *Search Results*** screen. Once the password is reset, the user will receive an E-mail notification with the password pattern for the user. IACS will require the user to enter the User ID and password pattern and change the password to a new password at the next login.

Action: From the **Manage users under my authority** screen, select the radio button to the left of the user record, as illustrated in Figure 63.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

Search Criteria

User Id(s):	FTLP505 Multiple User Id(s) should be comma separated
First Name:	starts with
Last Name:	starts with
E-mail:	starts with
Application:	Electronic Correspondence Referral System (ECRS) Web
Search for Archived Users ONLY	□
User Status	All
Role:	All roles
Results per page:	20

Search Results (1 results)

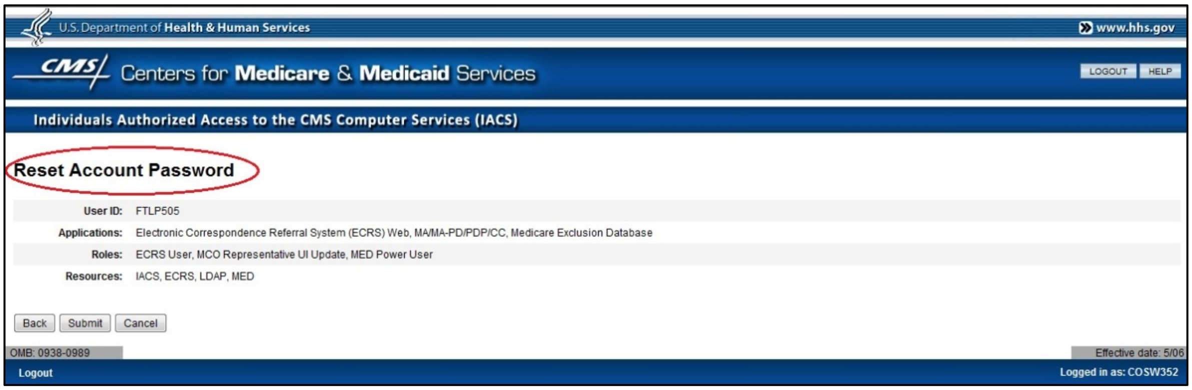
Select	▼User ID	First Name	Last Name	Email	Role	User Status
●	FTLP505	Jonas	Smith-Walker	jwalker-2012_01-6632@idm.com	ECRS User	Active

Figure 63: Manage users under my authority Screen – Reset Password Option

Action: Select the ***Reset Password*** button.

The **Reset Account Password** screen will display, as illustrated in Figure 64.

Note: The ***Reset Password*** button will not be active when the user status is 'Fully Disabled'.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Reset Account Password

User ID:	FTLP505
Applications:	Electronic Correspondence Referral System (ECRS) Web, MA/MA-PD/PDP/CC, Medicare Exclusion Database
Roles:	ECRS User, MCO Representative UI Update, MED Power User
Resources:	IACS, ECRS, LDAP, MED

Back
Submit
Cancel
OMB: 0938-0989
Effective date: 5/06
Logout
Logged in as: COSW352

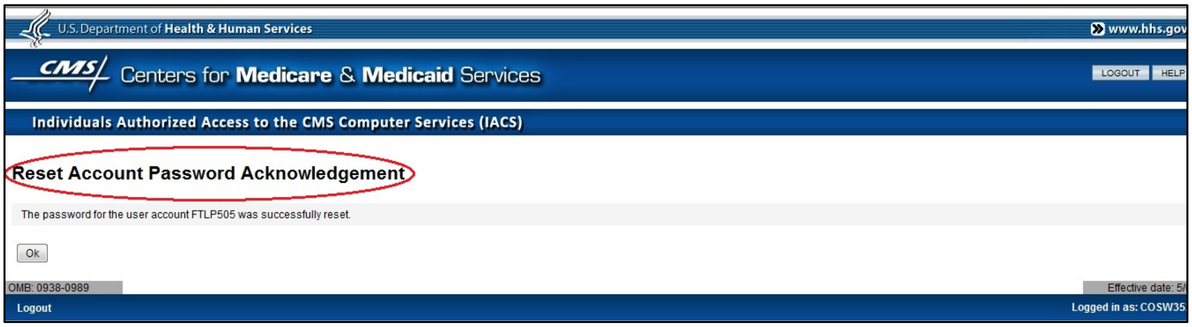
Figure 64: Reset User Password Screen

Action: Select the ***Submit*** button at the bottom of the screen.

The **Reset Account Password Acknowledgement** screen will display a message that the password was reset successfully, as illustrated in Figure 65.

If the user selects the ***Back*** button, the user will be returned to the **Manage users under my authority – *Search Results*** screen.

If the user selects the ***Cancel*** button, the user will be returned to the **My Profile** screen.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Reset Account Password Acknowledgement

The password for the user account FTLP505 was successfully reset.

Ok
OMB: 0938-0989
Effective date: 5/
Logout
Logged in as: COSW35

Figure 65: Reset Account Password Acknowledgement Screen

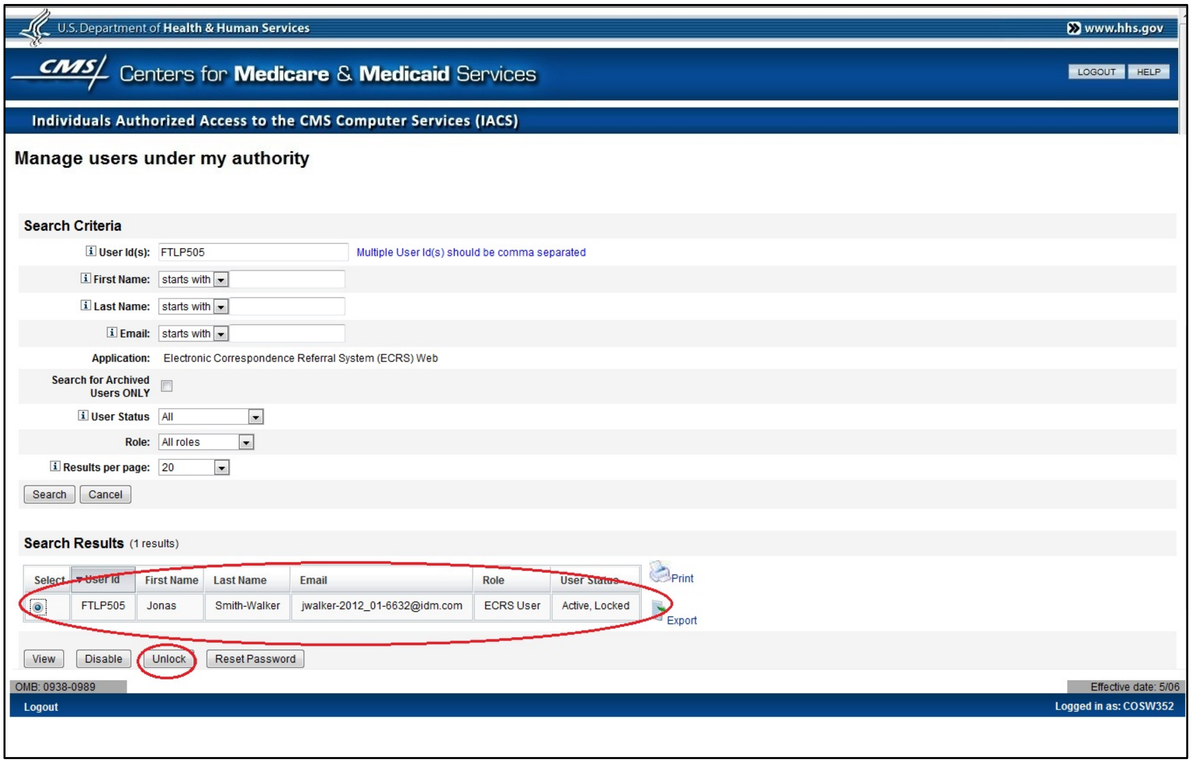
Action: Select the ***OK*** button at the bottom of the screen.

Note: An E-mail will be sent to the user with the password pattern for the user, once the reset password process has been completed.

After the Helpdesk selects ***OK,*** the screen will refresh to the ***Search Results*** on the **Manage users under my authority** screen, as illustrated in Figure 63.

13.4.4 Unlock User Account

Helpdesks can unlock a user's account within their scope of responsibility by using the ***Unlock*** button from the **Manage users under my authority – *Search Results*** screen. The Helpdesk needs to first verify that the user's account status is shown as 'Locked', as illustrated in Figure 66.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

Search Criteria

User Id(s):	FTLP505 Multiple User Id(s) should be comma separated
First Name:	starts with
Last Name:	starts with
Email:	starts with
Application:	Electronic Correspondence Referral System (ECRS) Web
Search for Archived Users ONLY	□
User Status	All
Role:	All roles
Results per page:	20

Search Cancel

Search Results (1 results)

Select	User Id	First Name	Last Name	Email	Role	User Status
●	FTLP505	Jonas	Smith-Walker	jwalker-2012_01-6632@idm.com	ECRS User	Active, Locked

Print
Export

View Disable Unlock Reset Password

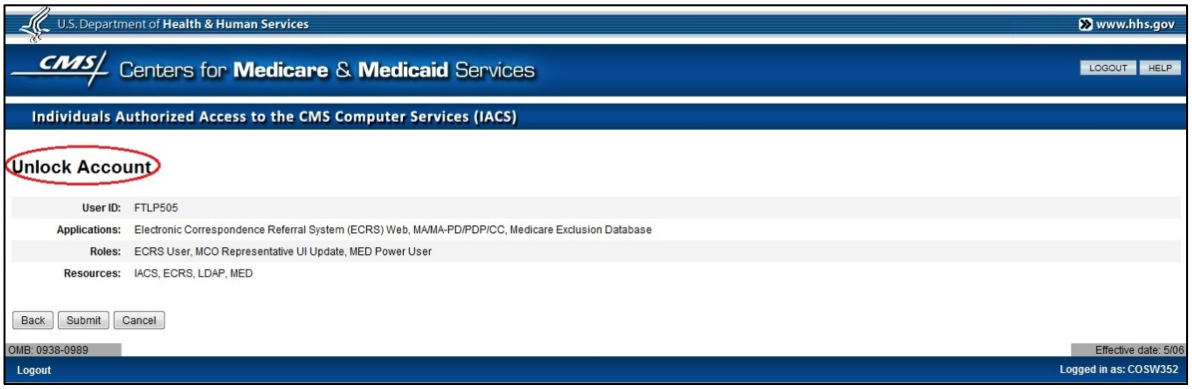
Figure 66: Manage users under my authority Screen – Unlock Option

Action: Select the radio button to the left of the user record you want to unlock.

Action: Select the ***Unlock*** button.

The **Unlock Account** screen will display, as illustrated in Figure 67.

Note: The ***Unlock*** button will not be active when the user status is not 'Locked' or 'Fully Disabled'.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

Unlock Account

User ID:	FTLP505
Applications:	Electronic Correspondence Referral System (ECRS) Web, MA/MA-PD/PDP/CC, Medicare Exclusion Database
Roles:	ECRS User, MCO Representative UI Update, MED Power User
Resources:	IACS, ECRS, LDAP, MED

Back Submit Cancel

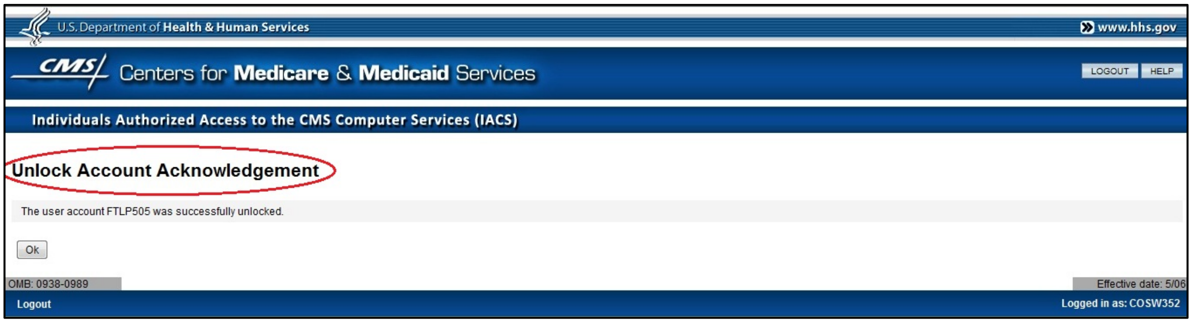
OMB: 0938-0989
Effective date: 5/06
Logout
Logged in as: COSW352

Figure 67: Unlock Account Screen

Action: Select the ***Submit*** button at the bottom of the screen.

If the user selects the ***Back*** button, the user will be returned to the **Manage users under my authority – *Search Results*** screen.

If the user selects the ***Cancel*** button, the user will be returned to the **My Profile** screen.



U.S. Department of Health & Human Services

www.hhs.gov

Centers for Medicare & Medicaid Services

Individuals Authorized Access to the CMS Computer Services (IACS)

Unlock Account Acknowledgement

The user account FTLP505 was successfully unlocked.

OMB: 0938-0989

Effective date: 5/06

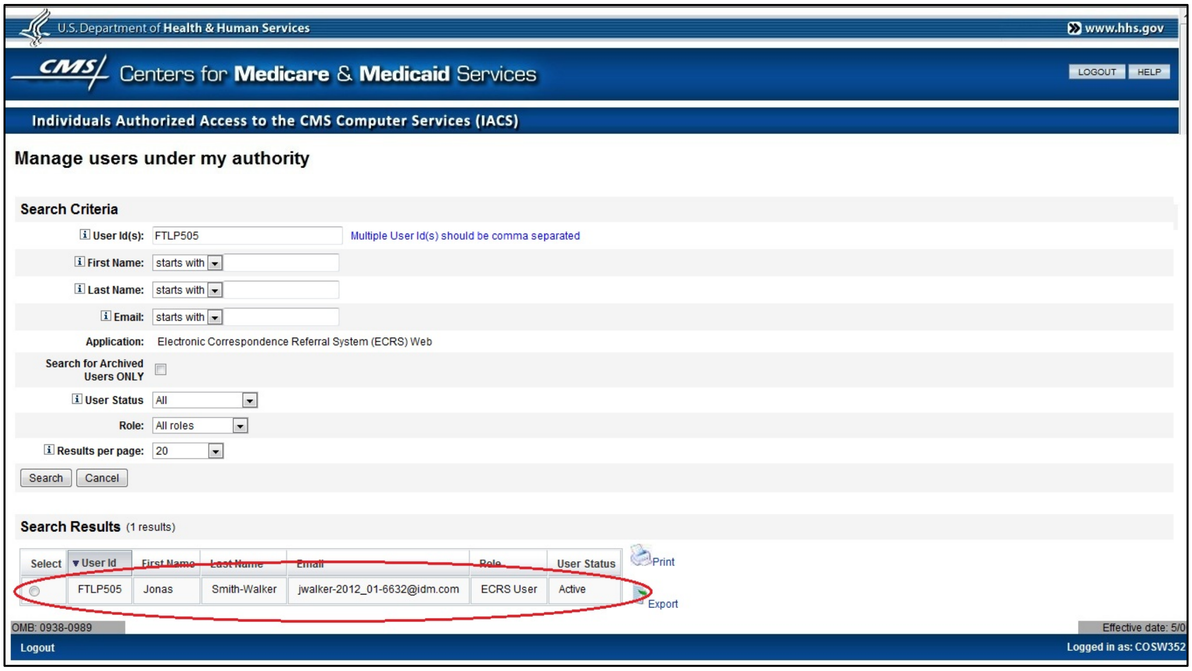
Logged in as: COSW352

Figure 68: Unlock Account Acknowledgement Screen

The **Unlock Account Acknowledgement** screen will display a message that the account was unlocked successfully, as illustrated in Figure 68.

Action: Select the ***OK*** button at the bottom of the screen.

After the Helpdesk selects ***OK,*** the screen will refresh to the ***Search Results*** on the **Manage users under my authority** screen. The search results will display the user's status as 'Active' under the *User Status* column, as illustrated in Figure 69.



U.S. Department of Health & Human Services

www.hhs.gov

Centers for Medicare & Medicaid Services

Individuals Authorized Access to the CMS Computer Services (IACS)

Manage users under my authority

Search Criteria

User Id(s):	FTLP505	Multiple User Id(s) should be comma separated
First Name:	starts with	
Last Name:	starts with	
Email:	starts with	
Application:	Electronic Correspondence Referral System (ECRS) Web	
Search for Archived Users ONLY	□	
User Status	All	
Role:	All roles	
Results per page:	20	

Search Results (1 results)

Select	User Id	First Name	Last Name	Email	Role	User Status
○	FTLP505	Jonas	Smith-Walker	jwalker-2012_01-6632@idm.com	ECRS User	Active

OMB: 0938-0989

Effective date: 5/0

Logged in as: COSW352

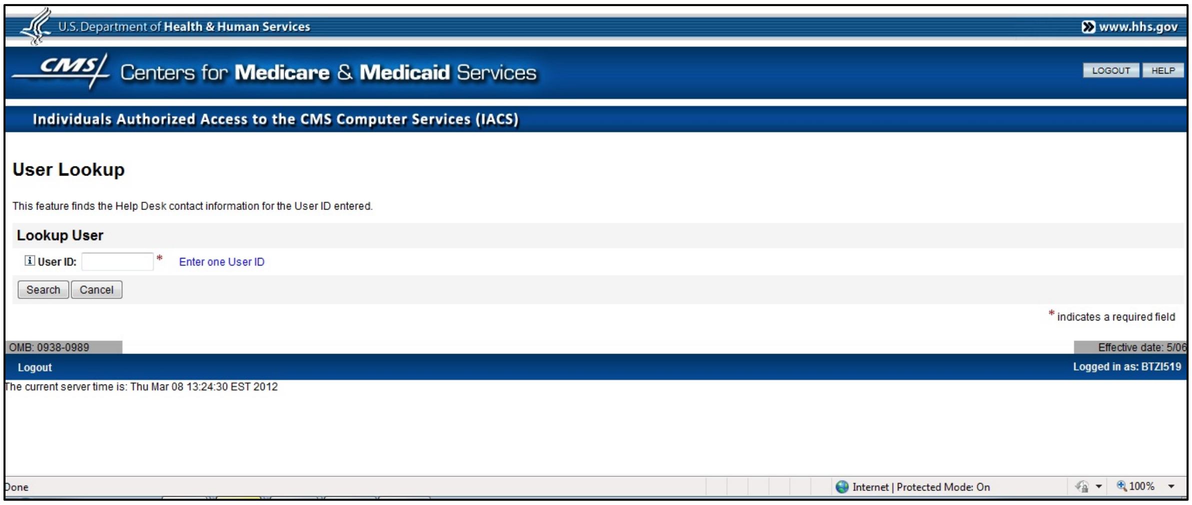
Figure 69: Manage users under my authority Screen – Shows User (Active)

14.0 Using User Lookup

The **User Lookup** feature is available to all users with the help desk role. These users will be able to use this feature to find the application's Help Desk contact information for any IACS user.

Action: Select the User Lookup hyperlink on the **My Profile** screen.

The **User Lookup** screen will display, as illustrated in Figure 70.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

User Lookup

This feature finds the Help Desk contact information for the User ID entered.

Lookup User

User ID: * Enter one User ID

* indicates a required field

OMB: 0938-0989 Effective date: 5/06

Logged in as: BTZI519

The current server time is: Thu Mar 08 13:24:30 EST 2012

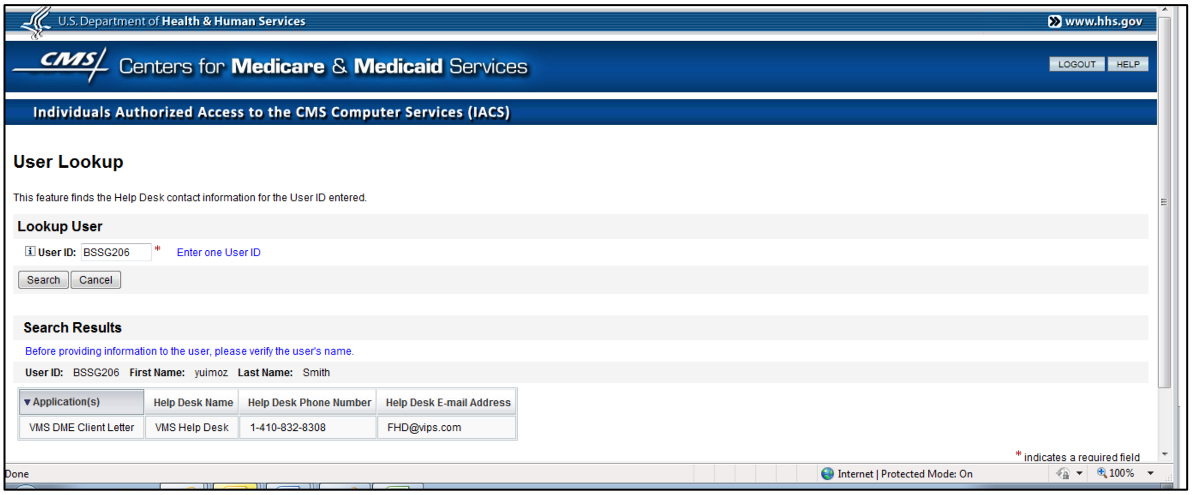
Done
Internet | Protected Mode: On
100%

Figure 70: User Lookup Screen

Action: Enter a User ID in the *User ID* field.

Action: Select the ***Search*** button.

The screen will refresh and the **Search Results** will display at the bottom of the screen, as illustrated in Figure 71.



U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
LOGOUT
HELP
Individuals Authorized Access to the CMS Computer Services (IACS)

User Lookup

This feature finds the Help Desk contact information for the User ID entered.

Lookup User

User ID: BSSG206 * Enter one User ID

Search Results

Before providing information to the user, please verify the user's name.

User ID: BSSG206 First Name: yuimoz Last Name: Smith

▾Application(s)	Help Desk Name	Help Desk Phone Number	Help Desk E-mail Address
VMS DME Client Letter	VMS Help Desk	1-410-832-8308	FHD@vips.com

* indicates a required field

Figure 71: User Lookup Search Results

Notes:

- The user will receive the 'No Information is available' message if one of the following conditions occur:

    1. The User ID may be typed incorrectly.

    2. The user account may be archived.

    3. The User ID is not associated with any application; for instance, the User ID may be for an IACS Administrator.

- The system will not be able to return the Help Desk contact information for a user without roles in his profile. The search will return the user name and the message that the user does not have a role.

15.0 IACS User Account Life Cycle

This section explains how IACS manages the life cycle of a user's account and enforces the CMS security policy.

15.1 Password Expiration

In compliance with the CMS security policy, IACS passwords are required to be changed at least every 60 days. This security requirement is also driven by federal regulation. Section 8.1 describes the procedures to change the password.

A user that has not changed the password in over 60 days will be prompted to do so at the next login.

15.2 60 Day Inactivity – Disable Account

In compliance with CMS security policy, IACS automatically disables any user that has not logged into either their application or IACS for 60 days or more. Once the user's account has been disabled, the user will not be able to access the CMS application. The user will be able to re-activate his account the next time he logs in to IACS. The user will be prompted to answer the Security Questions and the Authentication Questions. Once IACS identifies the user as a valid IACS user, he will be asked to change the password. Section 8.5 describes the procedures to re-activate the account.

15.3 Archiving Accounts

Archiving is the process of removing a user's account information from the IACS system. If the user attempts to log in to IACS after his account has been archived, a message will appear on screen that his account cannot be found. A user's IACS account will be automatically archived only under the following circumstances:

- Certification failure
- MA/MA-PD/PDP/CC users without contracts for 60 days.

15.3.1 Archiving Accounts Due to Certification Failure

IACS users are required to annually certify their continued need to access CMS applications. The user will receive an advisory E-mail 45 days prior to the Annual Certification date. The user will have 45 days to respond to the Certification request. After submitting the Annual Certification request, the Approver will have at least 30 days to approve or reject the certification request.

A user's IACS account will be archived for the following reasons:

- A user failed to submit an Annual Certification request within the time frame.
- A user submitted the Certification request and no action was taken by the Approver within the time frame.
- A user's Certification request was rejected.

If the user attempts to log in to IACS after the account has been archived, a message will appear stating that the account cannot be found.

Notes:

- The user's account will only be archived if there are no approved roles assigned to the account. For a user with multiple roles, if only one role is approved, the rejected role will be removed from the user's profile, and the user's account will not be archived.
- A user must use the New User Registration process to establish a new IACS account, once the account has been archived.

15.3.2 Archived Accounts for Users Without a Contract for 60 Days

The following MA/MA-PD/PDP/CC Application users will have their IACS user account archived if they do not have any contracts associated with their profile for 60 days or longer and they do not have any other IACS roles. The user will be sent an E-mail outlining the situation and provide instructions on what the user should do to maintain the IACS account.

- MA Submitter
- PDP Submitter
- MA Representative
- PDP Representative
- EPOC
- POSFE Contractor
- MMP User
- NET Submitter
- NET Representative

- Report View
- MCO Representative UI Update

Note: If the user has any other IACS roles apart from the MA/MA-PD/PDP/CC Application roles in his profile and has no associated contracts for 60 days or longer, the MA/MA-PD/PDP/CC Application role will be removed, but his IACS user account will not be archived.

15.3.3 Submitting a Request to Manually Archive a User's Account

IACS user accounts can be manually archived by an IACS Administrator for a security violation or when an employee no longer works in a capacity that requires an IACS account.

When a user's account has to be manually archived, a Service Request (SR) or Trouble Ticket (TT) has to be submitted to the IACS Administrator, requesting the IACS Administrator to archive the accounts manually.

The SR or TT must indicate one of the following reasons for requesting a manual archive:

- Security violation
- Access is no longer required

16.0 Troubleshooting & Support

The following section illustrates several types of error messages.

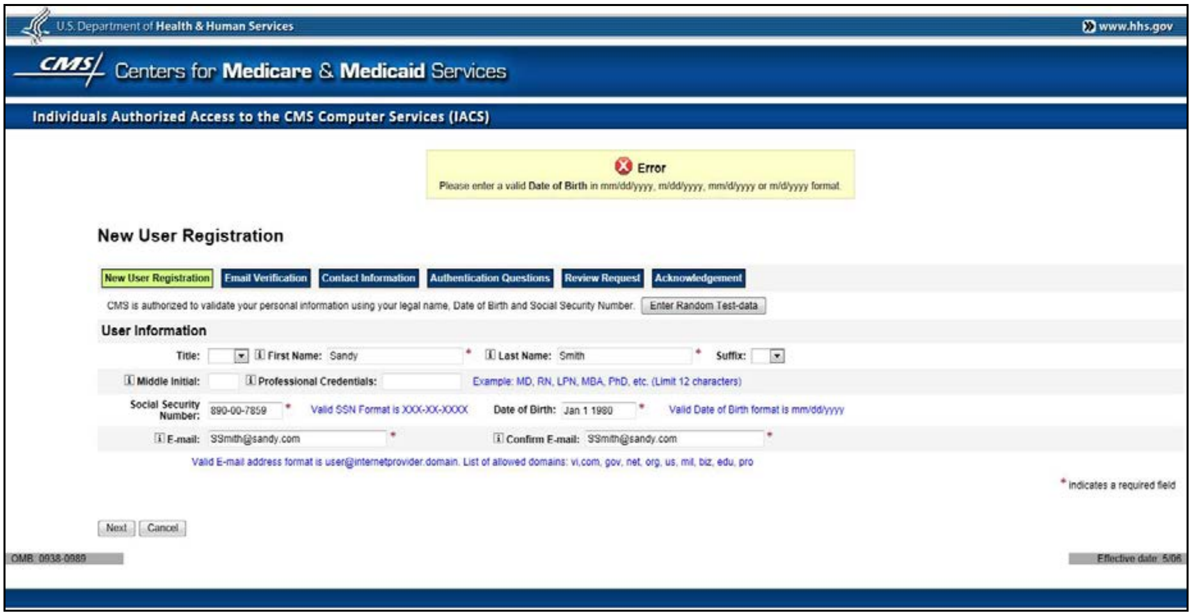
16.1 Error Messages

IACS provides a variety of on-screen error messages. These messages are self-explanatory and assist the user in resolving the error.

The following are some examples of the error and caution messages displayed.

If the ***User Information*** data fails validation, the **New User Registration** screen will refresh and display an error message above the ***User Information*** section, as illustrated in Figure 72.

If more than one ***User Information*** data fails validation, the system will display all the corresponding error messages at the same time. The user should fix all errors prior to proceeding to the next step.


U.S. Department of Health & Human Services
www.hhs.gov
CMS Centers for Medicare & Medicaid Services
Individuals Authorized Access to the CMS Computer Services (IACS)

Error
Please enter a valid **Date of Birth** in mm/dd/yyyy, m/dd/yyyy, mm/d/yyyy or m/d/yyyy format.

New User Registration

New User Registration
Email Verification
Contact Information
Authentication Questions
Review Request
Acknowledgement

CMS is authorized to validate your personal information using your legal name, Date of Birth and Social Security Number. [Enter Random Test-data]

User Information

Title: ▾ First Name: Sandy * Last Name: Smith * Suffix: ▾

Middle Initial: Professional Credentials: Example: MD, RN, LPN, MBA, PhD, etc. (Limit 12 characters)

Social Security Number: 890-00-7859 * Valid SSN Format is XXX-XX-XXXX Date of Birth: Jan 1 1980 * Valid Date of Birth format is mm/dd/yyyy

E-mail: SSmith@sandy.com * Confirm E-mail: SSmith@sandy.com *

Valid E-mail address format is user@internetprovider.domain. List of allowed domains: vi,com, gov, net, org, us, mil, biz, edu, pro

* indicates a required field

[Next] [Cancel]

OMB 0938-0989 Effective date 5/06

Figure 72: New User Registration Screen: Input Validation Failure Message

Action: Review the user information entered for correctness.

Action: Make any needed changes to the user information.

Action: Select the ***Next*** button to continue.

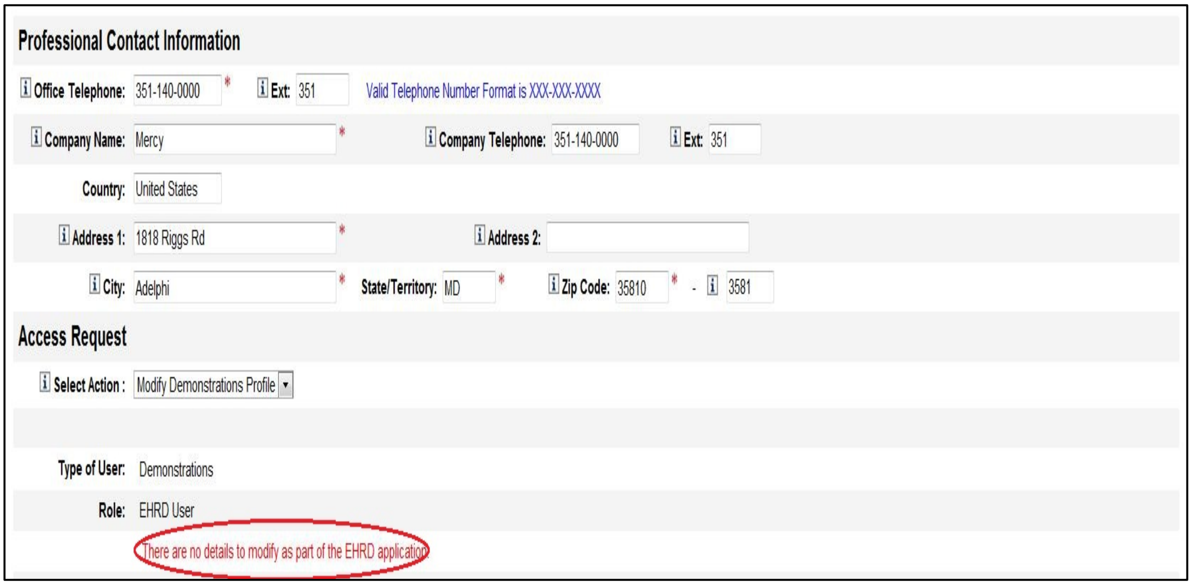
When the user selects the ***Next*** button, the system will attempt to validate the data entered by the user. If a problem is encountered again, the appropriate error messages will appear on the screen as shown in the example above.

If the information entered is validated successfully, the next screen will display.

IACS provides on-screen cautions and warnings to help guide users through procedures that require specific data formatting or to alert the user before finalizing an action.

Caution and Warning messages are presented in a variety of formats: as a text warning message at the top of the active screen, as information text on the screen where an issue has been identified, and as a caution message which will require the user’s action.

Additional examples of caution and warning messages are shown below.



Professional Contact Information

Office Telephone: 351-140-0000 * Ext: 351 Valid Telephone Number Format is XXX-XXX-XXXX

Company Name: Mercy * Company Telephone: 351-140-0000 Ext: 351

Country: United States

Address 1: 1818 Riggs Rd * Address 2:

City: Adelphi * State/Territory: MD * Zip Code: 35810 * - 3581

Access Request

Select Action : Modify Demonstrations Profile

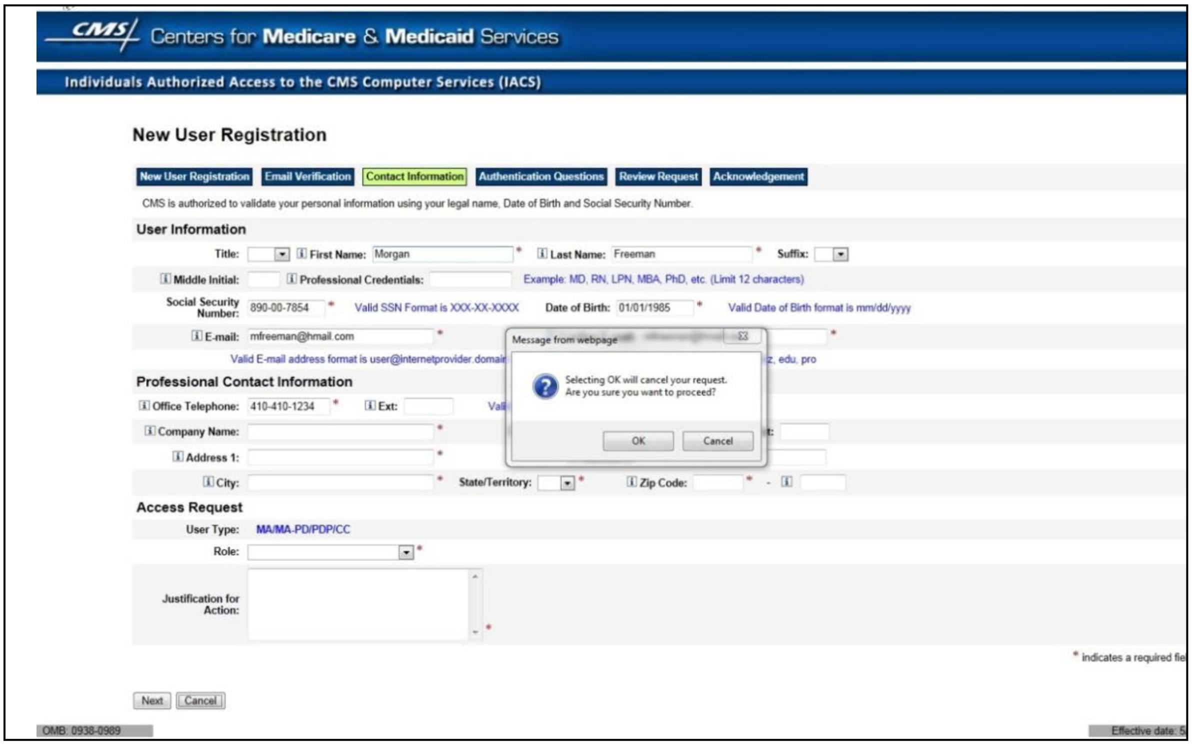
Type of User: Demonstrations

Role: EHRD User

There are no details to modify as part of the EHRD application

Figure 73: Information Message

The message shown at the bottom of Figure 73 notifies the user that the option selected cannot currently be used.



Centers for Medicare & Medicaid Services

Individuals Authorized Access to the CMS Computer Services (IACS)

New User Registration

New User Registration | Email Verification | Contact Information | Authentication Questions | Review Request | Acknowledgement

CMS is authorized to validate your personal information using your legal name, Date of Birth and Social Security Number.

User Information

Title: First Name: Morgan * Last Name: Freeman * Suffix:

Middle Initial: Professional Credentials: Example: MD, RN, LPN, MBA, PhD, etc. (Limit 12 characters)

Social Security Number: 890-00-7854 * Valid SSN Format is XXX-XX-XXXX Date of Birth: 01/01/1985 * Valid Date of Birth format is mm/dd/yyyy

E-mail: mfreeman@hmail.com *

Valid E-mail address format is user@internetprovider.domai z, edu, pro

Message from webpage

Selecting OK will cancel your request.
Are you sure you want to proceed?

OK Cancel

Professional Contact Information

Office Telephone: 410-410-1234 * Ext: Vali

Company Name: *

Address 1: *

City: * State/Territory: * Zip Code: * -

Access Request

User Type: MA/MA-PD/PDP/CC

Role: *

Justification for Action: *

* indicates a required fie

Next Cancel

OMB: 0938-0989 Effective date: 5

Figure 74: Caution Message

The message shown in Figure 74 cautions the user that the user's action will cancel the registration. The user selects the ***OK*** button to confirm the action or selects the ***Cancel*** button to continue with the registration process.

17.0 Frequently Asked Questions

1. *I registered and was approved as a PQRS Submitter for the PQRS/eRx application without associating to an organization. How can I add the organization to my profile?*

   To associate to an organization after you have been approved, you will need to disassociate your current role and then request the PQRS Submitter role again. When you request the PQRS Submitter role, select the radio button **option "I want to associate to an Organization"**. Once selected, search and associate to the organization you desire.

2. *My password was reset by the Help Desk; however, I am still unable to log in. What password should I use?*

   Once your password is reset, you will receive an E-mail with a one-time password. Use your IACS User ID and the password received in the E-mail to log in. After a successful login, you will be prompted to change the password in accordance with the password policy.

3. *How can I register as a PS&R/STAR or a PQRS/eRx Security Official for an existing organization?*

   To register as a Security Official for an existing organization for PS&R/STAR and PQRS/eRx Applications, choose the *Security Official* role from the *Role* drop-down list. You will see the following options display on the screen:

   - Create an organization
   - Associate to an existing organization

   Select the "***Associate to an Existing Organization****"* option. Once selected, search and associate to the organization you desire. Organizations can only have one Security Official. If the organization you have chosen already has a Security Official, you will be prompted to confirm the action. Your request will be subject to approval and once approved, you will be the Security Official for the selected organization.

4. *As an HPG user, how can I change my Submitter ID?*

   IACS does not allow an HPG user to modify the Submitter ID. You will need to contact the MCARE Help Desk with your request, who in turn, will open a Service Request directed to the IACS Administrators to modify the Submitter ID. Refer to Section 18.0 for Help Desk contact details.

5. *As the MCARE Help Desk, how can I modify the Submitter ID for an HPG User?*

   As the MCARE Help Desk, you are not authorized to modify a user's Submitter ID. Only the IACS Administrators have the capability to add or modify the Submitter ID. You should open a Service Request directed to the IACS Administrators with the

Submitter ID information. If your intention is to remove the Submitter ID from an HPG User's profile, then you could do that by using the **Manage users under my authority** function.

6. *I need to change my name and/or date of birth. I am unable to modify this information using the Modify User/Contact Information hyperlink. How can I modify my personal information?*

   Legitimate changes to the First Name, Last Name, and/or Date of Birth will require a Service Request. You should contact your application Help Desk, who in turn, will submit the Service Request to the IACS Administrator to modify your personal information. Refer to Section 18.0 for Help Desk contact details.

7. *As a user with the help desk role, how do I handle requests from users to change their First Name, Last Name, or Date of Birth?*

   Users cannot modify their First Name, Last Name, and Date of Birth fields in their IACS user profile due to security reasons. The help desk role does not have the capability to modify the user's profile; only the IACS Administrators have the capability to modify the user information mentioned above. You should open a Service Request to the IACS Administrators with the user's request. IACS Administrators will be able to edit the user's profile and modify the requested information.

8. *I modified my profile recently and added an additional role. Now, I am required to re-certify for this role. Why is this happening so soon?*

   The date for Annual Certification is determined by the date you were issued an IACS ID and not by the date you modified your profile to add the new role. Therefore, getting a new role assigned any time before your Annual Certification due date will still require you to certify for all roles in your profile as of the certification date. For example, if your IACS ID was created on July 1, your Annual Certification will be due on July 2 of the following year; if a new role was added to your profile prior to July 2 then all the roles in your profile, including the new role, will be subject to certification.

9. *When I submit a request for Annual Certification, I am alerted by a message stating that my request cannot be processed. Since IACS prevents me from submitting my request, how can I ensure that my roles are certified?*

   You are seeing a warning message because you have one or more roles in one of the following applications: COB, CSR, MA/MA-PD/PDP/CC, PQRS/eRx or PS&R/STAR Applications and one of these roles does not have an Approver defined in the system. Therefore, IACS will not have a way to route your certification request for approval and your request for certification will remain unprocessed. Please contact your Help Desk for further instructions. Refer to Section 18.0 for Help Desk contact details.

   Note: In the case of a user having multiple roles in PQRS/eRx or PS&R/STAR Applications and one of those roles do not have an Approver, the certification request will still remain unprocessed for all the roles.

For COB, CSR, MA/MA-PD/PDP/CC Applications, IACS allows users to submit certification requests when at least one Approver has been found for an item in the certification request. Refer to Frequently Asked Questions 27 and 28 for further information.

10. *When I submit a request for Annual Certification, the message on the screen states that there are no contracts associated with my IACS account. What do I need to do?*

    Your Annual Certification request cannot be processed when there are no contracts associated with your role. To retain your IACS account, you will need to request and be approved for a contract before your certification due date. If you choose to take no action before your certification due date, your IACS account will be archived.

11. *When I submit a request for Annual Certification, the message on the screen states that the IACS account has no call centers. What do I need to do?*

    Your Annual Certification request cannot be processed because your IACS account requires the role to be associated with a call center. To retain your IACS account you will need to request a call center, and be approved for an association with that call center, before your certification due date. If you choose to take no action before your certification due date, your IACS account will be archived.

12. *When I submit a request for Annual Certification, the message on the screen states that there are no roles assigned to my IACS account. What do I need to do?*

    Your Annual Certification request cannot be processed because your IACS account requires a role. To retain your IACS account, you will need to request a role and be approved for that role before your certification due date. If you choose to take no action before your certification due date, your IACS account will be archived.

13. *I have a MA Submitter role. Why am I not able to log in to IACS using my IACS User ID /Password?*

    Certain MA/MA-PD/PDP/CC Application users who do not have any contracts associated with their profile for 60 days and do not have any other application roles in IACS will be archived by the system by the 61st day. Since you have a MA Submitter role, your account could have been archived. Refer to Section 15.3.2 for further information. Once an account is archived, you must go through New User Registration to establish a new IACS account.

14. *I have a MA Submitter role and an ECRS User role. Why am I not able to see my MA Submitter role displayed on my View Profile screen?*

    Certain MA/MA-PD/PDP/CC Application users who do not have any contracts associated with their profile for 60 days and have other application roles in IACS, will have their MA/MA-PD/PDP/CC Application role removed by the system on the 61st day. Since you are a MA Submitter, your role could have been removed. You will have to request the MA Submitter role again using the **Modify Account Profile** function. Refer to Section 15.3.2 for additional information on the MA/MA-PD/PDP/CC 60-day contract requirement.

15. *As a PS&R Security Official, how do I modify the CCNs associated with my organization?*

    A PS&R Security Official can modify the CMS Certification Numbers (CCN) associated with his organization as part of profile modification. To modify the CCN you should follow the below steps:

    1. From the **Modify Account Profile** screen, select the Modify PS&R/STAR Profile option from the *Select Action* drop-down list.

    2. From the *My Current Access Profile* table, select the View/Edit organization details option from the *Action* drop-down list.

    3. The **Organization Information** with the *CMS Certification Number* field will display.

    4. Modify the *CMS Certification Number* field entry as desired. Enter the justification reason and select the ***Next*** button to continue with completing the profile modification.

       Note: The modified list of CMS Certification Numbers in the *CMS Certification Number* field will replace the previous list of CMS Certification Numbers associated with that organization once it is approved by the PS&R/STAR Helpdesk.

16. *As the Help Desk, can I fully disable a user who has more than one application role?*

    Yes. One of the functions given to a user with the help desk role is the ability to fully disable a user under the scope of your responsibility, even if the user has roles in other applications.

    Helpdesks will be able to perform this function using the **Manage users under my authority** help desk function. The disable action will disable the user for all applications.

    The Helpdesk user will receive a warning notice that the user will be disabled.

    The **Manage users under my authority** help desk function warns the Helpdesk user by displaying a message stating that the user has roles in other applications and the disable action will disable the user in all those applications. If the Helpdesk proceeds with the action, IACS will fully disable the user and send an E-mail notification to the other Application Helpdesks.

17. *I have not logged in to IACS for more than 6 months. What steps do I need to take to enable my account?*

    CMS requires inactive accounts to be disabled. The account will be considered inactive if the user has not logged in for 60 days. The user’s account will be disabled and the user will be unable to access any application. The user will be able to re-activate his account by using IACS’s self-service function. Below are the steps the user should take:

1. Navigate to https://applications.cms.hhs.gov.

2. Select the Account Management hyperlink in the white space in the center of the screen or in the menu bar toward the top of the screen.

3. Select the My Profile hyperlink in the **Account Management** screen.

4. Accept the Terms and Conditions.

5. Log in using the User ID and Password.

6. When prompted, answer the Security Questions and Authentication Questions.

7. Change the Password.

If the user is not prompted to answer the Security Questions and Authentication Questions, then he must contact the application help desk, who in turn, should open a Service Request directed to the IACS Administrators to re-activate the account.

18. *As a PS&R/STAR Helpdesk, how can I view the CMS Certification Number (CCN) of the user's associated organization?*

The organization's CCN information can be found in the ***Other Info*** tab on the **View Profile** screen using the Manage users under my authority hyperlink. From the **Manage users under my authority** screen, use the search criteria to find the user. After execution of the search, select the user from the search results and select the ***View*** button. The **View Profile** screen – ***Identity*** tab will display. From the **View Profile** screen, select the ***Other Info*** tab to view the user's CCN(s) information.

19. *As the Help Desk, how can I add or remove roles for users under my scope of responsibility?*

As a user with the help desk role, you are not allowed to add or remove roles. IACS allows users to disassociate from their role using the **Modify Account Profile** function without the need for approval. Help desk functions that you can perform are search and view user accounts, reset passwords, unlock user accounts, and disable user accounts.

20. *Why is the 'Last Password Change Date' blank for some users in the PQRS User Report?*

The PQRS User Report will display the date the users last changed their password in the *Last Password Change* Date column. The *Last Password Change Date* column in the report will be blank for users with the following conditions:

1. A new user to IACS who has received his first time User ID/Password and has not changed his password.

2. An existing user requested a password reset within the first 60 days since his IACS User account has been established and has not logged in with the user's password pattern.

Note: The following fields in the PQRS User Report will be blank if the user exists only in the IPC resource and not in IACS: *User Status, Last Password Change Date, Create Date, and Last Certification Date*.

21. *I am a registered EPOC for the MA/MA-PD/PDP/CC Application. The request that I planned on approving is no longer in my Inbox. Why am I unable to see the pending request?*

    When an existing MA/MA-PD/PDP/CC Application user requests an additional MAMA role or a report access type modification, the request needs to be approved by all the approvers of the corresponding contracts in the user's profile.

    If one of the contracts was rejected by one of the corresponding approvers, then all the contracts associated with the request will be considered rejected. Therefore, the request will be removed from your Inbox. You will receive an E-mail notification that one of the EPOCs has rejected the request and no further action is required. This request has not modified the user's profile. The user will retain his existing roles and contracts.

22. *As a PS&R/STAR Helpdesk or PQRI Helpdesk, how can I promote a Backup Security Official of an organization to a Security Official?*

    You cannot promote a Backup Security Official to a Security Official of an organization. The Backup Security Official will need to request the Security Official role by modifying his profile. IACS routes the role request to the Helpdesk for approval. An organization can have only one Security Official. Following your approval, the Backup Security Official will no longer have his current role of Backup Security Official and will acquire the new role of Security Official for the organization.

    Note: End Users of a given organization can also request and acquire the role of Security Official of the organization upon Helpdesk approval.

23. *I am a SO for one organization and BSO for another organization. While attempting to disassociate users from my organization, I noticed that the Edit feature of the Manage users function does not display the same users that are in the search results. Why is this?*

    As a Security Official (SO) for the PS&R/STAR or PQRS/eRx applications, you have the capability to disassociate users in your organization from PS&R/STAR or PQRS/eRx applications. The SO role also allows you to view the users of other organizations. When you select the search criteria *All Organizations* and then select the ***Edit*** button, the screen will refresh with the list of users in your organization.

    Since you also have the Backup Security Official role for another organization, you will be able to view those users. The BSO role does not have the capability to disassociate users. Therefore, when selecting the ***Edit*** button on the **Manage users under my authority** screen, those users will not display.

24. *When I try to register, I get an error message saying the SSN is already in use. What should I do?*

    This message means that the SSN entered has an IACS account. First, validate that the SSN is typed correctly. If the SSN is correct, you may have an account. To verify this, use the ***Forgot Your User ID****?* feature on the **Login to IACS** screen or CMS web page.

    1. Go to https://applications.cms.hhs.gov.

    2. Navigate to the Account Management hyperlink.

    3. Select the Forgot Your User ID hyperlink.

    4. Enter *First Name*, *Last Name*, *Date of Birth*, *SSN*, and *E-mail*. After the information is validated, an E-mail will be sent to you with your User ID.

    If you are unable to retrieve your User ID, please contact your Help Desk for *assistance.*

25. *I am unable to complete the E-mail verification step. I have not received the E-mail with the Verification Code. What should I do?*

    Here are possible solutions to your problem.

    - Is the E-mail correct? Verify the E-mail address displayed on the **E-mail Address Verification** screen. If the E-mail is not correct, cancel your request and start over again.
    - If the E-mail you provided is correct, please check your Junk/Spam folder.
    - If the E-mail address that you entered is correct and you do not see the E-mail in the junk folder, please contact your E-mail Administrator for resolution.

26. *I am a MA/MA-PD/PDP/CC application EPOC approver and notice that a user has contracts that I did not approve. Why does this happen?*

    This happens when a user initiates a new contract request and a role request and one is approved before the other. The request you are reviewing is a snapshot of the user's profile at the time the request is made. Assume you are reviewing the role request; an approver has approved the additional contract request, while you are reviewing the role request. You will not know that the additional contract request was initiated and approved. Once the role request is approved, all approved contracts will be associated with the user's roles. If you determine that the user should not have a particular contract, as the EPOC, you can use the manage users function to remove the contract.

27. *When I try to submit my Annual Certification request for an MAPD application, I am getting the 'no approver found' message and I am unable to submit my Certification request. Why is this happening and what do I need to do?*

    Annual Certification requests for the MAPD applications MA/MA-PD/PDP/CC, COB and CSR can only be submitted when the appropriate approver(s) are available to process the entire request.

    At the time of your certification request, IACS determined that the entire request could not be processed because there were no approvers. For the MA/MA-PD/PDP/CC, COB or CSR applications, E-mails are sent to authorized personnel that will arrange to have an approver register for the contract(s), call center(s) or state in your profile. Once the approver has been approved, you will be able to submit your Annual Certification request.

    The request must be submitted prior to the certification due date. If you are not able to submit the certification request due to the approver not being available, you may request a 45 day extension. You will need to work with your CMS contact or organization to determine if this is an option.

28. *When I try to submit my Annual Certification request for an MAPD application, I am getting a message that an approver was not found for all of the items in my profile. I am given an option to continue or cancel. What should I do?*

    You are getting this message because you may have multiple items in your profile for MAPD applications, MA/MA-PD/PDP/CC, COB, or CSR, and an approver was not found for at least one item. The message also states that an authorized person has been notified to arrange for an approver to register.

    For instance, you may have two contracts and an approver was found for only one of the contracts. Your options are to:

    1. Submit the request. When approved, your profile will show the one approved contract. You will no longer have the contract that could not be approved. Once the approver for that contract has registered, you will be able to add the contract to your profile by using the **Modify Account Profile** feature on the **My Profile** screen.

    Or

    2. Cancel the request to return to the **My Profile** screen. You will be able to submit your Annual Certification request if an approver has been approved for the contract before you certification due date. When your Certification request is approved you will have both contracts in your profile.

    Keep in mind, if the Certification Request is not submitted prior to your certification due date, your IACS account will be archived.

29. *Where can I view the Gentran mailbox, contract number, agency name or COR name for a user with the MED User role in IACS?*

    The MED Help Desk and MED Approver will be able to view the Gentran mailbox information. The contract number, agency name and COR name can be viewed by the MED Help Desk.

    The **Manage users under my authority** feature for the MED Help Desk will display the information in the ***Other Info*** tab on the **View Profile** screen for the selected user.

    The **Manage users under my authority** feature for the MED Approver will display the Gentran mailbox information in the search results grid.

    The MED User will be able to view and edit the information using the **Modify Account Profile** feature. On the **Modify Account Profile** screen, the user selects the *Select Action: Modify Medicare Exclusion Data Profile* and then selects the *Action: View/Edit Gentran Mailbox* to view or edit the information.

30. *I have an EPOC role and I would like to register for another MA/MA-PD/PDP/CC role. I am unable to disassociate from my EPOC role. How can the EPOC role be removed from my profile?*

    You must remove all contracts from your profile, then submit a Service Request (SR) to IACS Administration to remove the role. Once the IACS Administrator removes the EPOC role from your profile, you will be able to use the **Modify Account Profile-Add Application** option to request another role. Please note, any account without contracts for 60 days will be archived.

31. *How can a MA/MA-PD/PDP/CC user register for a contract that has been terminated?*

    Terminated contracts are removed from a user’s profile 60 days after the contract’s effective termination date. If a user needs to have one or more terminated contracts added to their user profile, the CMS MAPD Business Owner will have to submit a Service Request (SR) to IACS Administration. The SR must include the terminated Plan Contract Number(s), PDE Mailbox Number(s) and/or RAPS Mailbox Number(s), the User ID, and a “Retain Until” date. The “Retain Until” date prevents the contract from being removed prior to the date specified.

18.0 CMS Applications Help Desks Support and Information

This section provides the Help Desk contact information for IACS supported applications.

Note: The Help Desk contact information is available on the CMS website ***Help Resources*** area of the **Account Management** screen or on the Help Resources link of the https://applications.cms.hhs.gov website.

Application	Help Desk	Contact	Hours of Operation
Bundled Payments EFT	Bundled Payments EFT Help Desk	BundledPayments@cms.hhs.gov	Monday - Thursday, 10am - 3pm EST
CMS Administration – Physician Value	PV Admin Helpdesk	QRUR@cms.hhs.gov 888-734-6433	
COB	MAPD Help Desk	800-927-8069 mapdhelp@cms.hhs.gov	Monday - Friday: 6am - 9pm EST
CPC	CPC Help Desk	800-381-4724 cpcisupport@telligen.org	Monday - Friday: 6am - 10pm EST Saturday: 8am - 12pm EST
CSP-MCSIS	MCSIS Help Desk	410-786-4727 mcsis_application_support@cms.hhs.gov	
CSR	MAPD Help Desk	800-927-8069 mapdhelp@cms.hhs.gov	Monday - Friday: 6am - 9pm EST
DMEPOS	CBIC Help Desk	877-577-5331 cbic.admin@palmettogba.com	
ECRS	EDI Help Desk	646-458-6740 ecrshelp@hmedicare.com	Monday - Friday: 8am - 5pm EST
esMD	esMD Help Desk	410-786-1352 Daniel.kalwa@cms.hhs.gov	Monday - Friday: 8am - 3pm EST
Gentran	IACS Administration	iacs_admin@cms.hhs.gov	
HETS UI	MCARE Help Desk	866-440-3805 mcare@cms.hhs.gov	
HPG	MCARE Help Desk	866-440-3805 mcare@cms.hhs.gov	
HSTP	HSTP Help Desk	410-786-6693 hstp_application_support@cms.hhs.gov	
Internet Server	IACS Administration	iacs_admin@cms.hhs.gov	
MACPro	MACPro Help Desk	410-786-2580 macpro_helpdesk@cms.hhs.gov	Monday - Friday: 9am - 5pm EST

Application	Help Desk	Contact	Hours of Operation
MARx UI	MAPD Help Desk	800-927-8069 mapdhelp@cms.hhs.gov	Monday - Friday: 6am – 9pm EST
MDR	MAPD Help Desk	800-927-8069 mapdhelp@cms.hhs.gov	6am - 9pm EST
MED	EUS Help Desk	866-484-8049 866-523-4759 TTY/TDD eussupport@cgi.com	7am - 7pm EST
Medicare Advantage/ Prescription Drug Plans	MAPD Help Desk	800-927-8069 mapdhelp@cms.hhs.gov	Monday - Friday: 6am – 9pm EST
myCGS	CGS DME JC Provider Call Center	1-866-270-4909 cgs.dme.mac.email.inquiries@cgsadmin.com	7:00am - 5:00pm Central Time
Novitasphere	Novitasphere Helpdesk	877-235-8073 websiteEDI@highmark.com	8:00am - 4:00pm EST Monday, Tuesday, Wednesday, Friday 8:00am – 2:00pm EST Thursday
PQRS/eRx	QNet Help Desk	866-288-8912 qnetsupport@sdps.org	6am - 6pm EST
PS&R/STAR	EUS Help Desk	866-484-8049 866-523-4759 TTY/TDD eussupport@cgi.com	7am - 7pm EST
PV/PQRS Registration System	PV Helpdesk	QRUR@cms.hhs.gov 888-734-6433	
The SPOT	FCSO Help Desk	1-904-791-6767 sspab@fcso.com	
VMS Client Letter	VMS Help Desk	410-832-8308 THD@vips.com	Monday - Friday 7am - 7pm EST

19.0 Glossary

The following definitions are provided for terms used or implied in this User Guide as well as relevant cross references to additional terms that are used within those definitions.

Term	Definition
CMS	The Centers for Medicare & Medicaid Services – the Health and Human Services agency responsible for Medicare and parts of Medicaid.
COB	Coordination of Benefits - Access to this application is restricted to the employees of Coordination of Benefits Contractor (COBC) only.
CPC	Comprehensive Primary Care (CPC) Initiative - The CPC Web Portal will serve as the main repository for Select Practices to access key resources, submit data surrounding the CPC Initiative milestones, and engage in systematic data sharing with participating Public and Private Health Care Payers.
DMEPOS	Durable Medical Equipment, Prosthetics, Orthotics & Supplies
ECRS	Electronic Correspondence Referral System - This application allows authorized users to fill out various online forms, electronically transmit requests for changes to existing Common Working File (CWF) Medicare Secondary Payer (MSP) information and inquiries concerning possible MSP coverage.
EDI	Electronic Data Interchange – refers to the exchange of routine business transactions from one computer to another in a standard format, using standard communications protocols.
Fully Disabled	The user status of ‘Fully Disabled’ denotes that a user has been manually disabled by the Helpdesk or by an IACS Administrator for security reasons. The disabled user is removed from all resources. A disabled user will not be able to log into any of the IACS administered applications, use IACS self-service features to reset the password or retrieve his IACS User ID. Only an IACS Administrator can enable a ‘Fully Disabled’ user.
HHS	The Department of Health and Human Services – a government agency that administers many of the “social” programs at the federal level dealing with the health and welfare of the citizens of the United States. HHS is the “parent” of CMS.
HIPAA	Health Insurance Portability And Accountability Act of 1996 – a Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. Also known as the Kennedy-Kassebaum Bill, the Kassebaum-Kennedy Bill, K2, or Public Law 104-191.

Term	Definition
Locked	The user status is set to 'Locked' when the user failed to provide the correct User ID and/or Password after three consecutive login attempts. A 'Locked' user will not be able to access IACS unless he is unlocked, but will still be able to log into any IACS administered applications for which he has access rights. Users can unlock their account using self-service features or by contacting the Help Desk to unlock the account.
Medicaid	A joint federal and state program that helps with medical costs for some people with low incomes and limited resources. Medicaid programs vary from state to state, but most health care costs are covered for those who qualify for both Medicare and Medicaid.
Medicare	A Federal health insurance program enacted in 1965 that is financed by a combination of payroll taxes, premium payments, and general Federal revenues. This program provides health insurance to people age 65 and over, those who have permanent kidney failure requiring dialysis or transplant, and certain individuals under 65 with disabilities.
NPI	National Provider Identifier (NPI) – a unique identification number for use in standard health care transactions. The NPI is issued to health care providers and covered entities that transmit standard HIPAA electronic transactions (e.g. electronic claims and claim status inquiries). The NPI fulfills a requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and was required to be used by health plans and health care clearinghouses in HIPAA standard electronic transactions by May 23, 2007. The NPI contingency period allowed health care providers and covered entities until May 23, 2008 to become fully compliant with the NPI rule.
Partially Disabled	A user status is shown as 'Partially Disabled' when the user has not logged into the system for more than 60 days. A 'Partially Disabled' user cannot log in to any application that he could previously access. A 'Partially Disabled' user can enable himself using the IACS self-service function or by contacting the Helpdesk.
SSA	Social Security Administration – the government agency that administers the social security program.
SSN	Social Security Number – a unique identification number assigned to individuals by the SSA.
Top of the Chain of Trust User	IACS uses a hierarchical system of approval for registration requests, profile modification requests, and annual certification requests referred to as the Chain of Trust. End User requests are approved by Approvers. Approvers are approved by Authorizers. Authorizers are approved by the Business Owner or their designee. Business Owners typically do not have an IACS User ID. Thus, Authorizers are referred to as Top of the Chain Users, since they are the last users in the chain who must have an IACS User ID.

20.0 Acronyms

This section defines acronyms used or referenced in this document.

Acronym	Definition
AO	Authorized Official
BAO	Backup Authorized Official
BPID	Bundled Payments Participant ID
BSO	Back-up Security Official
CBA	Competitive Bidding Area
CBIC	Competitive Bidding Implementation Contractor
CC	Cost Contract
CCN	CMS Certification Number
CHIP	Children’s Health Insurance Program
CMS	The Centers for Medicare & Medicaid Services
COB	Coordination of Benefits
COBC	Co-ordination of Benefits Contractor
CPC	Comprehensive Primary Care
CSP	Center for Strategic Planning
CSR	Customer Service Representative
CWF	Common Working File
DBidS	Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) Bidding System
DOB	Date of Birth
DME	Durable Medical Equipment
DME MAC	Durable Medical Equipment Medicare Administrative Contractor
DMEPOS	Durable Medical Equipment, Prosthetics, Orthotics & Supplies
ECRS	Electronic Correspondence Referral System
EDI	Electronic Data Interchange
EHR	Electronic Health Record
EPOC	External Point of Contact, Organizational IACS Approver
ECRS	Electronic Correspondence Referral System (ECRS)

Acronym	Definition
EST	Eastern Standard Time
EFT	Electronic Funds Transfer
esMD	Electronic Submission of Medical Documentation
EUS	External User Services
FCSO	The SPOT – First Coast Service Options' Internet portal
FI/Carrier/MAC	Fiscal Intermediary/Carrier/Medicare Administration Contractor
GUI	Graphical User Interface
HETS UI	HIPAA Eligibility Transaction System User Interface
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HPG	HIPAA Eligibility Transaction System Provider Graphical User Interface
HSTP	Health System Tracking Project
IACS	Individuals Authorized Access to the CMS Computer Services
ID	Identification
ID	Identifier
IP	Individual Practitioner
ISV	Internet Server
IT	Information Technology
IUI	Integrated User Interface
IVR	Interactive Voice Response
LSA	Local Service Administrator
MA	Medicare Advantage
MAC	Medicare Administrative Contractor
MACPro	Medicaid and CHIP Program System
MA/MA-PD/PDP/CC	Medicare Advantage/Medicare Advantage-Prescription Drug/Prescription Drug Plan/Cost Contracts
MA-PD	Medicare Advantage – Prescription Drug
MARx	Medicare Advantage and Prescription Drug
MARx UI	Medicare Advantage and Prescription Drug User Interface
MCARE	Medicare Customer Assistance Regarding Eligibility

Acronym	Definition
MCSIS	Medicaid and Children’s Health Insurance Program (CHIP) State Information Sharing System
MCO	Managed Care Organization
MDR	Medicaid Drug Rebate
MED	Medicare Exclusion Database
MEIC	The Medicare Eligibility Integration Contractor
MSP	Medicare Secondary Payer
NIST	National Institute of Standards and Technology
NPI	National Provider Identifier
PDE	Prescription Drug Event
PDP	Prescription Drug Plan
PECOS	Provider Enrollment, Chain and Ownership System
PII	Personally Identifiable Information
PTAN	Provider Transaction Access Number
POSFE	Point-of-Sale Facilitated Enrollment
PQRI	Physician Quality Reporting Initiative
PQRS	Physician Quality Reporting System
PQRS/eRx	Physician Quality Reporting System and E-Prescribing Incentive Programs
PS&R/STAR	Provider Statistical and Reimbursement / System Tracking for Audit and Reimbursement
PV	Physician Value
QRUR	Quality and Resource Use Report
RACF	Resource Access Control Facility
RAPS	Risk Adjustment Processing System
SO	Security Official
SR	Service Request
SSA	Social Security Administration
SSN	Social Security Number
SHIP	State Health Insurance Plans
SPAP	State Pharmacy Assistance Programs

Acronym	Definition
TIN	Taxpayer Identification Number
VMS	ViPS Medicare System

Appendix A IACS Application Role Approval Matrix

Bundled Payments EFT Application

The Bundled Payments EFT supports Bundled Payments for Care Improvement EFT Users.

Role	Approved By	Additional Information
Bundled Payments EFT Help Desk	Top of the Chain	This user’s role is an authorized representative of CMS that provides help desk assistance to Bundled Payments EFT users.
Bundled Payments EFT User	Bundled Payments EFT Help Desk	The user with this role is trusted with Care Improvement data file transfers for Bundled Payments for Care Improvement EFT users.

CMS Administration – Physician Value Application

CMS Administration – Physician Value provides help desk support for Group Practices and Individual Eligible Professionals users of the Physician Value – Physician Quality Reporting System.

Role	Approved By	Additional Information
PV Admin Helpdesk Approver	Top of the Chain	The user with this role provides help desk support for Group Practices and Individual Eligible Professionals users of the Physician Value – Physician Quality Reporting System.
PV CMS Administrator	PV Admin Helpdesk Approver	This user’s role is to view registration data through the administrative interface and view QRUR reports, drill down data and dash boards.
PV Helpdesk Tier1 User	PV Admin Helpdesk Approver	This user’s role is to search and view registration data through the PV-PQRS Admin interface.
PV Helpdesk Tier2 User	PV Admin Helpdesk Approver	This user’s role is to search and modify registration data and QRUR reports.
PV PQRS Registration System Reports User	PV Admin Helpdesk Approver	This user’s role is to access PV-PQRS Registration Statistical Reports.

COB Application

Access to the Coordination of Benefits (COB) is restricted to the employees of the Coordination of Benefit Contractor (COBC) only.

Role	Approved By	Additional Information
Authorizer	Top of the Chain	The user with this role is an employee of COB and is trusted with approving requests for the Approver and COB Helpdesk roles in IACS.
Approver	Authorizer	The user with this role is an employee of COB and will have the approval authority for all users of all COB organizations.
COB Helpdesk	Authorizer	The user with this role is an authorized representative of CMS who will provide help desk assistance to COB Application users.
User/Transmitter	Approver	The user with this role is trusted with transmitting batch files containing membership changes and health status corrections.

Comprehensive Primary Care (CPC) Initiative Application

The Comprehensive Primary Care (CPC) web portal allows Select Practices to submit and share data with participating Public and Private Health Care Payers.

Role	Approved By	Additional Information
CPC Support	Top of the Chain	The user with this role provides help desk assistance to CPC Application users. The CPC Support user functions as an Authorizer in IACS.
CPC Basic User	CPC Support	Users with this role include practices that are participating in the CPC Initiative. This role will provide access to online functionality and reports at the practice level.
CPC Market User	CPC Support	This role is limited to individuals at the participating payers in the CPC Initiative.
CPC CMMI User	CPC Support	This role is limited to CMS Innovation Center staff.
CPC Contractor - Operations Support	CPC Support	This role is limited to CPC contractors providing operational support to the CMS Innovation Center.
CPC Contractor - Learning and Diffusion	CPC Support	This role is limited to the CPC contractor providing education and outreach to practices participating in the CPC Initiative.
CPC Contractor - Evaluation	CPC Support	This role is limited to the CPC contractor providing an evaluation of the CPC Initiative to the CMS Innovation Center.

Role	Approved By	Additional Information
CPC Contractor - Payment	CPC Support	This role is limited to the CPC contractor who is providing the payment to the practices participating in the CPC Initiative. This role is not to be used by the payers in the various markets.

CSP-HSTP Application

The Health System Tracking Project (HSTP) application is a web portal for tracking and monitoring of activities, milestones, and results from the implementation of Health Reform legislation.

Role	Approved By	Additional Information
HSTP Helpdesk User	Top of the Chain	The user with this role will provide help desk assistance to CSP-HSTP Application users and functions as an Authorizer in IACS.
HSTP End User	HSTP Helpdesk Users	The user with this role is a staff member who is trusted to perform Medicare business for the application.

CSP-MCSIS Application

The Medicaid and Children’s Health Insurance Program, CHIP, State Information Sharing System, MCSIS, is a web-based application that is a single source for collecting and sharing Medicare, Medicaid and CHIP provider termination data.

Role	Approved By	Additional Information
MCSIS Helpdesk User	Top of the Chain	The user with this role will provide help desk assistance to CSP-MCSIS Application users and functions as an Authorizer in IACS.
MCSIS End User	MCSIS Helpdesk User	The user with this role is a staff member who is trusted to perform Medicare business for the application.

CSR Application

Community Based Organization/Customer Service Representative

Role	Approved By	Additional Information
Authorizer	Top of the Chain	The user with this role is trusted with approving requests for the Approver role.
Approver	Authorizer	The user with this role is trusted with approving requests for CSR users.

Role	Approved By	Additional Information
User	Approver	The user with this role is a customer service representative or staff member who is trusted to perform business for the organization.
Local Service Administrator (LSA)	Authorizer	The LSA role can only be requested by an existing IACS user with the CSR Approver role.

DMEPOS Bidding System (DBidS) Application

Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) Competitive Bidding Program Community - The DMEPOS Competitive Bidding Program Community is for suppliers submitting a bid for selected products in a particular Competitive Bidding Area (CBA).

Role	Approved By	Additional Information
DMEPOS Authorizer1	Top of the Chain	The user with this role is trusted with approving requests for the DMEPOS IT Help Desk role.
DMEPOS Authorizer2	Top of the Chain	The user with this role is trusted with approving requests for the CBIC Tier 1, CBIC Tier 2, or CBIC Input roles.
CBIC Tier 1	DMEPOS Authorizer2	The user with this role provides Tier 1 help desk assistance for the DMEPOS Application users.
CBIC Tier 2	DMEPOS Authorizer2	The user with this role provides Tier 2 help desk assistance for the DMEPOS Application users. The CBIC Tier 2 user can modify DMEPOS profiles for DMEPOS users within the scope of the user's responsibility.
Authorized Official (AO)	Auto Approved	The user with this role is an appointed official to whom the organization has granted the legal authority to enroll the organization in the Medicare program. To register for this role, the user must be listed on the CMS 855S Medicare Enrollment application as an Authorized Official. The AO creates the organization. Each organization can have only one AO.
Backup Authorized Official (BAO)	Authorized Official	The user with this role is an appointed official to whom the organization has granted the legal authority to enroll the organization in the Medicare program. To register for this role, the user must be listed on the CMS 855S Medicare Enrollment as an Authorized Official. The BAO is not a required role for an organization (PTAN).

Role	Approved By	Additional Information
End User	Authorized Official or Backup Authorized Official	The user with the End User role is trusted to input bid data. The End User cannot approve Form A or certify Form B. An organization (PTAN) can have one or more End Users.

ECRS Application

Electronic Correspondence Referral System (ECRS) Web - This application allows authorized users to fill out various online forms and electronically transmit requests for changes to existing Common Working File (CWF) Medicare Secondary Payer (MSP) information, and inquiries concerning possible MSP coverage.

Role	Approved By	Additional Information
ECRS HelpDesk	Top of the Chain	The user with this role will provide help desk assistance for the ECRS Application users and functions as an Authorizer in IACS.
ECRS Approver	ECRS HelpDesk	The user with this role is trusted with approving requests for the ECRS User role.
ECRS User	ECRS Approver	The user with this role is a staff member who is trusted to perform Medicare business for the application.

esMD Application

Electronic Submission of Medical Documentation (esMD)

Role	Approved By	Additional Information
esMD Help Desk	Top of the Chain	The user with this role will help users with access and/or password reset requests.
esMD Approver	esMD Help Desk	The user with this role will provide access to users requesting system access.
esMD Reports	esMD Approver	The user with this role will have access to esMD submission data.
esMD Admin	esMD Approver	The user with this role will have access to esMD data (OIDs & NPIs).

Gentran Application

Gentran only access. This registration link is for those users who have no association with any other application, but need Gentran mailbox access. If users need access to an application that requires Gentran, they must register for that application to get access to their Gentran mailbox.

Role	Approved By	Additional Information
Gentran Helpdesk	Top of the Chain	The user with this role will provide help desk assistance for the Gentran Application users and functions as an Authorizer in IACS.
Gentran Approver	Gentran Helpdesk	The user with this role is trusted with approving requests for the Gentran User role.
Gentran User	Gentran Approver	The user with this role is a staff member who is trusted to perform Medicare business for the application.

HETS UI Application

HIPAA Eligibility Transaction System User Interface - This is a pilot with registration restricted to those organizations that are pre-approved.

Role	Approved By	Additional Information
MCARE Help Desk	Top of the Chain	The user with this role will provide help desk assistance for the HETS UI and HPG applications and functions as an Authorizer in IACS.
Security Official (SO)	MCARE Help Desk	The Security Official represents the organization or facility in IACS. There can be two Security Officials at an organization or facility.
HETS Approver	Security Official	The user with this role is trusted with approving requests for the HETS User.
HETS User	HETS Approver or MCARE Help Desk	If a HETS Approver does not exist for an organization, the requests will be routed to the MCARE Help Desk.

HPG Application

HIPAA Eligibility Transaction System (HETS) Provider Graphical User Interface (GUI)

Role	Approved By	Additional Information
HPG User (*)	MCARE Help Desk	The user with this role is a staff member who is trusted to perform Medicare business for the application. HPG User with a Submitter ID other than P-type is associated with a Gentran mailbox.

* Users with this role should not attempt to register for Gentran separately.

Internet Server Application

Internet Server only access. This registration link is for those users who have no association with any other application listed on the CMS portal web page, but need Internet Server access. If you need access to an application that also requires Internet Server access, you must register for that application to get access.

Role	Approved By	Additional Information
Internet Server Help Desk	Top of the Chain	The user with this role will provide help desk assistance for the Internet Server Application users.
Internet Server Approver	Internet Server Help Desk	The user with this role is trusted with approving requests for the Internet Server User.
Internet Server User	Internet Server Approver	The user with this role is a staff member who is trusted to perform Medicare business for the application.

MA/MA-PD/PDP/CC Application

Medicare Advantage/Medicare Advantage - Prescription Drug/Prescription Drug Plan/Cost Contracts/ Medicaid State Agency

Role	Approved By	Additional Information
Authorizer	Top of the Chain	The user with this role is trusted with approving requests for the EPOC role.
IUI Authorizer	Top of the Chain	The user with this role is trusted with approving requests for the IUI Helpdesk, MAPD Helpdesk, and MAPD Helpdesk Admin roles.
State Authorizer	Top of the Chain	The user with this role is trusted with approving requests for the MA State/Territory, State Health Insurance Plans (SHIP), and State Pharmacy Assistance Programs (SPAP) approvers.
EPOC	Authorizer	The user with this role is trusted with approving end user requests as noted in the table.

Role	Approved By	Additional Information
MA State/Territory Approver	State Authorizer	The user with this role is trusted with approving requests and will not have access to MA Part D applications.
SHIP Approver	State Authorizer	The user with this role is trusted with approving requests and will not have access to MA Part D applications.
SPAP Approver	State Authorizer	The user with this role is trusted with approving requests and will not have access to MA Part D applications.
IUI Helpdesk	IUI Authorizer	The user with this role will be able to view all application screens and information, except for the Report Order screens.
MAPD Helpdesk	IUI Authorizer	The user with this role provides help desk assistance to MA/MA-PD/PDP/CC and CSR Application users.
MAPD Helpdesk Admin	IUI Authorizer	The user with this role provides administrative help desk assistance to the MA/MA-PD/PDP/CC and CSR Application users.
MA Representative	EPOC	The user with this role will be able to view application screens and all information for the periods during which the beneficiary was enrolled in the user's plan, except for the Batch File Status and Report Order screens.
MA State/Territory User	MA State/Territory Approver	The user with this role will be able to view MA Part D applications.
MA Submitter (*)	EPOC	The user with this role will be able to view application screens and all information for the periods during which the beneficiary was enrolled in the user's plan, including the Batch File Status and Report Order screens. This role provides access to the Gentran mailbox. The user must select the *Report Access Type* of Financial or Non-Financial.
MMP User	EPOC	The user with the Medicare and Medicaid Plan (MMP) User role will be able to access MARx related to the health plans providing services to Medicare beneficiaries in their state as a part of the Medicare and Medicaid Plan demonstration (formerly known as Financial Alignment Demonstrations).
PDP Representative	EPOC	The user with this role will be able to view only Part D information on all application screens for the periods during which the beneficiary was enrolled in the user's plan, except for the Batch File Status and Report Order screens.

Role	Approved By	Additional Information
PDP Submitter	EPOC	The user with this role will be able to view only Part D information on all application screens for the periods during which the beneficiary was enrolled in the user's plan, including the Batch File Status and Report Order screens.
NET Representative	EPOC	The user with this role will be able to view plan information.
NET Submitter (*)	EPOC	The user with this role will be able to send and receive files on behalf of a plan. This role provides access to the Gentran mailbox. The user must select the Report Access Type of Financial or Non-Financial.
MCO Representative Update	EPOC	The user with this role will be able to enter and correct plan-responsible beneficiary enrollment related data through the MARx online user interface (MARx UI).
Report View (*)	EPOC	This role provides access to the Gentran mailbox. The user must select the Report Access Type of Financial or Non-Financial.
POSFE Contractor	EPOC	Point-of-Sale Facilitated Enrollment (POSFE) contractor cannot enter or select contracts. IACS will assign the contract number as 'R0000' once the user is approved.
SHIP End User	SHIP Approver	The user with this role will be able to view SHIP Part D applications.
SPAP End User	SPAP Approver	The user with this role will be able view MA Part D applications.
IUI Administrator	IUI Authorizer	The user with this role will be able to view all application screens and information, except for the Report Order screens.

* Users with this role should not attempt to register for Gentran separately.

MACPro Application

The purpose of the Medicaid and CHIP Program System (MACPro) is to support an efficient automated business process for submitting, reviewing, and taking final action on all Medicaid and CHIP actions.

Role	Approved By	Additional Information
MACPro Help Desk	Top of the Chain	The user with this role provides first level support for access to MACPro.
MACPro Approver	MACPro Help Desk	The user with this role is responsible for approving MACPro users.

MACPro User	MACPro Approver	The user with this role is an authorized user of the Medicaid and CHIP Program System (MACPro).
MACPro Report User 1	MACPro Approver	The user with this role is an authorized user of the Medicaid and CHIP MicroStrategy reports.
MACPro Report User 2	MACPro Approver	The user with this role is an authorized user of the Medicaid and CHIP MicroStrategy reports.
MACPro Report User 3	MACPro Approver	The user with this role is an authorized user of the Medicaid and CHIP MicroStrategy reports.

MDR Application

Medicaid Drug Rebate: Exchanges data between CMS and the States - Data exchanges include quarterly drug rebate files to states; quarterly drug utilization to CMS; utilization discrepancy reports to states; and quarterly rebate offset amounts to states.

Note: Users registering for the MDR Application will only get a User ID/Password granting access to the Gentran mailbox associated with MDR. The User ID/Password will not allow the user to authenticate (using Access Manager) to the MDR Application.

Role	Approved By	Additional Information
Helpdesk	Top of the Chain	The user with this role will provide help desk assistance for the MDR Application users.
Approver	Helpdesk	The user with this role is responsible for approving requests for the State Technical Contact users.
State Technical Contact	Approver	The user with this role is a staff member who is trusted to perform Medicare business for the application.

MED Application

The Medicare Exclusion Database (MED) is updated monthly with sanction and reinstatement information on excluded providers, and is made available to approved entities only.

Role	Approved By	Additional Information
MED Help Desk User	Top of the Chain	The user with this role will provide help desk assistance to MED Application users.
MED Approver	MED Help Desk User	The user with this role is responsible for approving requests for the MED End Users.
MED User (*)	MED Approver	The user with this role is a staff member who is trusted to perform Medicare business for the application. This role is associated with a Gentran mailbox.
MED Power User (*)	MED Approver	This is a designated role for internal CMS use. This role is associated with a Gentran mailbox.

Role	Approved By	Additional Information
MED Administrator (*)	MED Approver	This is a designated role for internal CMS use. This role is associated with a Gentran mailbox.

* Users with this role should not attempt to register for Gentran separately.

MyCGS Application

MyCGS Web application registration

Role	Approved By	Additional Information
CGS Helpdesk	Top of the Chain	The CGS Helpdesk role should only be selected when the user is an employee of CGS and a member of the CGS Security Team.
CGS Authorized Official	CGS Helpdesk	An Authorized Official must be an owner, general partner, chairperson of the board, chief financial officer, chief executive officer, or president, OR must hold a position of similar status and authority within the supplier's organization. The authorized official has the authority to sign the initial CMS 855S application on behalf of the supplier and is listed as the Authorized Official in the Supplier’s PECOS file.
CGS Back-up Authorized Official	CGS Helpdesk	The Back-up Authorized Official is meant to perform the actions of the Authorized Official for a company when the Authorized Official is unavailable. Users should only select this role if they have previously discussed it with their Authorized Official.
CGS End User	CGS Authorized Official/ CGS Back-up Authorized Official	End users are members of the supplier/provider community seeking to access information about their beneficiaries in order to properly bill Medicare.
CGS Customer Service Rep	CGS Helpdesk	To register for this role, the user must be an employee of CGS and a member of the Customer Service Department.
CGS Technical Group	CGS Helpdesk	To register for this role, the user is an employee of CGS and a member of the DME MAC Tech Team.

Novitasphere Application

Internet Provider Portal for Novitas Solutions, Inc.

Role	Approved By	Additional Information
Novitas Help Desk User	Top of the Chain	The user with this role is a Novitas Solutions employee that supports the Novitasphere Help Desk.
Provider Office Approver	Novitas Help Desk User	The user with this role is an individual located at the Provider's office and will be designated as the Security Official to validate all End Users' requests for their organization.
Provider Office Back-up Approver	Novitas Help Desk User	The user with this role performs many of the same functions as the Provider Office Approver.
Billing Office Approver	Novitas Help Desk User	The user with this role is located at the Billing Office and will be designated as the Security Official to validate all End Users' requests for their organization.
Billing Office Back-up Approver	Novitas Help Desk User	The user with this role performs many of the same functions as the Billing Office Approver.
Novitas Solutions Approver	Novitas Help Desk User	The user with this role is a Novitas Solutions, Inc. employee and will be designated as the Security Official to validate all End Users' requests for their organization.
Novitas Solution Back-up Approver	Novitas Help Desk User	The user with this role performs many of the same functions as the Novitas Solutions Approver.
Novitasphere End User	Approver role associated with the organization	This role should be requested by any individual that wants to utilize the Novitasphere portal.

PQRS/eRx Application

Physician Quality Reporting System and E-Prescribing Incentive Programs - This registration link is for users requesting access to the PQRS Portal to access their Feedback Reports and/or submit data to the Physician Quality Reporting System and E-Prescribing Incentive Programs.

Role	Approved By	Additional Information
PQRI Helpdesk	Top of the Chain	The user with this role is an authorized representative at the QualityNet Help Desk that will provide help desk assistance for the PQRS/eRx Application users.
Security Official (SO) or Security Official 2-Factor	PQRI Helpdesk	The user with this role must be the designated Security Official for the organization and will register the organization in IACS. There can be only one Security Official for an organization. The Security Official is the only individual that can update the organization information in IACS.
Backup Security Official (BSO)	Security Official of the organization	The user with this role performs many of the same functions as a Security Official in an organization. There can be one or more Backup Security Officials in an organization.
Backup Security Official 2-Factor	PQRI Helpdesk	The user with this role performs many of the same functions as a Security Official and requires 2-Factor Authentication. The BSO must have a 2-Factor Authentication Approver Role in any organization where users can select the EHR Submitter or PQRS Submitter (2-Factor Authentication) role.
EHR Submitter	2-Factor Security Official or 2-Factor Backup Security Official of the organization	The EHR Submitter with this role will be required to use 2-Factor Authentication due to the sensitive nature of the data.
EHR Vendor	PQRI Helpdesk	The user with this role is a member of the EHR Organization and can request access to CMS applications.
End User	Security Official or Backup Security Official associated with the organization	The user with this role is a staff member who is trusted to perform Medicare business for the application.
Health Information Exchange (HIE) User	PQRI Helpdesk	The user with this role is authorized to request a PQRI feedback report on behalf of an HIE organization. The HIE User will be required to use 2-Factor Authentication due to the sensitive nature of the data.

Role	Approved By	Additional Information
Individual Practitioner	PQRI Helpdesk	The user with this role is a solo practitioner enrolled in Medicare reporting with a single NPI and receives Medicare payment under his Social Security Number.
Individual Practitioner with 2-Factor Authentication	PQRI Helpdesk	The Individual Practitioner with this role has the option to select the *Request EHR Submission (2-Factor) role* radio button, if the user needs to submit EHR/PII data.
PQRI Admin	PQRI Helpdesk	The user with this role performs administrative functions within the PQRS/eRx Application.
PQRI Maintainer	PQRI Helpdesk	The user with this role performs maintenance functions within the PQRS/eRx Application.
PQRS Representative	Security Official or Backup Security Official associated with the organization PQRI Helpdesk if role is not associated with an organization	The user with this role is authorized to view and retrieve PQRS Reports including PHI and patient level reports.
PQRS Submitter	2-Factor Security Official or 2-Factor Backup Security Official associated with the organization	The user with this role is authorized to submit PQRS Reports including PHI and patient level reports.
Registry End User	PQRI Helpdesk	The user with this role is a member of the Registry organization.

PS&R/STAR Application

This registration link is for users requesting access to Provider Statistical and Reimbursement / System Tracking for Audit and Reimbursement Application (PS&R/STAR). During New User Registration, users are required to select one of the following: FI/Carrier/MAC, Medicare Provider, PS&R/STAR System Maintainer, or Helpdesk.

Role	Approved By	Additional Information
PS&R/STAR Helpdesk	Top of the Chain	The user with this role provides help desk assistance to the PS&R and STAR application users.
PS&R/STAR Security Official	PS&R/STAR Helpdesk	The user with this role must be the designated Security Official for the FI/Carrier/MAC organization. There can be only one PS&R/STAR Security Official for the FI/Carrier/MAC organization.

Role	Approved By	Additional Information
PS&R/STAR Backup Security Official	PS&R/STAR Security Official	The user with this role will be able to back up the PS&R/STAR Security Official and approve End Users and Admins requests for the FI/Carrier/MAC organization. There can be one or more PS&R/STAR Backup Security Officials.
PS&R Security Official	PS&R/STAR Helpdesk	The user with this role must be the designated Security Official for the Medicare Provider organization. There can be only one PS&R Security Official for the Medicare Provider organization.
PS&R Backup Security Official	PS&R/STAR Helpdesk	The user with this role will be able to back up the Security Official and approve End Users and Admins requests for the Medicare Provider organization. There can be one or more PS&R Backup Security Officials.
PS&R Admin	User Type: FI/Carrier/MAC PS&R/STAR Security Official or PS&R/STAR Backup Security Official User Type: Provider PS&R Security Official or PS&R Backup Security Official User Type: System Maintainer Business Owner	The user with this role performs administrative functions within the application.
STAR User 1 – STAR User 8	User Type: FI/Carrier/MAC PS&R/STAR Security Official or PS&R/STAR Backup Security Official User Type: System Maintainer Business Owner	The user with this role is a staff member who is trusted to perform Medicare business for the application.

Role	Approved By	Additional Information
PS&R User	User Type: FI/Carrier/MAC PS&R/STAR Security Official or PS&R/STAR Backup Security Official User Type: Provide PS&R Security Official or PS&R Backup Security Official User Type: System Maintainer Business Owner	The user with this role is a staff member who is trusted to perform Medicare business for the application.

PV/PQRS Registration System Application

The Physician Value / Physician Quality Reporting System (PV/PQRS) Registration System allows Group Practices to select their reporting method for the PQRS and the Value Modifier, if applicable, and allows Individual Eligible Professionals to select the Administrative Claims reporting method to avoid the PQRS payment adjustment.

Role	Approved By	Additional Information
PV Helpdesk Approver	Top of the Chain	The user with this role is an authorized representative of CMS who will provide help desk assistance to PV CMS Administrators.
PV PQRS Group Security Official	PV Helpdesk Approver	This user’s role is one individual in a physician group practice that will be able to select the PQRS reporting method for the group; will be able to view QRUR reports; and/or, approve other users in the group, so that other users in the group can select the group’s PQRS reporting mechanism and view QRUR reports.
PV PQRS Individual	PV Helpdesk Approver	This user’s role is an Individual Eligible Professional (EP) that is able to select the PQRS Administrative Claims reporting mechanism to avoid the PQRS payment adjustment, and/or approve another user on behalf of the EP, and can select the PQRS Administrative Claims reporting mechanism for that EP.
PV PQRS Group Representative	PV PQRS Group Security Official	This user’s role is a representative of a physician group practice that will be able to select the PQRS reporting method, on behalf of the group, and be able to view QRUR reports for the group practice.
PV PQRS Individual Representative	PV PQRS Individual	This user’s role is a representative of an Individual Eligible Professional (EP) that will be able to select the PQRS reporting method, on behalf of the EP.

The SPOT – First Coast Service Options Internet Portal

The SPOT offers an array of self-service resources to furnish essential Medicare processing information within a secure, online environment.

Role	Approved By	Additional Information
FCSO Help Desk User	Top of the Chain	The user with this role provides help desk assistance for The SPOT- FCSO Internet portal users.
FCSO Portal User	FCSO Help Desk	The user with this role is a staff member who is trusted to perform Medicare business for the application.

VMS Client Letter

VMS Client Letter Application is the Durable Medical Equipment Medicare Administrative Contractor integrated correspondence system. Approvers and End Users of the system are required to be an employee or agent of a Durable Medical Equipment Medicare Administrative Contractor and must have a valid and active RACF ID to register for an approver and/or end user role.

Role	Approved By	Additional Information
VMS Helpdesk	Top of the Chain	The user with this role will provide help desk assistance for the VMS Client Application users.
JA Approver	VMS HelpDesk	The user with this role is trusted to approve requests for Jurisdiction A end users.
JB Approver	VMS HelpDesk	The user with this role is trusted to approve requests for Jurisdiction B end users.
JC Approver	VMS HelpDesk	The user with this role is trusted to approve requests for Jurisdiction C end users.
JD Approver	VMS HelpDesk	The user with this role is trusted to approve requests for Jurisdiction D end users.
JA LG User JA History JA ZPIC User	JA Approver	The user with these role are staff members who are trusted to perform Medicare business for Jurisdiction A.
JB LG User JB History JB ZPIC User	JB Approver	The user with these role are staff members who are trusted to perform Medicare business for Jurisdiction B.
JC LG User JC History JC ZPIC User	JC Approver	The user with these role are staff members who are trusted to perform Medicare business for Jurisdiction C.
JD LG User JD History JD ZPIC User	JD Approver	The user with these role are staff members who are trusted to perform Medicare business for Jurisdiction D.

Appendix B Request Timeout Days

IACS allows Approvers sufficient time to process pending requests. IACS will expire the request if no action is taken within the specified time. The table below shows the type of role and the request timeout days after which the registration and modification requests will be cancelled if the Approver has not taken any action.

Role Type	Request Timeout (Number of Calendar Days)
Authorizer	24
Help Desk User	24
Security Official	60
Backup Security Official, Backup Authorized Official, Approver	24
End User (All roles without Approval authority)	12

PQRS/eRx Request Timeout days

The PQRS/eRx Application differs from the standard request timeout followed by most of the applications. The table below shows the type of PQRS/eRx Application roles and the request timeout days after which the registration and modification requests will be cancelled if the Approver has not taken any action.

Role Type	Request Timeout (Number of Calendar Days)
PQRI Help Desk	60
Security Official	60
Backup Security Official	60
End User	60
EHR Submitter	60
Individual Practitioner	60
Registry End User	12
EHR Vendor	12
PQRI Admin	12
PQRI Maintainer	12
PQRS Submitter	12
PQRS Representative	12

Index