Individuals Authorized Access to the CMS Computer Services (IACS)

IACS User Guide

Document Version 1.0

June 2012

Document No.: IACS.UG.1.0
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	QSSI

CONTENTS

1.0 Introduction 1

2.0 Overview 1

2.1 User Guide Conventions 1
2.2 Browser Requirements 2
2.3 Cautions and Warnings 3

3.0 What is an IACS Account 3

4.0 IACS Supported CMS Applications 3

5.0 Understanding Roles 4

6.0 New User Registration 20

6.1 Register for a CMS Application 20
6.2 Registration Completion 31
6.3 Application Specific Registration 32
6.3.1 COB Registration 32
6.3.2 CSR Registration 32
6.3.3 DMEPOS Registration 32
6.3.4 Gentran Registration 32
6.3.5 HETS UI Registration 33
6.3.6 HPG Registration 33
6.3.7 Internet Server Registration 33
6.3.8 MA/MA-PD/PDP/CC Registration 33
6.3.9 MED Registration 35
6.3.10 Novitasphere Registration 35
6.3.11 PQRS/eRx Registration 36
6.3.12 PS&R/STAR Registration 38
6.3.13 VMS Client Letter Registration 39
6.4 Top of the Chain User Registration 39

7.0 Using IACS 40

7.1 IACS Login 40
7.2 My Profile Screen 42

8.0 Managing User IDs & Passwords 44

8.1 Change Password - Password Expiration 44
8.2 Forgot Your Password? 44
8.3 Forgot Your User ID? 45
8.4 Re-Activate Account 45
8.5 Locked Account 45

9.0 Modify User/Contact Information 46

9.1 Modify User/ Contact Information – Change E-mail 46

10.0 Modify Account Profile 49

10.1 View User’s Access Profile 49
10.2 Add Application 50
10.3 MA/MA-PD/PDP/CC - Add and Remove Contracts 51

10.4 Disassociate from Current Role 53
10.5 Add Role 54
10.6 Modify Report Access 56
10.7 Modify User Profile – Other Application Modifications 57

11.0 Annual Certification 58

11.1 E-mail Notifications 59
11.2 Certify Account Profile 59

12.0 Approve Pending Request 61

12.1 Pending Approvals 61
12.1.1 PQRS/eRx PECOS Verification 65
12.1.2 Search Pending Requests 66
12.2 Search and View (only) Pending Requests 69
12.3 Annual Certification Approval 69
12.3.1 Approver E-mail Notifications 69
12.3.2 Approve/Reject/Defer Requests for Annual Certification 70

13.0 Managing Users Under My Authority 71

13.1 Authorized Official, Security Official, EPOC – Search and Manage Users 71
13.2 Manage Contracts 72
13.3 Help Desk Functions using Manage users under my authority 77
13.4 Searching for User Accounts 80
13.4.1 View User Account Information 83
13.4.2 Disable User Account 87
13.4.3 Reset User Password 90
13.4.4 Unlock User Account 91

14.0 User Lookup 94

15.0 IACS Account Life Cycle 95

15.1 Password Expiration 95
15.2 180 Day Partial Disable 95
15.3 Archiving Accounts 95
15.3.1 Certification Failure 95
15.3.2 MA/MA-PD/PDP/CC Users without Contracts for 60 days 96

16.0 Troubleshooting & Support 97

16.1 Error Messages 97
16.2 Validation Failure 97
16.3 Frequently Asked Questions 100
16.4 Support 106

17.0 Glossary 107

18.0 Acronyms 109

Appendices 113
Appendix A - Request Timeout Days 113
Index 114

FIGURES

Figure 1: CMS Applications Portal Introduction Screen 21
Figure 2: Account Management Screen 22
Figure 3: New User Registration Menu Screen 22
Figure 4: New User Registration Screen 23
Figure 5: E-mail Address Verification 24
Figure 6: New User Registration Screen: Contact Information 25
Figure 7: New User Registration Screen: Access Request Area, Role Drop-down 26
Figure 8: New User Registration Screen: Access Request Area, MA Submitter 27
Figure 9: New User Registration Screen: Access Request Area, Contract Number & RACF ID Field – MA Submitter 28
Figure 10: Authentication Questions Screen 29
Figure 11: Review Registration Details Screen 30
Figure 12: Registration Acknowledgement Screen 31
Figure 13: Login to IACS Screen 41
Figure 14: My Profile Screen: MA/MA-PD/PDP/CC Application Users 42
Figure 15: Modify User/Contact Information Screen 47
Figure 16: Modify Request Confirmation Screen 48
Figure 17: Modification Request Acknowledgement Screen 48
Figure 18: Modify Account Profile Screen: Access Request Area – Select Action Drop-down 50
Figure 19: Modify Account Profile Screen: Access Request Area – Select Application Drop-down 51
Figure 20: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC User/Submitter Add or Remove Contracts 52
Figure 21: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC User/Submitter Disassociate from Role 53
Figure 22: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC Add Role 55
Figure 23: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC Modify Report Access 57
Figure 24: My Profile Screen: Certify Account Profile Hyperlink 59
Figure 25: Annual Certification: Review Account Profile Screen 60
Figure 26: Approver Inbox Screen 62
Figure 27: Approve/Reject Request Screen: Required Access Area – Grouped Pending Items 63
Figure 28: Confirm Action Dialogue box with Deferred Items 64
Figure 29: Approve / Reject Request screen with PECOS Validation 66
Figure 30: My Profile Screen 67
Figure 31: Approver Inbox Screen: Search Request(s) Hyperlink 67
Figure 32: Search Criteria for Pending Request(s) Screen 68
Figure 33: Search Criteria for Pending Request(s) Screen: Search Results 69
Figure 34: Inbox listing Pending Certification 70
Figure 35: Approve / Reject Request Screen: Certification Request 71
Figure 36: Manage user under my authority – Search Criteria 73
Figure 37: Manage users under my authority Screen – Search Results Area 74
Figure 38: Manage users under my authority Screen Search Results Area – Edit Button Selection 75
Figure 39: Manage users under my authority Screen: Search Results Area – Editable Search Results 76

Figure 40: Manage users under my authority Screen: Search Results Area – Single Justification for Action.....76
Figure 41: Review Details Screen.....77
Figure 42: My Profile Screen.....79
Figure 43: Manage users under my authority Screen - MA/MA-PD/PDP/CC.....80
Figure 44: Manage users under my authority Screen - ECRS.....80
Figure 45: Manage users under my authority Screen – Search Results.....82
Figure 46: Manage users under my authority Screen – Search Results (Archived Users).....83
Figure 47: Manage users under my authority Screen – Help Desk Function Buttons Enabled ..84
Figure 48: View Profile Screen – Identity Tab.....85
Figure 49: View Profile Screen – Professional Contact Tab.....85
Figure 50: View Profile Screen – Certification Tab.....86
Figure 51: View Profile Screen – Security Tab.....87
Figure 52: Manage users under my authority Screen –Disable Option.....88
Figure 53: Disable Account Screen.....88
Figure 54: Disable Account Acknowledgement Screen.....89
Figure 55: Manage users under my authority Screen – Shows User (Fully Disabled).....89
Figure 56: Manage users under my authority Screen – Reset Password Option.....90
Figure 57: Reset User Password Screen.....90
Figure 58: Reset Account Password Acknowledgement Screen.....91
Figure 59: Manage users under my authority Screen – Unlock Option.....92
Figure 60: Unlock Account Screen.....92
Figure 61: Unlock Account Acknowledgement Screen.....93
Figure 62: Manage users under my authority Screen – Shows User (Active).....93
Figure 63: User Lookup Screen.....94
Figure 64: User Lookup Search Results.....94
Figure 65: New User Registration Screen: Validation Failure Message.....97
Figure 66: Warning Message.....98
Figure 67: Information Message.....99
Figure 68: Caution Message.....99

TABLES

Table 1: Possible Role Combinations for MA/MA-PD/PDP/CC.....33
Table 2: Applications and the corresponding Helpdesks with Approval Authority.....61
Table 3: Manage user under my authority - Roles with Edit Capabilities.....72
Table 4: Applications and Help Desk Roles using Manage users under my authority.....78

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 data combines to create a substantial risk to CMS and Beneficiaries. Legislations, like the Health Insurance Portability and Accountability Act (HIPAA), Federal Standards published by the National Institute of Standards and Technology (NIST), and CMS policies have been established to control that 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; 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 for one of the CMS applications
- Modifying user registration information
- Certifying annually the need for continued access to CMS systems
- Processing (approving, denying, 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 with 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/mapdhelpdesk/IACS.html) to provide additional information and instruction for IACS users.

2.1 User Guide Conventions

This document provides screen prints and corresponding narratives to describe the typical account registration and account management procedures. 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 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 work **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.

2.2 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 6.0 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.

2.3 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.

3.0 What is an IACS Account

An IACS account provides the CMS application user a single User ID to access CMS systems as listed in Section 4.0 and identifies the user as an approved user of the application(s).

An IACS account is created once the New User Registration request has been approved. The User ID identifies the user, the CMS application, and the role assignment. When the user logs in to the approved CMS application with his IACS User ID, the user will be identified with the user's role and access privileges. Once registered, the user will be using IACS to manage the account as follows:

- Reset password
- "Forgot Your Password?" self-service recovery
- "Forgot Your User ID?" self-service recovery
- Change password every 60 days
- Add new application or role
- Remove role
- Modify User and Professional Contact Information
- Annual Certification of account

4.0 IACS Supported CMS Applications

This **IACS User Guide** provides the procedures to obtain an IACS User ID and manage an IACS account for the following CMS applications:

- Coordination of Benefits (COB)
- 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)
- Customer Service Representatives (1-800-Medicare CSR)
- Durable Medical Equipment, Prosthetics, Orthotics & Supplies (DMEPOS) Bidding System (DBidS)
- Electronic Correspondence Referral System (ECRS) Web
- GENTRAN
- HIPAA Eligibility Transaction System User Interface (HETS UI)
- HIPAA Eligibility Transaction System Provider Graphical User Interface (HPG)

- Internet Server (ISV)
- 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)
- 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)
- System Tracking for Audit and Reimbursement (STAR)
- VMS Client Letter

5.0 Understanding Roles

IACS uses a hierarchical system of approvals, referred to as the Chain of Trust, for registration requests, profile modification requests, and annual certification requests. 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: Acronyms in this section are defined in the Glossary at the end of this document

COB Application:

Access to the Coordination of Benefits (COB) application is restricted to the employees of the Coordination of Benefits Contractor (COBC) only.

- **Authorizer**
  - The Authorizer is the top of the chain user trusted with approving requests for New User Registration, modification of user profile, and re-certification for Approver and COB Helpdesk roles.
- **Approver**
  - The Approver is trusted with approving new user creation requests, requests for Modify user profile, and re-certification for COB User/Transmitter roles. The COB Approver will have the approval authority for all users of all COB organizations.

- **COB Helpdesk**
  - The COB Helpdesk user is an authorized representative of CMS who will provide help desk assistance to COB Application Users. The COB Helpdesk role is an end user role that does not have approval authority.
- **User/Transmitter**
  - The User/Transmitter is trusted with transmitting batch files containing membership changes and health status corrections.

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.

- **HSTP Helpdesk User**
  - The HSTP Helpdesk User is the top of the chain user who will provide help desk assistance to CSP - HSTP Application users. The HSTP Helpdesk User functions as an Authorizer in IACS and approves new user creation requests, requests for Modify user profile, and re-certification requests for users with the HSTP End User role.
- **HSTP End User**
  - The HSTP End User 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 and Medicaid and CHIP provider termination data.

- **MCSIS Helpdesk User**
  - The MCSIS Helpdesk User is the top of the chain user who will provide help desk assistance to CSP-MCSIS Application Users. The MCSIS Helpdesk User functions as an Authorizer in IACS and approves new user creation requests, requests for profile modification, and re-certification requests for users with the MCSIS End User role.
- **MCSIS End User**
  - The MCSIS End User is a staff member who is trusted to perform Medicare business for the application.

CSR Application:

Community Based Organization/Customer Service Representative

- **Authorizer**

- The Authorizer is the top of the chain user trusted with approving requests for new user registration, modification of user profile, and re-certification for Approver roles.

- **Approver**
  - The Approver is trusted with approving new user creation requests, requests for Modify user profile, and re-certification for CSR Users.

- **User**
  - The User is a customer service representative or staff member who is trusted to perform business for the organization.

- **Local Service Administrator (LSA)**
  - The LSA user is an authorized representative of CMS who is trusted to perform Medicare business for the application. 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).

Helpdesks

- **DMEPOS Authorizer1**
  - The DMEPOS Authorizer1 is the top of the chain user trusted with approving requests for New User Registration, modification of user profile, and re-certification for DMEPOS IT Help Desk role.

- **DMEPOS Authorizer2**
  - The DMEPOS Authorizer2 is the top of the chain user trusted with approving requests for New User Registration, modification of user profile, and re-certification for CBIC- Tier1 or CBIC- Tier2 or CBIC- Input role.

- **CBIC Tier 1**
  - The CBIC Tier-1 user is an authorized representative to provide Tier-1 help desk assistance for the DMEPOS Application Users.

- **CBIC Tier 2**
  - The CBIC Tier-2 user is an authorized representative to provide Tier-2 help desk assistance for the DMEPOS Application Users.

- The CBIC Tier-2 user can search and modify DMEPOS user profiles within the scope of his responsibility.

AO, BAO, and End User

- **Authorized Official (AO)**
  - The AO is an appointed official to whom the organization has granted the legal authority to enroll the organization in the Medicare program and to commit the organization to abide by the statutes, regulations, and program instructions of the Medicare program per the CMS 855S Medicare Enrollment Application.
  - The AO must be listed on the CMS 855S application as an Authorized Official.
  - The AO is trusted to approve the access requests of the Backup Authorized Officials and End Users. The AO is held accountable by CMS for the behavior of those they approve within their organization.
  - Each organization can have only one AO.
- **Backup Authorized Official (BAO)**
  - The BAO is an appointed official to whom the organization has granted the legal authority to enroll the organization in the Medicare program and to commit the organization to abide by the statutes, regulations, and program instructions of the Medicare program per the CMS 855S Medicare Enrollment Application.
  - The BAO must be listed on the CMS 855S application as an Authorized Official.
  - The BAO is trusted to approve the access request of End Users.
  - Each organization can have one or more BAOs if approved by the organization's AO.
  - The BAO is not a required role for an organization; however, it is highly recommended that each organization establish this role to ensure adequate coverage for approval of End Users and to replace the organization's AO, if the need arises.
- **End User**
  - The End User is an individual entrusted by the organization to input bid data.
  - The End User cannot approve Form A or certify Form B. The approval and certification function is reserved for the AO and/or BAO.
  - Each organization can have one or more End Users if approved by the organization's AO or BAO.

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.

- **ECRS HelpDesk**
  - The ECRS HelpDesk is the top of the chain user who will provide help desk assistance for the ECRS Application Users. The ECRS HelpDesk user functions as an Authorizer in IACS and approves new user creation requests, requests for modify user profile, and re-certification for users with the ECRS Approver role.
- **ECRS Approver**
  - The ECRS Approver is trusted with approving new user creation requests, requests for modify user profile, and re-certification for ECRS Users.
- **ECRS User**
  - The ECRS User is a staff member who is trusted to perform Medicare business for the application.

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.

- **Gentran Helpdesk**
  - The Gentran Helpdesk is the top of the chain user who will provide help desk assistance for the Gentran Application users.
- **Gentran Approver**
  - The Gentran Approver is trusted with approving new user creation requests, requests for Modify user profile, and re-certification for Gentran Users.
- **Gentran User**
  - The Gentran User 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.

- **MEIC Helpdesk**

- The MEIC Helpdesk (now known as MCARE Help Desk) is the top of the chain user who will provide help desk assistance for the CMS Medicare Eligibility Integration Contractor (MEIC). The MEIC Helpdesk is also trusted to approve registration, modification, and certification requests for Security Official and HPG Users. If the User/Approver does not exist, the User/Provider request is routed to the MEIC Helpdesk.

Approvers

- **Security Official (SO)**
  - The Security Official represents the organization or facility in IACS. There can be two Security Officials at a facility or organization. The Security Official is trusted with approving new user creation requests, requests for Modify user profile, and re-certification for users with the role of User/Approver.
- **User/Approver**
  - The User/Approver is trusted with approving new user creation requests, requests for Modify user profile, and re-certification for users with the role of User/Provider.

End User

- **User/Provider**
  - The User/Provider under HETS UI is a health care provider that has access to the HETS UI system to verify the eligibility information of the beneficiaries.

HPG Application:

HIPAA Eligibility Transaction System (HETS) Provider Graphical User Interface (GUI)

- **HPG User**
  - An HPG User is a staff member who is trusted to use the HPG to perform business on behalf of the organization.
  - This role is associated with a Gentran mailbox as long as a Submitter ID is associated with their profile; this rule applies to all users except for those with a P-type Submitter ID.

Note: Users with this role should not attempt to register for Gentran separately.

Internet Server:

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.

- **Internet Server Help Desk**

- The Internet Server Help Desk is the top of the chain user who will provide help desk assistance for the Internet Server Application Users.

- **Internet Server Approver**
  - The Internet Server Approver is trusted with approving new user creation requests, requests for modify user profile, and re-certification for Internet Server Users.

- **Internet Server User**
  - The Internet Server User 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

Authorizers

- **Authorizer**
  - The Authorizer is the top of the chain user trusted with approving requests for new user registration, modification of user profile, and re-certification for Approver role.

- **IUI Authorizer**
  - The IUI Authorizer is the top of the chain user trusted with approving requests for New User Registration, modification of user profile, and re-certification for IUI Helpdesk, IUI Administrator, MAPD Helpdesk, and MAPD Helpdesk Admin roles.

- **State Authorizer**
  - The State Authorizer is the top of the chain user trusted with approving requests for New User Registration, modification of user profile and re-certification for MA State/Territory Approver, State Health Insurance Plans (SHIP) Approver, and State Pharmacy Assistance Programs (SPAP) Approver.

Approvers

- **EPOC**
  - EPOC is trusted with approving new user creation requests, requests for Modify user profile and re-certification for the users with Submitter, Representative Contractor, and Report View roles.

- **MA State/Territory Approver**
  - The MA State/Territory Approver will be able to approve Medicare Advantage State and Territory Users that require access to their applications through IACS.

- This person will not have access to the MA Part D applications.

- **SHIP Approver**
  - The SHIP Approver will be able to approve SHIP Users that require access to their applications through IACS.
  - This person will not have access to the MA Part D applications.

- **SPAP Approver**
  - The SPAP Approver will be able to approve SPAP Users that require access to their applications through IACS.
  - This person will not have access to the MA Part D applications.

Helpdesks

- **IUI Helpdesk**
  - The IUI Helpdesk will be able to view all application screens and information, except for the Report Order screens.

- **MAPD Helpdesk**
  - The MAPD Helpdesk user is an authorized representative of CMS who will provide help desk assistance to MA/MA-PD/PDP/CC and CSR Application Users.

- **MAPD Helpdesk Admin**
  - The MAPD Helpdesk Admin user is an authorized representative of CMS who will provide administrative help desk assistance to MA/MA-PD/PDP/CC and CSR Application Users information.

End Users

- **MA Representative**
  - The MA Representative will be able to view all 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**
  - The MA State/Territory User will be able to view MA Part D applications through the integrated user interface.

- **MA Submitter**
  - The MA Submitter will be able to view all application screens and all information for the periods during which the beneficiary was enrolled in the user’s plan, including Batch File Status and Report Order screens.
  - This role allows the user to send and receive files on behalf of a plan.

- This role is associated with Financial, Non-Financial Gentran mailboxes or both depending on the user selection of the Report Access Type during registration.

Note: Users with this role should not attempt to register for Gentran separately.

- **PDP Representative**
  - The PDP Representative 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 Batch File Status and Report Order screens.
- **PDP Submitter**
  - The PDP Submitter 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 Batch File Status and Report Order screens.
  - This role allows the user to send and receive files on behalf of a plan.
  - This role is associated with Financial, Non-Financial Gentran mailboxes or both depending on the user selection of the Report Access Type during registration.
- **NET Representative**
  - The NET Representative will be able to view plan information.
- **NET Submitter**
  - The NET Submitter will be able to send and receive files on behalf of a plan.
  - This role is associated with Financial, Non-Financial Gentran mailboxes or both depending on the user selection of the Report Access Type during registration.

Note: Users with this role should not attempt to register for Gentran separately**.**

- **MCO Representative UI Update**
  - The MCO Representative UI Update User will be able to enter and correct plan-responsible beneficiary enrollment related data through the MARx online user interface (MARx UI).
  - This role will not have access to Gentran Mailbox.
- **Report View**
  - This role is associated with Financial, Non-Financial Gentran mailboxes or both depending on the user selection of the Report Access Type during registration.

Note: Users with this role should not attempt to register for Gentran separately.

- **POSFE Contractor**
  - A POSFE (Point-of-Sale Facilitated Enrollment) Contractor is a registered user who cannot enter or select contracts. When the POSFE Contractor is approved, the user is automatically assigned the ‘R0000’ Contract by the system.
- **SHIP End User**
  - The SHIP End User will be able to view SHIP Part D applications through the integrated user interface.
- **SPAP End User**
  - The SPAP End User will be able to view MA Part D applications through the integrated user interface.
- **IUI Administrator**
  - The IUI Administrator will be able to view all application screens and information, except for the Report Order screens.

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.

- **Helpdesk**
  - The Helpdesk is the top of the chain user who will provide help desk assistance for the MDR Application Users.
- **Approver**
  - The Approver is trusted with approving new user creation requests, requests for Modify user profile, and re-certification for State Technical Contact Users.
- **State Technical Contact**
  - The State Technical Contact is a staff member who is trusted to perform Medicare business for the application.

Medicare Exclusion Database 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.

- **MED Help Desk User**

  - The MED Help Desk User is the top of the chain user who will provide help desk assistance to MED Application users.

- **MED Approver**
  - The MED Approver is trusted with approving new user creation requests, requests for Modify user profile, and re-certification for MED End Users.

- **MED User**
  - The MED User is a staff member who is trusted to perform Medicare business for the application.
  - This role is associated with a Gentran mailbox.

Note: Users with this role should not attempt to register for Gentran separately.

- **MED Power User**
  - The MED Power User is a designated role for internal CMS use.
  - This role is associated with a Gentran mailbox.

Note: Users with this role should not attempt to register for Gentran separately.

- **MED Administrator**
  - The MED Administrator is a designated role for internal CMS use.
  - This role is associated with a Gentran mailbox.

Note: Users with this role should not attempt to register for Gentran separately.

Novitasphere:

Internet Provider Portal for Novitas Solutions, Inc.

- **Novitas Help Desk User**
  - This should be requested by only Novitas Solutions employees that support the Novitasphere Help Desk.

Approvers

- **Provider Office Approver**
- **Provider Office Back-up Approver**
  - This should be requested by the individual located at the Provider's Office that will be designated as the Security Official to validate all End Users' access for their organization.

- **Billing Office Approver**
- **Billing Office Back-up Approver**

- This should be requested by the individual located at the Billing Office that will be designated as the Security Official to validate all End Users' access for their organization.

- **Novitas Solutions Approver**
- **Novitas Solutions Back-up Approver**
  - This should be requested by the individual employed by Novitas Solutions, Inc. that will be designated as the Security Official to validate all End Users' access for their organization.

End Users

- **Novitasphere End User**
  - This should be requested by any individual that wants to utilize the Novitasphere portal.

Physician Quality Reporting System/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.

- **PQRI HelpDesk**
  - The PQRI HelpDesk user is the top of the chain user who is an authorized representative at the QualityNet Help Desk that will provide help desk assistance for the PQRS/eRx Application Users.
  - The PQRI HelpDesk user functions as an Authorizer in IACS and approves new user creation requests, requests for modify user profile, and re-certification for users with the Security Official (SO), Backup Security Official 2-Factor approver, PQRS Representative (Individual), PQRS Submitter (Individual), Individual Practitioner (IP), Registry End User, EHR Vendor, PQRI Maintainer, and PQRI Admin roles.

Approvers

- **Security Official**
  - The Security Official is the authorized representative of his organization and registers the organization in IACS.
  - There can be only one Security Official in an organization.
  - The Security Official is trusted to approve the access requests of Backup Security Officials.
  - The Security Official can approve the access requests of End Users.

- The Security Official is the only individual who can update the information in the organization profile in IACS.
- The Security Official can have a 2-Factor Authentication Approver Role.
- The Security Official 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).

- **Backup Security Official**
    - A Backup Security Official performs many of the same functions as a Security Official (see above) in an organization.
    - There can be one or more Backup Security Officials in an organization.
    - The Backup Security Official can approve the access requests of End Users and may assist the organization's Security Official with other administrative tasks.
    - The Backup Security Official can have a 2-Factor Authentication Approver Role.
    - The Backup Security Official 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).

End Users

- **EHR Submitter (2-Factor Authentication role)**
    - The EHR Submitter is part of a healthcare organization and is authorized to submit personally identifiable information (PII) to CMS applications.
    - The EHR Submitter will be required to use 2-Factor Authentication due to the sensitive nature of the data. Additional information is required for the EHR Submitter's profile to support 2-Factor Authentication.
- **EHR Vendor**
    - An EHR Vendor is part of the EHR Organization and can request access to CMS Applications.
    - EHR Vendors are allowed to select an organization from a pre-defined list of EHR Vendor Organizations during New User Registration.
- **End User**
    - An End User is a staff member who is trusted to perform Medicare business for the organization.
    - An End User is part of an organization.

- **Health Information Exchange (HIE) User**
    - The HIE User is authorized to request a PQRI feedback report on behalf of an HIE Organization.
    - The HIE User is required to use 2-Factor Authentication due to the sensitive nature of the data. Additional information is required for the HIE User's profile to support 2-Factor Authentication.
    - The HIE User is required to select an organization from a pre-defined list of HIE Organizations during New User Registration.
- **Individual Practitioner**
    - An Individual Practitioner is a solo practitioner enrolled in Medicare reporting with a single NPI and receives his Medicare payment under his Social Security Number.
- **Individual Practitioner with 2-FactorAuthentication**
    - An Individual Practitioner is a solo practitioner enrolled in Medicare reporting with a single NPI and receives his Medicare payment under his Social Security Number. If the Individual Practitioner would like to Submit EHR / PII data, he must select the *Request EHR Submission (2 factor) role* radio button during registration.
- **PQRI Admin**
    - The PQRI Admin user is an authorized representative of CMS who is responsible for performing Administrative functions within the PQRS/eRx Application.
- **PQRI Maintainer**
    - The PQRI Maintainer user is the authorized representative of CMS who is responsible for performing Maintenance functions on specific PQRS/eRx Application(s).
- **PQRS Representative**
    - The PQRS Representative is authorized to access the PQRS Portal to view and retrieve PQRS Reports including PHI and patient level reports.
    - The PQRS Representative will ordinarily be associated with an organization.
    - Users seeking the PQRS Representative role who do not belong to any organization may register without selecting an organization.
- **PQRS Submitter**
    - The PQRS Submitter is authorized to access the PQRS Portal to submit PQRS Reports including PHI and patient level reports.
    - The PQRS Submitter will ordinarily be associated with an organization.

- Users seeking the PQRS Submitter role who do not belong to any organization may register without selecting an organization.

- The PQRS Submitter will be required to use 2-Factor Authentication due to the sensitive nature of the data. Additional information is required for the PQRS Submitter's profile to support 2-Factor Authentication.

- **Registry End User**
    - A Registry End User is part of the Registry Organization and can request access to CMS applications.
    - Registry End Users are required to select an organization from a pre-defined list of Registry Organizations during New Users Registration.

Provider Statistical and Reimbursement / System Tracking for Audit and Reimbursement Application (PS&R/STAR):

This registration link is for users requesting access to PS&R and/or STAR application. During New User Registration, users are required to select one of the following: FI/Carrier/MAC, Providers, PS&R/STAR System Maintainer, and Helpdesk.

- **PS&R/STAR Helpdesk**
    - The PS&R/STAR Helpdesk is the top of the chain user who is an authorized representative that provides help desk assistance to the PS&R and STAR application users.
    - The PS&R/STAR Helpdesk approves Security Officials (SOs) that work for FI/Carrier/MAC, Medicare Providers, and System Maintainers that request PS&R/STAR End User roles.

Approvers

- **PS&R/STAR Security Official**
    - The PS&R/STAR Security Official is the authorized representative of his FI/Carrier/MAC Organization in IACS.
    - There can be only one Security Official in an FI/Carrier/MAC Organization.
    - The Security Official is trusted to approve the access requests of Backup Security Officials, End Users, and Admins.
    - The Security Official is the only individual who can update the information in the organization profile in IACS.

- **PS&R/STAR Backup Security Official**
    - A PS&R/STAR Backup Security Official performs many of the same functions as a PS&R/STAR Security Official in an FI/Carrier/MAC Organization.
    - There can be one or more Backup Security Officials in an organization.

- The Backup Security Official can approve the access requests of End Users and Admins. He may assist the organization's Security Official with other administrative tasks.

- **PS&R Security Official**
  - The PS&R Security Official is the authorized representative of his Medicare Provider Organization in IACS.
  - There can be only one Security Official in a Medicare Provider Organization.
  - The Security Official is trusted to approve the access requests of Backup Security Officials, End Users, and Admins.
  - The Security Official is the only individual who can update the organization information in IACS.

- **PS&R Backup Security Official**
  - A PS&R Backup Security Official performs many of the same functions as a PS&R Security Official in a Medicare Provider Organization.
  - There can be one or more Backup Security Officials in an organization.
  - The Backup Security Official can approve the access requests of End Users and Admins. He may assist the organization's Security Official with other administrative tasks.

End Users

- **PS&R Admin**
  - The PS&R Admin user is the authorized representative of CMS who is responsible for performing administrative functions within the application.

- **PS&R User**
  - A PS&R User is a staff member who is trusted to perform Medicare business.

- **STAR User 1 – STAR User 8**
  - A STAR User is a staff member who is trusted to perform Medicare business.

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.

- **VMS Help Desk**
  - The VMS Help Desk is the top of the chain user who will provide help desk assistance for the VMS Client Letter Application Users. The VMS Client

Letter Help Desk User functions as an Authorizer in IACS and approves new user creation requests, requests to Modify user profile, and re-certification for users with the VMS Client Letter Approver role.

- **VMS Client Letter Approvers**
  - The VMS Client Letter Approver is trusted with approving new end user requests, requests to Modify user profile, and re-certification for VMS Client Letter End Users.
    - **JA Approver** - approver for JA LG User, JA History, and JA ZIPIC User
    - **JB Approver** - approver for JB LG User, JB History, and JB ZIPIC User
    - **JC Approver** - approver for JC LG User, JC History, and JC ZIPIC User
    - **JD Approver** - approver for JD LG User, JD History, and JD ZIPIC User
- **JD Approver VMS Client Letter End Users**
  - VMS Client Letter End User is a VMS Client Letter application user who is trusted to perform functions associated with the VMS Client Letter Application for the jurisdiction for which they have been approved.
    - **Jurisdiction A End Users:** JA LG User, JA History, JA ZPIC User
    - **Jurisdiction B End Users:** JB LG User, JB History, JB ZPIC User
    - **Jurisdiction C End Users:** JC LG User, JC History, JC ZPIC User
    - **Jurisdiction D End Users:** JD LG User, JD History, JD ZPIC User

6.0 New User Registration

The following section provides instructions for the most common registration steps using the MA/MA-PD/PDP/CC Application, MA Submitter role as an 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.

The **CMS Applications Portal WARNING/REMINDER** screen will display.

If the user does not want to proceed any further and wants to exit, he needs to select 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.

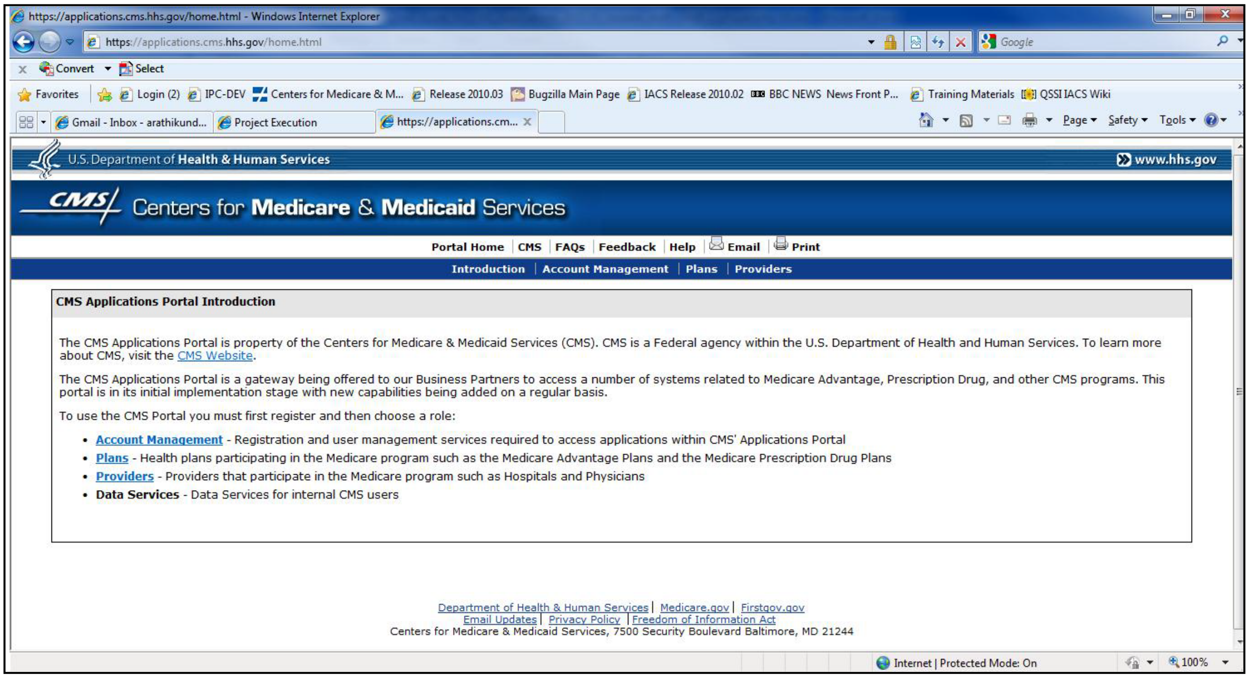


Figure 1: CMS Applications Portal Introduction Screen

Action: Select the Account Management hyperlink in either the white space 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.

Hyperlinks on this screen will allow users to access IACS registration, login functions, and the IACS Community Administration Interface.

The bottom area of the screen provides Help Resources with Help Desk contact information and E-mail hyperlinks.

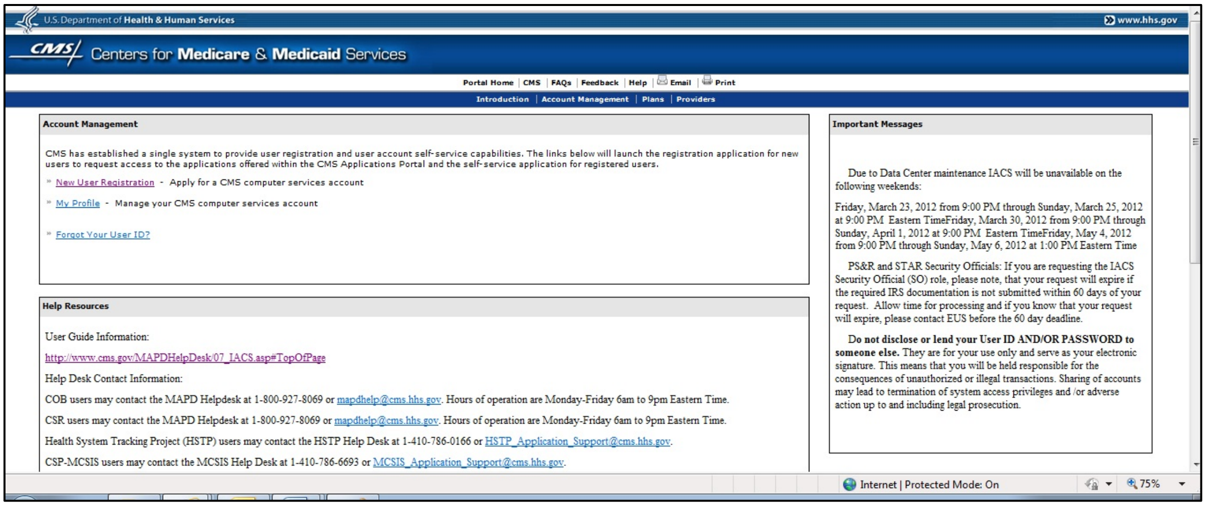


Figure 2: Account Management Screen

Action: Select the New User Registration hyperlink.

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

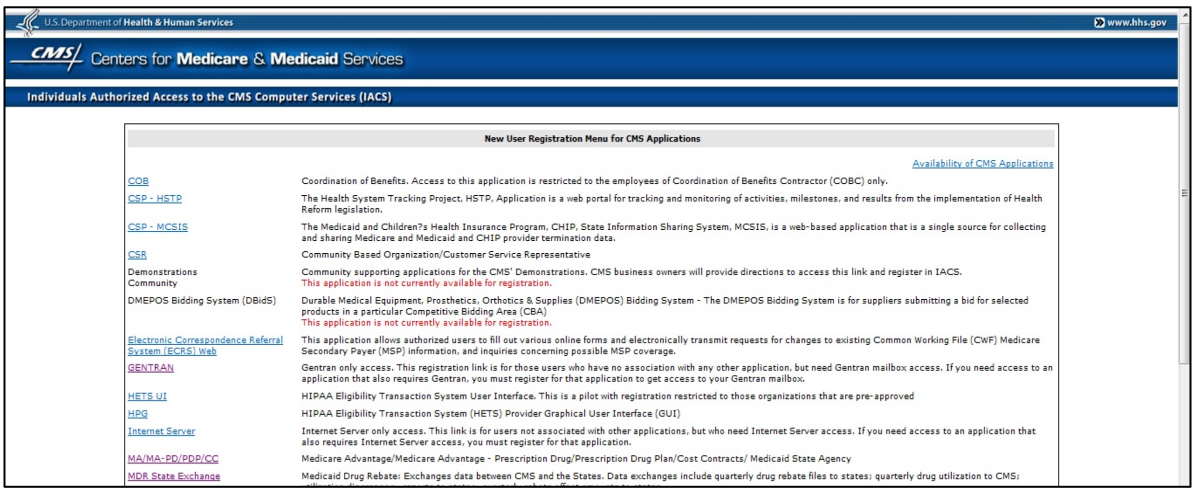


Figure 3: New User Registration Menu Screen

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 Applications*** 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.

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.

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 for 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 data that has been entered.

- 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 ***Cancel*** button is selected, the request will be cancelled and all information that was entered will be lost. A screen indicating this will be displayed. The user must select the ***OK*** button to confirm the action, exit that screen and close the browser window.

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

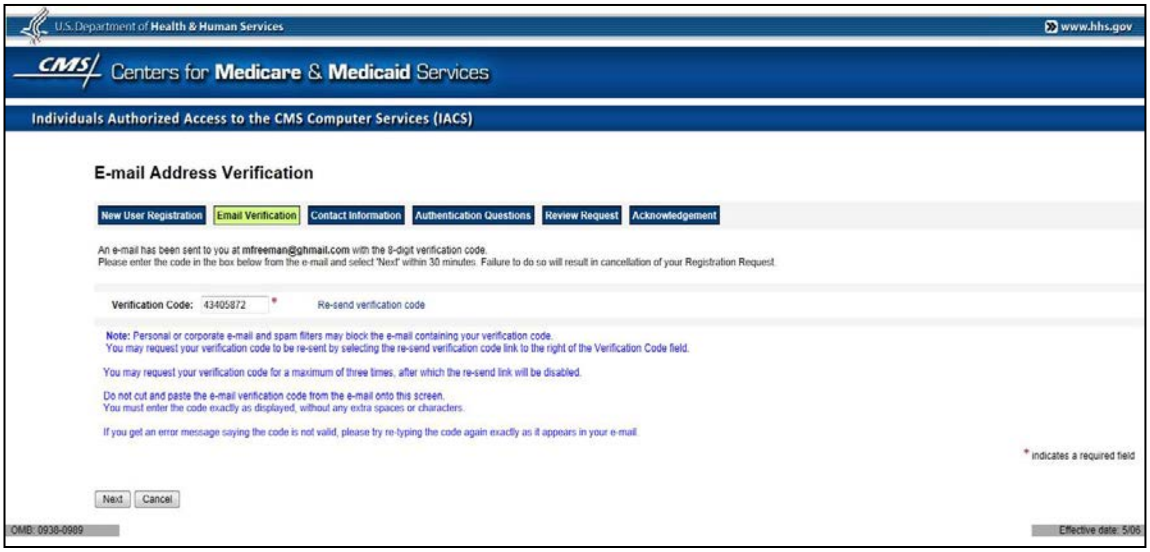


Figure 5: E-mail Address Verification

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.

Action: Leave the **E-mail Address Verification** screen open.

Note: The user will have 30 minutes to complete this step of the registration process. If the user does not complete this step in 30 minutes or if the user closes the **E-mail Address Verification** screen, his request will be cancelled and all information that he had entered will be lost.

Action: Proceed to the E-mail Inbox and open the message with the verification code. The E-mail subject line will be: ***IACS: Email Address Verification.*** Record the verification code that 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 resent up to three times. The user may also contact the Help Desk if he needs assistance or does not receive the E-mail 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.

If the ***Cancel*** button is selected, the application request will be cancelled and all information that was entered will be lost. A screen indicating this will be displayed. The user must select the ***OK*** button to confirm the action, exit that screen, and close the browser window.

Once the user has his 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.

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.

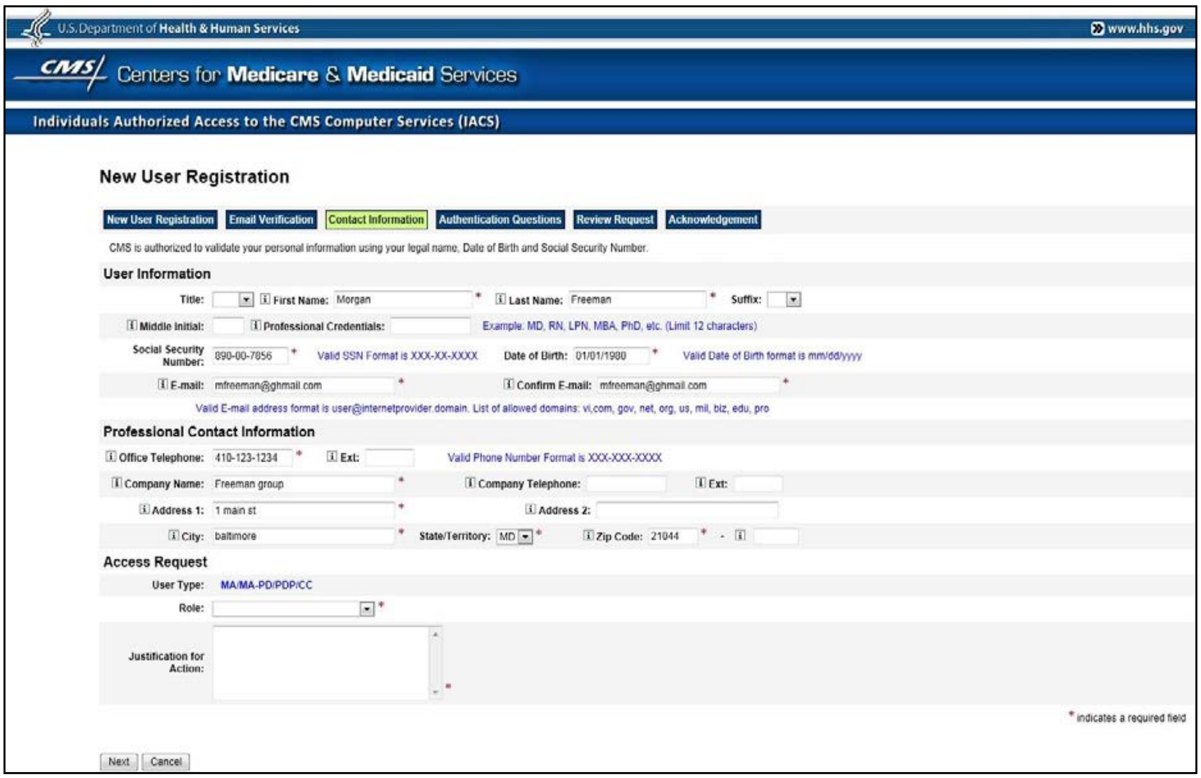


Figure 6: New User Registration Screen: Contact Information

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 that the user completed prior to his E-mail address verification. The user may modify the information that he wants except for the previously entered E-mail address in the ***User Information*** section.

The center of the screen contains an area labeled ***Professional Contact Information***. In this area, the user is required to enter his 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.

Note: The MA/MA-PD/PDP/CC Application will be used to illustrate common registration procedures and techniques that apply to registering for access to CMS applications. Depending on the needs of the CMS applications, there will be some minor differences in the information collected and the way the user will select/input this information.

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

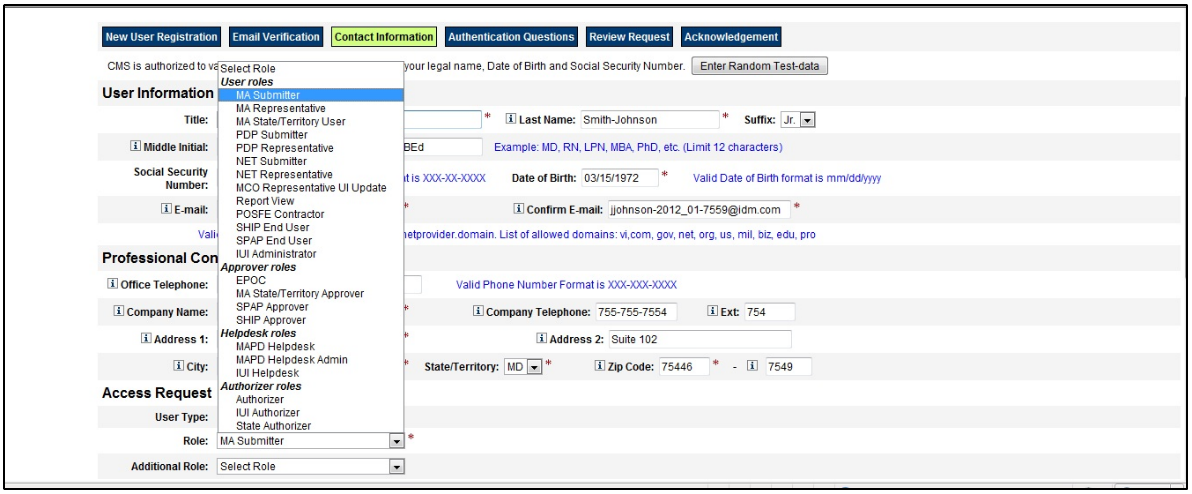


Figure 7: New User Registration Screen: Access Request Area, Role Drop-down

Action: In the *Role* field, select your desired Role***.***

Note: The MA/MA-PD/PDP/CC Application, MA Submitter role, will be used to illustrate common registration procedures and techniques that apply to registering for access to 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, and/or*
  - *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.

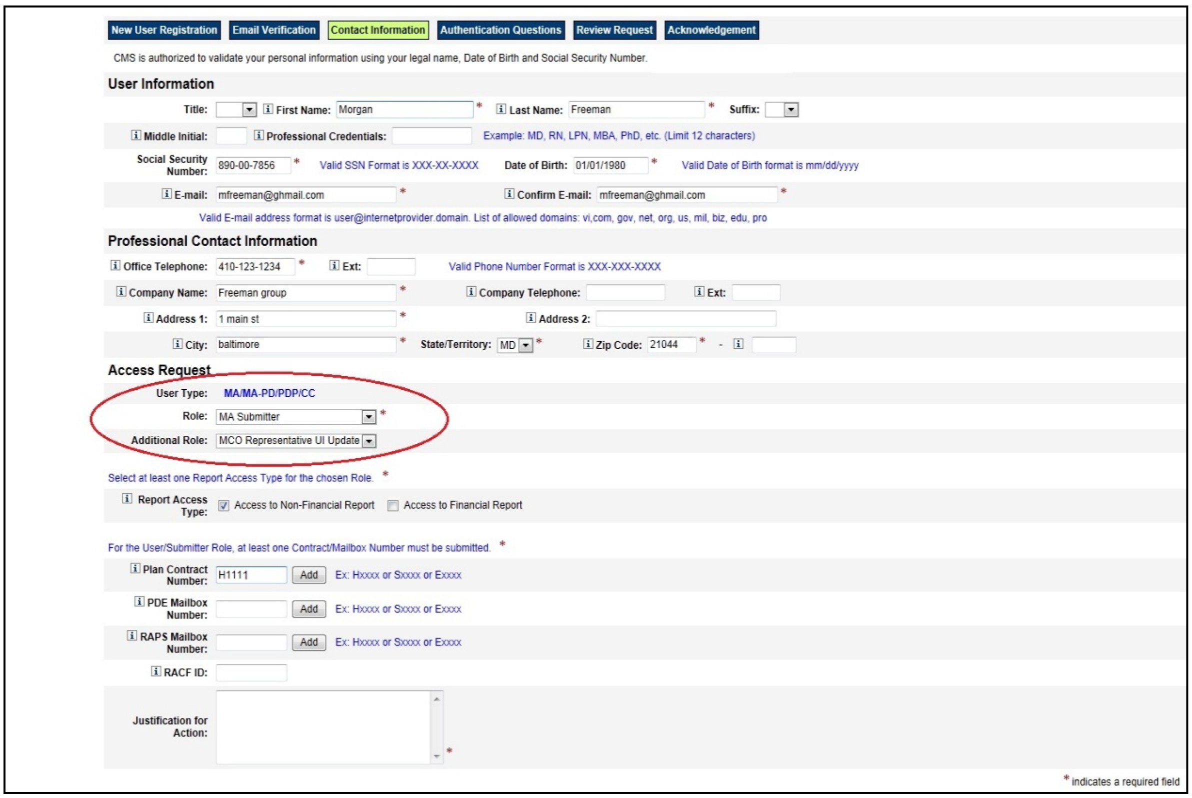


Figure 8: New User Registration Screen: Access Request Area, MA Submitter

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 entered Contract Number fields is an additional field for the user to enter the *RACF ID* if he has this ID number. If the user has forgotten the *RACF ID,* he needs to call the Help Desk to obtain his *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.

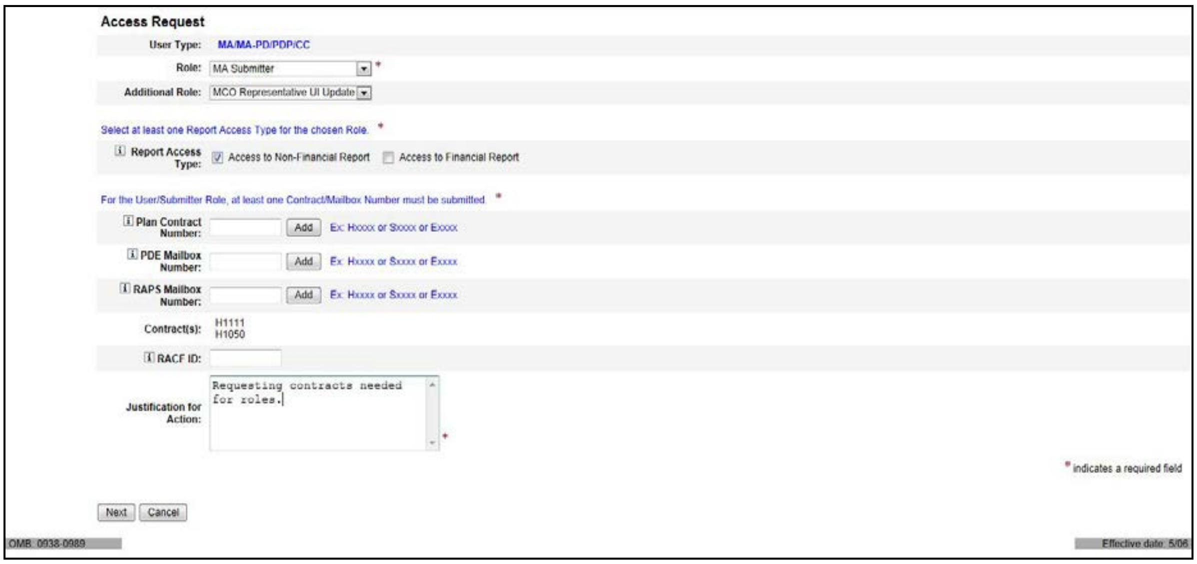


Figure 9: New User Registration Screen: Access Request Area, Contract Number & RACF ID Field – MA Submitter

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

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

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

If the user selects the ***Cancel*** button, his application request will be cancelled and all information that was entered will be lost. A screen indicating this will be displayed. The user must select the ***OK*** button to confirm the action, exit that screen, and close the browser window. The system will then return the user to the **CMS Applications Portal Introduction** 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' self-service features, ***Forgot your User ID?*** or ***Forgot your password?***.

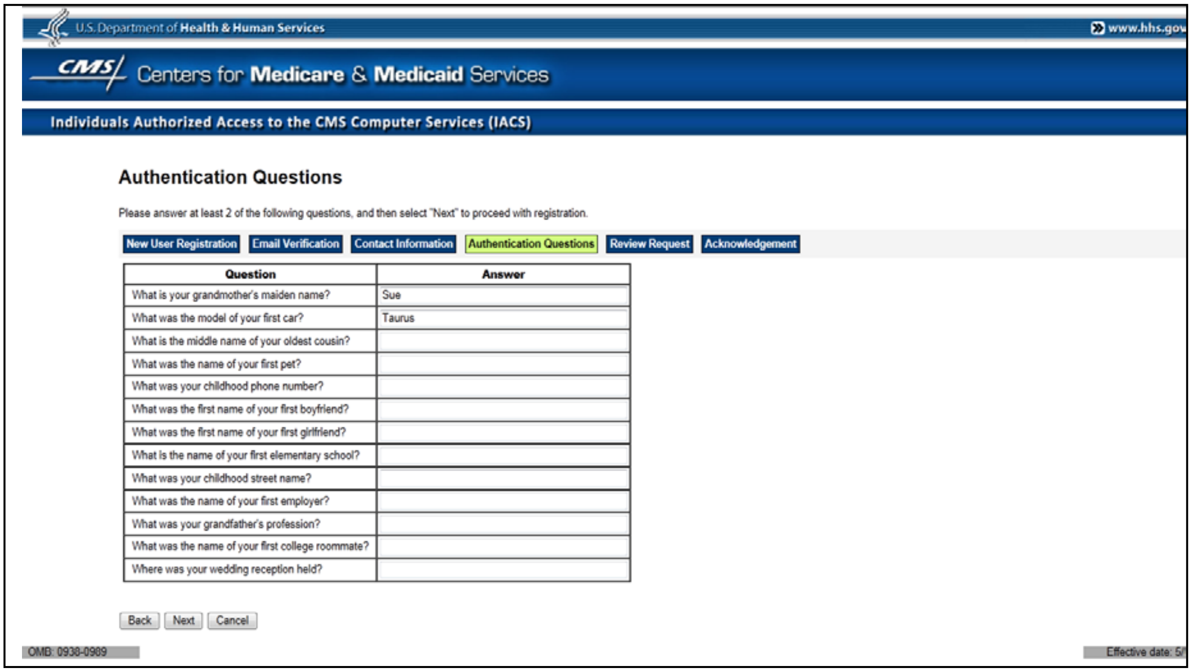


Figure 10: Authentication Questions Screen

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

Action: Select the ***Next*** button when you are done.

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

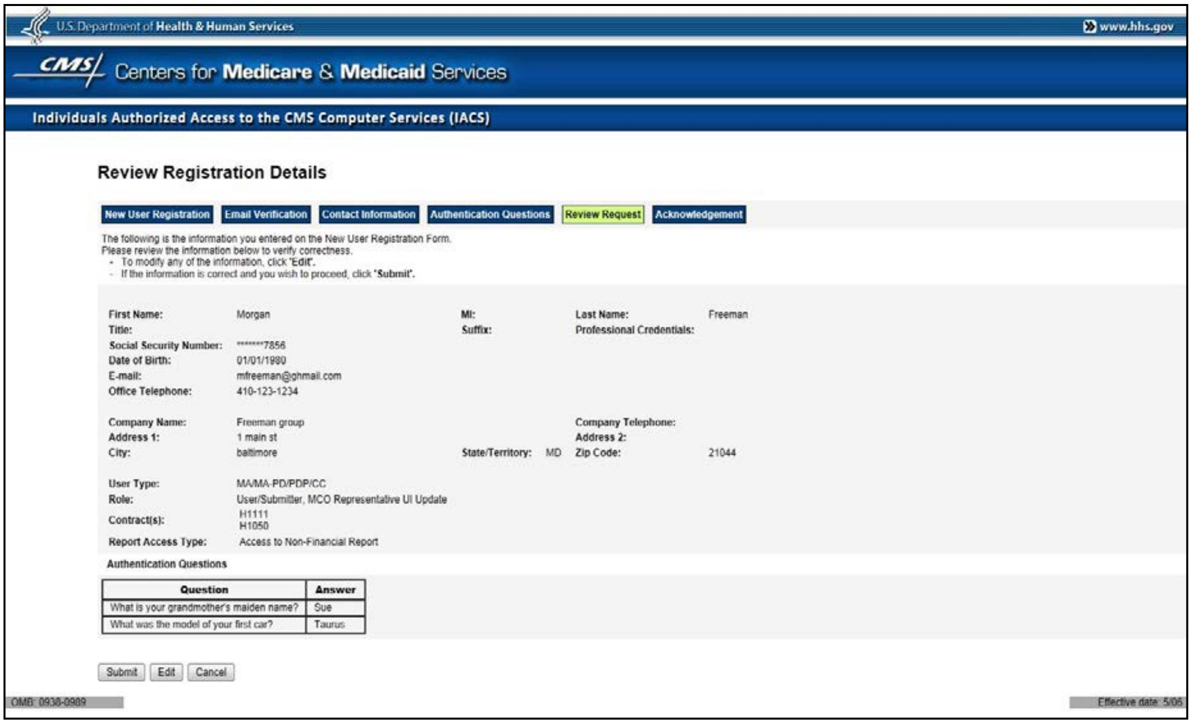


Figure 11: Review Registration Details Screen

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

If you need to make any modification 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 that he wants 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.

If the user selects the ***Cancel*** button, the application request is cancelled and all information he entered will be lost. A screen indicating this will be displayed. He must select the ***OK*** button to exit that screen. The system will then return him to the **CMS Applications Portal Introduction** 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 if 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.

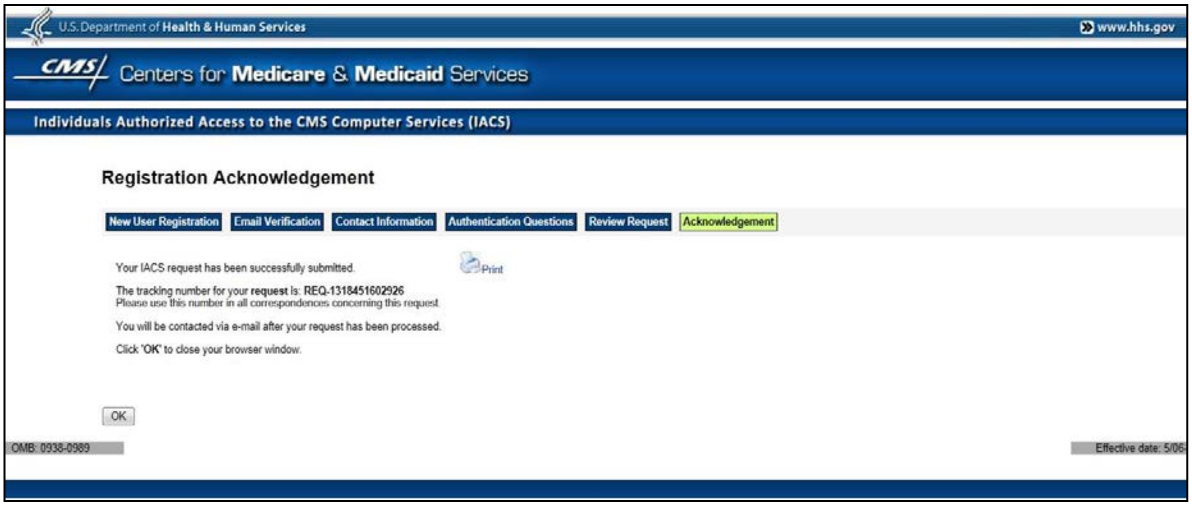


Figure 12: Registration Acknowledgement Screen

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

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

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

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 the user registers, he will need to contact his Help Desk. See Section 16.4 for Help Desk contact information.

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

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

1. The first (Subject: FYI: User Creation Completed – Account ID Enclosed) will contain the IACS User ID.

2. The second (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 his initial password the first time he logs in.

If the user's request for registration is denied, the user will be sent an E-mail informing him that his request has been denied. The E-mail will also include the justification for the denial.

If the Approver or 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.

6.3 Application Specific Registration

6.3.1 COB Registration

- The User/Transmitter registering for COB Application will have to enter an Organization Number and select Organization Identifier from a drop-down list.
- RACF ID is not required.

6.3.2 CSR Registration

- The Approver and User registering for CSR Application will select a Call Center from a list of existing call centers.
- RACF ID is not required.

6.3.3 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
- All users registering for the **DMEPOS Application** have to provide the Provider Transaction Access Number (PTAN).
- A user who is registering as an Authorized Official should enter the Organization Name.
- A user who is registering as an Authorized Official can be associated with more than one PTAN.

6.3.4 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.
- Users registering for the Gentran User role will be able to input one or more Gentran mailbox numbers in a multi-text input box.
- Users registering through this (Gentran) link will also need to complete a CMS Form 20037, have the CMS Business Owner sign as “1st Approver”, and fax it to IACS Administration to gain access to the desired Gentran mailbox.

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

6.3.5 HETS UI Registration

- The user registering as a Security Official, Approver, and End User must enter NPI and Select Provider Type.
- The user registering as a Security Official will have to complete the EDI Registration Form to create an organization. Security Official should enter at least one Contractor Name. The Associated Billing NPI is required.

6.3.6 HPG Registration

- The 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.

Note:

- 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.

6.3.7 Internet Server Registration

- The user registering as an Internet Server User will be required to enter the Business Application 3 Letter High Level Qualifier.

6.3.8 MA/MA-PD/PDP/CC Registration

Users registering 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 can only enter Contracts starting with ‘H’, ‘E’, ‘S’, and ‘9’.

- A user registering as an MA Submitter or MA Representative can add an additional role using the *Additional Role* drop-down list that provides the available roles 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 reports or both, by selecting the appropriate *Report Access Type* check boxes.

MA State/Territory Approver:

- A user registering as a MA State Territory Approver /User will have to select a State from a list of all states.

MA State/Territory User:

- A user registering as a MA State Territory Approver /User will have to select a State from a list of all states.
- A user registering as a MA State/Territory User can add an additional SPAP End User role using the *Additional Role* drop-down list on the **New User Registration** screen.

MCO Representative UI Update:

- A user registering as an MCO Representative UI Update can only enter Contracts starting with ‘H’, ‘E’, ‘S’, and ‘9’.
- A user registering as an MCO Representative UI Update can add an additional role 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.
- The user can 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 reports or both by selecting the appropriate *Report Access Type* check boxes.

PDP Submitter and PDP Representative:

- A user registering as a PDP Submitter can only enter contracts starting with ‘S’, ‘E’, and ‘9’.
- A user registering as a PDP Submitter or PDP Representative can add an additional role 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 reports or both by selecting the appropriate *Report Access Type* check boxes.

Report View:

- A user registering as a Report View can add an additional role 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 reports 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 have to select a State/Territory from the list of states/territories.

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 have to select a State/Territory from the list of states/territories.
- A user registering as a SPAP End User can add an additional MA State/Territory User role using the *Additional Role* drop-down list on the **New User Registration** screen.

6.3.9 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.
- A user registering as a MED User can provide Contract Number, Agency name and COR Name.

6.3.10 Novitasphere Registration

- A user registering as a Provider Office Approver, Billing Office Approver, or Novitas Solutions Approver will create the organization.
- A user registering as a Provider Office Approver will be required to provide the Legal Business Name, Tax ID, and NPI-PTAN-Submitter ID combinations. The organization NPI-PTAN-Submitter ID combination should be in the following format: NP1,PTAN1,SubmitterID1,NPI2,PTAN2,SubmitterID2 etc.

- A user registering as a Business Office Approver role will be required to provide the Legal Business Name, Tax ID, and Submitter ID. The Submitter ID should be in following format: SubmitterID1,SubmitterID2 etc.
- A user registering as a Novitas Solution Approver role will be required to provide the Legal Business Name and Tax ID. The NPI-PTAN-Submitter ID must be blank.
- A user registering as a Back-up Approver or Novitasphere End User will be able to search and associate to an organization as needed.

6.3.11 PQRS/eRx Registration

Security Official:

- A user registering as a Security Official may choose either to create a new organization or associate to an existing organization.
- A user registering as a Security Official will have the option to select the 2-Factor Authentication Approver Role.
- The SO for PQRS/eRx will be able to enter multiple NPI and PTAN values during New User Registration.

Backup Security Official:

- The user will be required to search and associate to an existing PQRI Organization during the registration process.
- A user registering as a Backup Security Official will have the option to select the 2-Factor Authentication Approver Role.
- The BSO 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 2-Factor Authentication Approver Role for the organization selected by the user.
- The user will be able to choose the preferred 2nd factor pass code notification method by selecting the E-mail, SMS/Mobile or Interactive Voice Response Number (IVR) from the drop-down labeled as *Preferred 2nd Factor Passcode Notification Method*.
- The user will be required to enter the Mobile Phone Number if the SMS/Mobile was selected as the Preferred 2nd factor pass code notification method.
- The user will be required to input the Interactive Voice Response Number if the IVR Number was selected as the Preferred 2nd factor pass code notification method.
- The user will be required to search and associate to an existing PQRI Organization during the self-registration process.

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 PQRI Organization during the self-registration process.

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 pass code notification method by selecting the E-mail, SMS/Mobile or Interactive Voice Response Number (IVR) from the drop-down labeled as *Preferred 2nd Factor Passcode Notification Method*.
- The user will be required to enter the Mobile Phone Number if the SMS/Mobile was selected as the Preferred 2nd factor pass code notification method.
- The user will be required to input the Interactive Voice Response Number if the IVR Number was selected as the Preferred 2nd factor pass code 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 pass code notification method by selecting the E-mail, SMS/Mobile or Interactive Voice Response Number (IVR) from the drop-down labeled as *Preferred 2nd Factor Passcode Notification Method*.
- The user will be required to enter the Mobile Phone Number if the SMS/Mobile was selected as the Preferred 2nd factor pass code notification method.
- The user will be required to input the Interactive Voice Response Number if the IVR Number was selected as the Preferred 2nd factor pass code notification method.

Registry End User:

- A user registering as a Registry End User will be able to select an organization from a pre-defined list of Registry 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 appropriate radio button option.
- 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 pass code notification method by selecting the E-mail, SMS/Mobile or Interactive Voice Response Number (IVR) from the drop-down labeled as *Preferred 2nd Factor Passcode Notification Method*.
- The user will be required to enter the Mobile Phone Number if the SMS/Mobile was selected as the Preferred 2nd factor pass code notification method.
- The user will be required to input the Interactive Voice Response Number if the IVR Number was selected as the Preferred 2nd factor pass code notification method.
- The user will be required to search and associate to an existing PQRI Organization if he chooses to associate to an 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 to the system by selecting the appropriate radio button option.
- The user will be required to search and associate to an existing PQRI 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.

6.3.12 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 during the self-registration process.

PS&R Security Official:

- A user 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) during the self-registration process.

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 during the self-registration process.

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.

6.3.13 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.

6.4 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 with "how to" instructions to open a Service Request (SR) to IACS Administrators indicating their approval or rejection of the requests, as shown below:

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 is described in Section 5.0.

7.0 Using IACS

7.1 IACS Login

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

- Reset password
- "Forgot Your Password?" self-service recovery
- "Forgot Your User ID?" self-service recovery
- Change password every 60 days
- Add new application or role
- Remove role
- Modify User and Professional Contact Information
- Annual Certification of account

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

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

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 13.

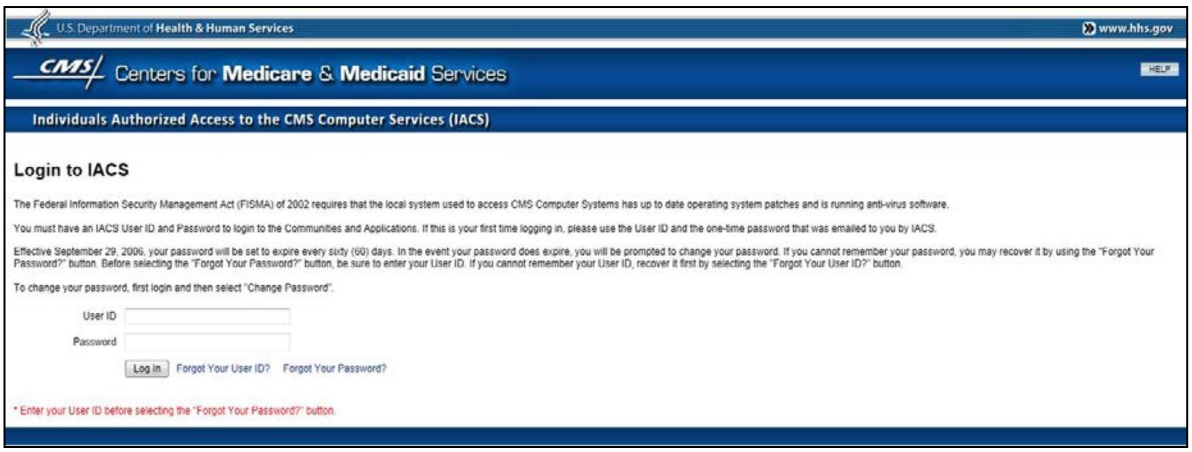


Figure 13: Login to IACS Screen

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 14. Refer to Section 7.2 for more information.

Figure 14: My Profile Screen: MA/MA-PD/PDP/CC Application Users

Action: Select the hyperlink for the function you want or logout.

Note: The first time the user logs into IACS, he will be prompted to change the initial password. After the user has successfully changed the initial password, 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 links below to navigate the IACS application. The hyperlinks will be displayed based on the user's role(s).

The following hyperlink is available for all application users, except COB, CSR, HETS UI, and HPG. The application will determine which fields are editable.

- 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 and 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 Look-up
    - 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

The following hyperlink is available to the IACS Administrator.

- IACS Administration Page (Alternate method of performing help desk functions. This feature will be removed in the next IACS release.)

8.0 Managing User IDs & Passwords

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

- The password must be changed every 60 days.
- The password must be eight characters long.
- The password may not begin with a number.
- The password must contain at least one letter and one number (no special characters).
- Letters must be mixed case. The password must have at least one upper case and one lower case letter.
- The password must not contain the User ID.
- The password must not contain four consecutive characters of 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 - 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.

8.2 Forgot Your Password?

The user needs to follow the steps below to reset his password from the Login screen:

1. On the **Login to IACS** screen, enter the User ID and then select the ***Forgot Your Password?*** button.
2. Enter the last four digits of the SSN and the E-mail address and select the ***Next*** button.
3. When prompted, answer the authentication questions.

4. An E-mail will be sent to the user's account on record with the temporary password.
5. Log in to IACS with the temporary password and change the password.

8.3 Forgot Your User ID?

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

1. From the Login 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 7.0 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*.

8.4 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 180 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.
2. Select the Account Management hyperlink in either 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.

8.5 Locked Account

If the user has not been able to login 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 questions, a one-time password will be sent to the user's E-mail account. The user must log in to IACS with the one-time password and change the password.

The user can also contact the Help Desk for assistance. When the Help Desk unlocks the account, the user can login, with his current User ID and password, if he remembers it, or create another password using Forgot your Password?. If the Help Desk unlocks and resets the user's password, the user will receive a one-time password. The user must log in to IACS with the one-time password and change the password. Refer to Section 16.4 for 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

Note:

- 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 only be allowed to modify the E-mail address.
- The **Modify User/Contact Information** hyperlink will not display for the following applications: COB, CSR,HETS UI, and HPG.

9.1 Modify User/ Contact Information – Change E-mail

When the user selects the Modify User/Contact Information hyperlink, the **Modify User/Contact Information** screen will display as illustrated in Figure 15.

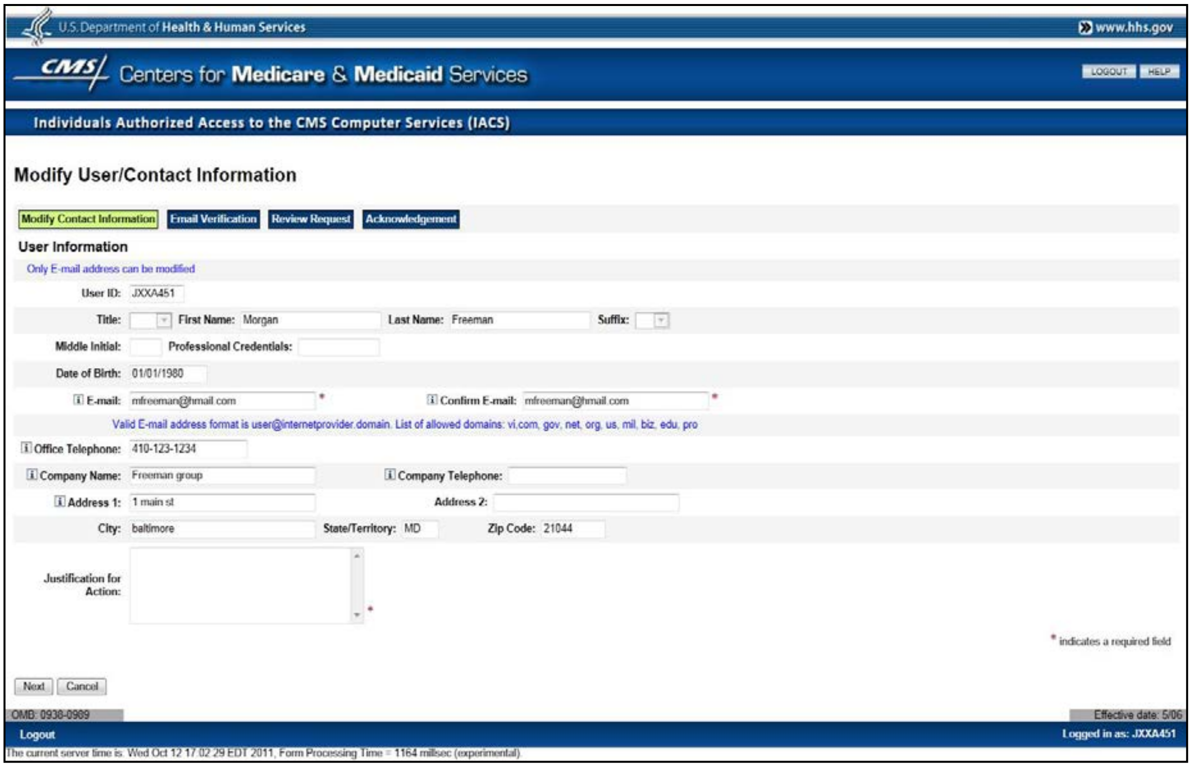


Figure 15: Modify User/Contact Information Screen

Action: Modify the ***User Information*** and/or professional contact as needed***.***

Note: If the user makes changes to his E-mail address, the screen will refresh when he leaves the *E-mail* field after making the changes and a *Confirm E-mail Address* field will appear in which the user must confirm his new E-mail address.

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

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.

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

If the ***Cancel*** button is selected, the request is cancelled and all information that was entered will be lost. A screen indicating this will be displayed. The user must select the ***OK*** button to confirm the action.

The user must follow the instructions for E-mail Address verification as described 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 16.

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

Figure 16: Modify Request Confirmation Screen

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

Note: The modifications will not take effect unless the ***Submit*** button is selected.

If the user selects the ***Cancel*** button, his request will be cancelled and any modification that was entered will be lost. A screen indicating this will be displayed. The user must select the ***OK*** button to confirm the action, exit that screen and close the browser window.

When the user selects the ***Submit*** button**,** a **Modification Request Acknowledgement** screen will display as illustrated in Figure 17**.**

He must select the ***OK*** button to complete the account profile modification**.**

Figure 17: 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 Modify Account Profile process.

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 confirming that IACS has received his request and providing him with a Request Number. He should use that request number to contact the Help Desk regarding the request. The user should also have the request number from the **Modification Request Acknowledgement** screen available for the Help Desk.

If an E-mail notification is not received within 24 hours after the user modifies his profile, he will need to contact the Help Desk. For Help Desk contact information, see Section16.4.

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
- Disassociate from current role
- Add role
- Modify Report Access
- Modify the user's profile, some common options are to associate and/or disassociate with other organizations within an application.

Note: The user cannot be an approver and a user for 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 and show 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*** and professional contact information are displayed.

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 18. 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. These actions are illustrated in the example in Figure 18*.*

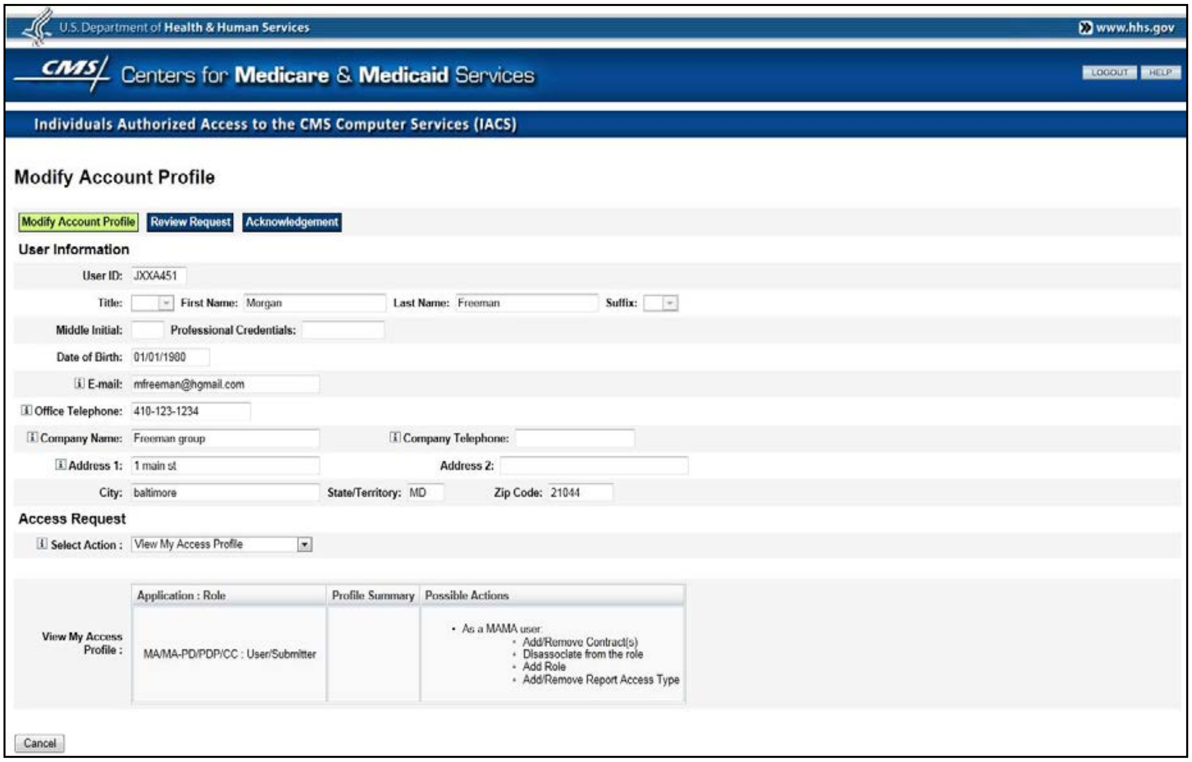


Figure 18: Modify Account Profile Screen: Access Request Area – Select Action Drop-down

10.2 Add Application

If the user selects the action, ***Add Application***, the screen will refresh and he will be presented with a screen where the ***Access Request*** portion is similar to the one shown in Figure 19. The applications he will be able to add are those applications integrated with IACS.

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.

The *Select Application* field contains a drop-down list of the CMS applications integrated with IACS as illustrated in Figure 19.

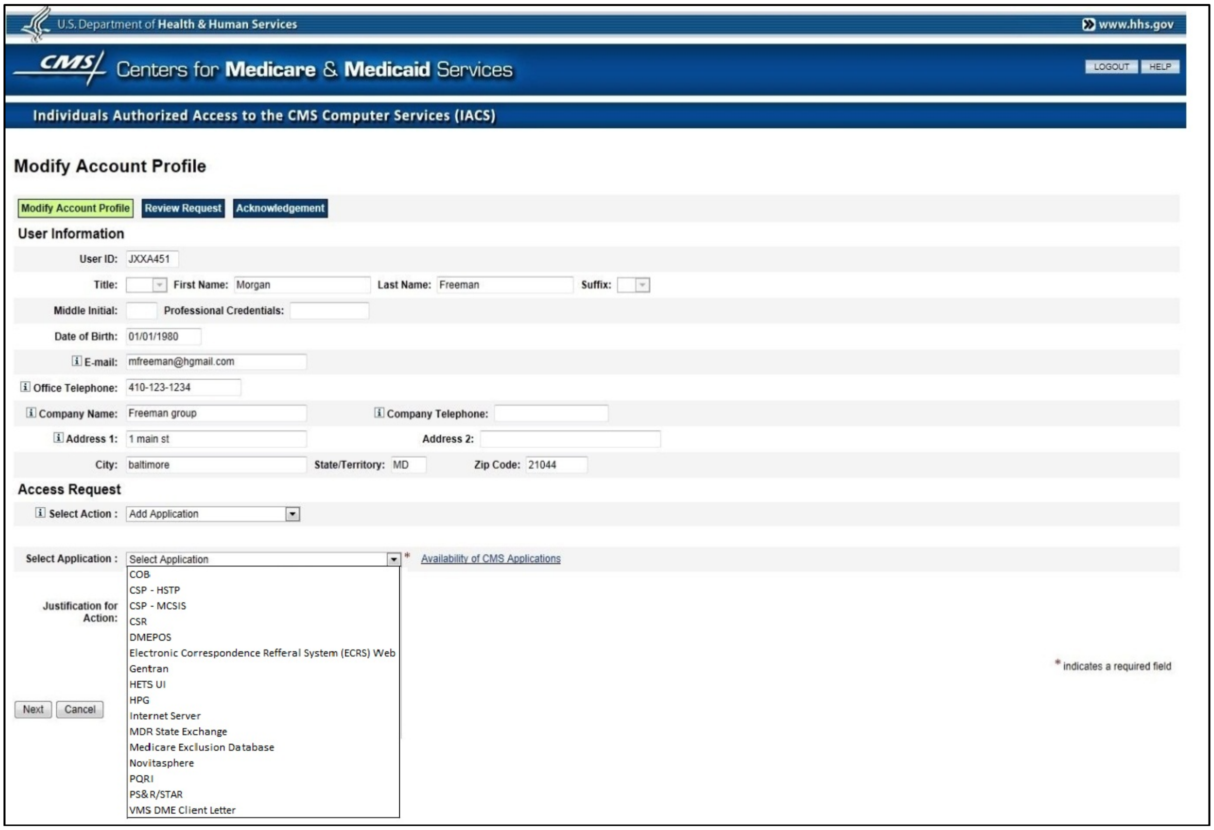


Figure 19: Modify Account Profile Screen: Access Request Area – Select Application Drop-down

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

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 and he will be presented with a screen in which the ***Access Request*** area is similar to the one shown in Figure 20.

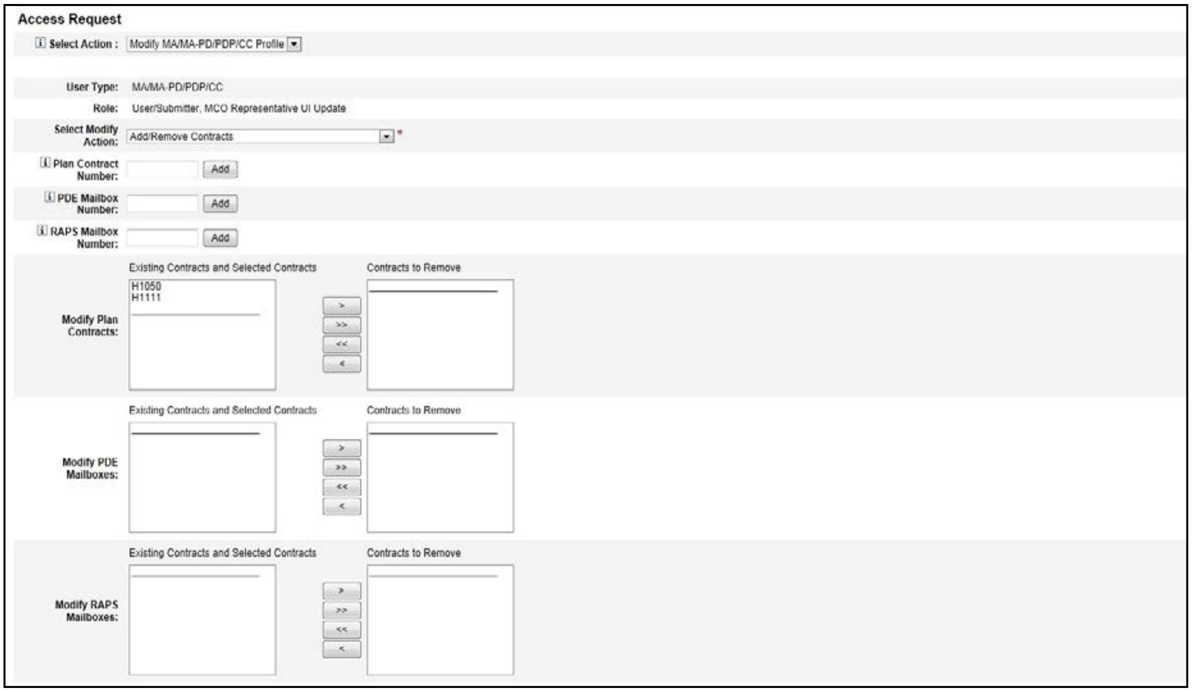


Figure 20: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC User/Submitter Add or Remove Contracts

If the user wants to add a Contract Number to his current list of contract numbers, then he needs to do the following:

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

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

If the user wants to add another contract number, he needs to repeat the above actions.

If the user wants to remove a contract number from his current list of contract numbers, he needs to do the following:

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

Action: Select the box with the right facing arrow.

The system will move the selected contract number to the *Contracts to Remove* box to the right. The user can move the contract number back to the *Existing Contracts and Selected Contracts* box by selecting the box with the left facing arrow.

If the user wants to move all contract numbers in the *Existing Contracts and Selected Contracts* box to the *Contracts to Remove* box, he should select the box with the double right-facing arrow.

The user can move all the contract numbers back to the *Existing Contracts* and *Selected Contracts* boxes by selecting the box with the double left facing arrow.

After making the 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 after entering the justification statement.

The system will display the **Modify Request Confirmation** screen as illustrated in Figure 16.

Refer to Section 9.1or further information on completing the ***Modify Account Profile*** process.

10.4 Disassociate from Current Role

If the user selects the action, ***Modify Profile,*** then selects the option ***Disassociate from User/Submitter Role***, the screen will refresh and a confirmation message and check box will appear in the ***Access Request*** area as illustrated in Figure 21.

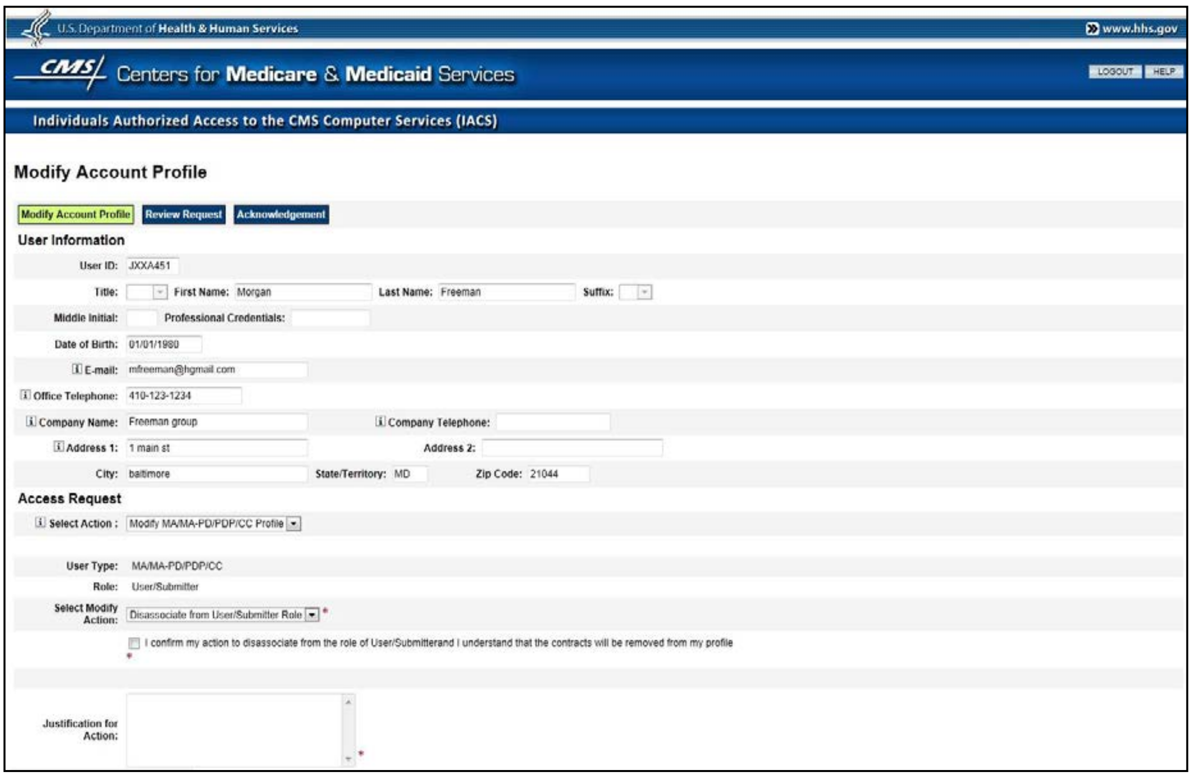


Figure 21: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC User/Submitter Disassociate from Role

Note:

- 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, then, 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 16.

Refer to Section 9.1 for further information on completing the ***Modify Account Profile*** process.

Note:

- 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.
- 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 22.

- *Role* drop-down: User can select a role from the role dropdown
- *Report Access Type* check boxes: User can modify the selection of Access to Financial and Non-Financial report access
- Contract Selection fields: User can Add/Remove contracts.

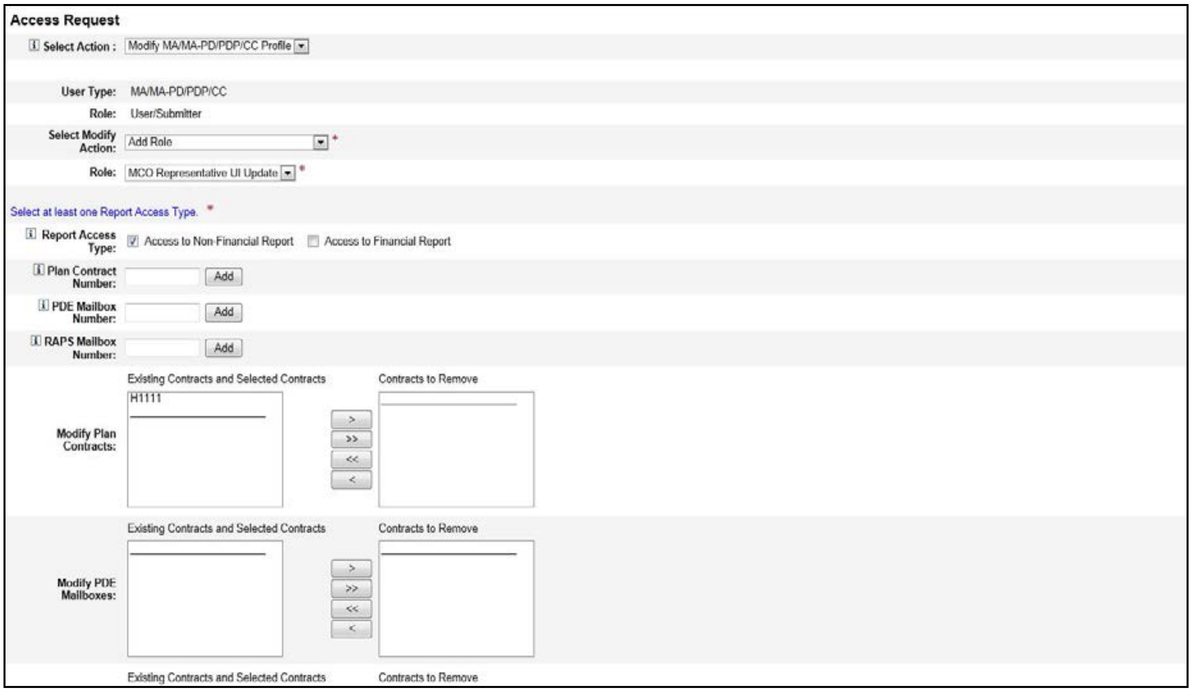


Figure 22: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC Add Role

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

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.

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

Action: Using the Contract Selection fields, add or remove a contract. Refer to Section 10.3 for adding or removing contracts.

After making the 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 16.

Note:

- The following application 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.
- PQRS/eRx Users will be able to request one or more of the following roles within an organization:
  - EHR Submitter
  - End User
  - PQRS Submitter
  - PQRS Representative
- PS&R/STAR Users will be able to request one or more of the following roles within an FI/Carrier/MAC organization and get the roles assigned upon appropriate approval.
  - PS&R User
  - PS&R Admin
  - STAR User 1 – STAR User 8
- PS&R/STAR Users will be able to request one or more of the following roles within a Provider organization and get the roles assigned upon appropriate approval.
  - PS&R User
  - PS&R Admin
- PS&R/STAR System Maintainer will be able to request one or more roles and get the roles assigned upon appropriate approval.
  - PS&R User
  - PS&R Admin
  - STAR User 1 – STAR User 8

10.6 Modify Report Access

Modify Report Access Type function 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 23.

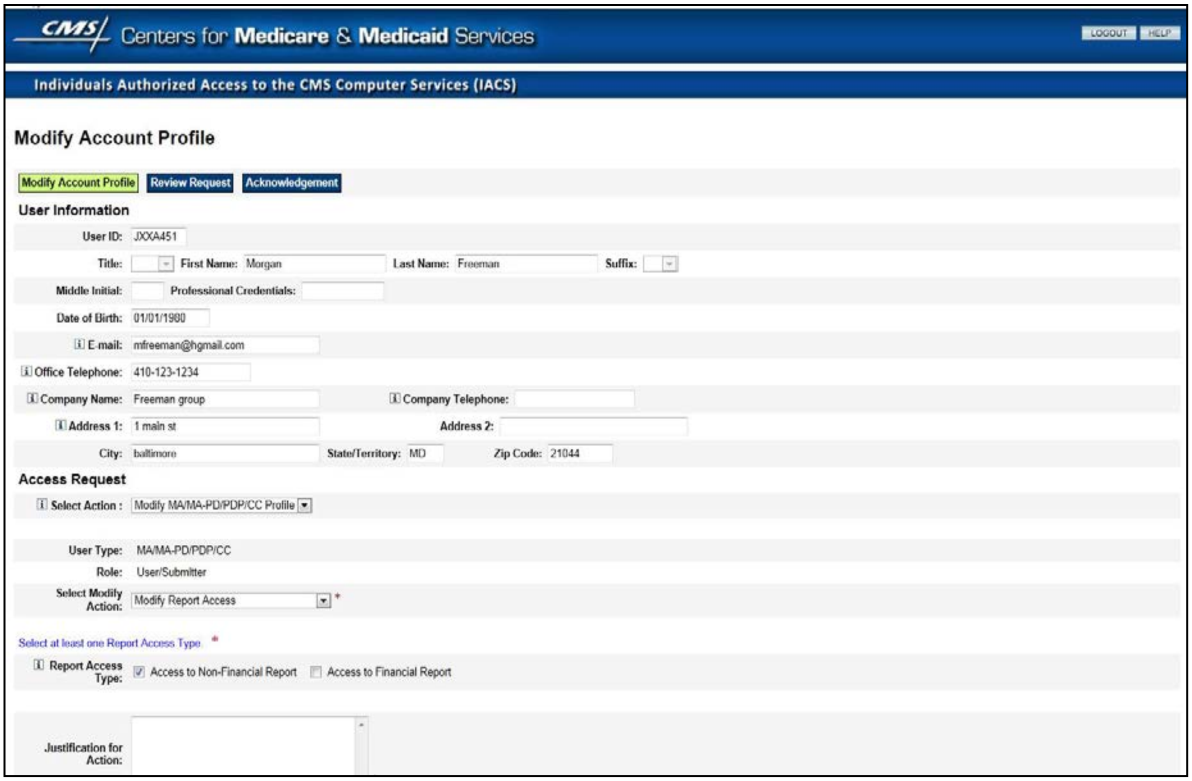


Figure 23: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC Modify Report Access

Action: Select the desired *Report access type*.

Note: User can modify his prior selection of the *Report Access Type*. At least one *Report Access Type* should be selected.

After making the 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 16.

10.7 Modify User 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, 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 role(s) and *State/Territory for Access*.

- Only the roles listed in Table 1 can request an additional role within the MA/MA-PD/PDP/CC Application.
- Modify Report Access Type function will not be applicable for MA/MA-PD/PDP/CC users who do not have access to Gentran mailbox (es).

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 and the Legal Business Name.
- A user registered for the following roles will be able to modify his current selection of preferred 2nd factor pass code notification method using the drop-down labeled as *Preferred 2nd Factor Passcode Notification Method*:
  - EHR Submitter
  - HIE User
  - PQRS Submitter User
  - Individual Practitioner with 2-Factor Authentication
- 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 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 Annual Certification

Starting November 15, 2010 IACS has been enforcing the Annual Certification requirement for all applications supported by IACS. Users registered through IACS for CMS applications are required to certify annually their continued need for access to CMS systems.

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 roles will be slightly different. The E-mail notification will inform the user that he must add a role to his profile in order to maintain the account. The role 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 24. 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.

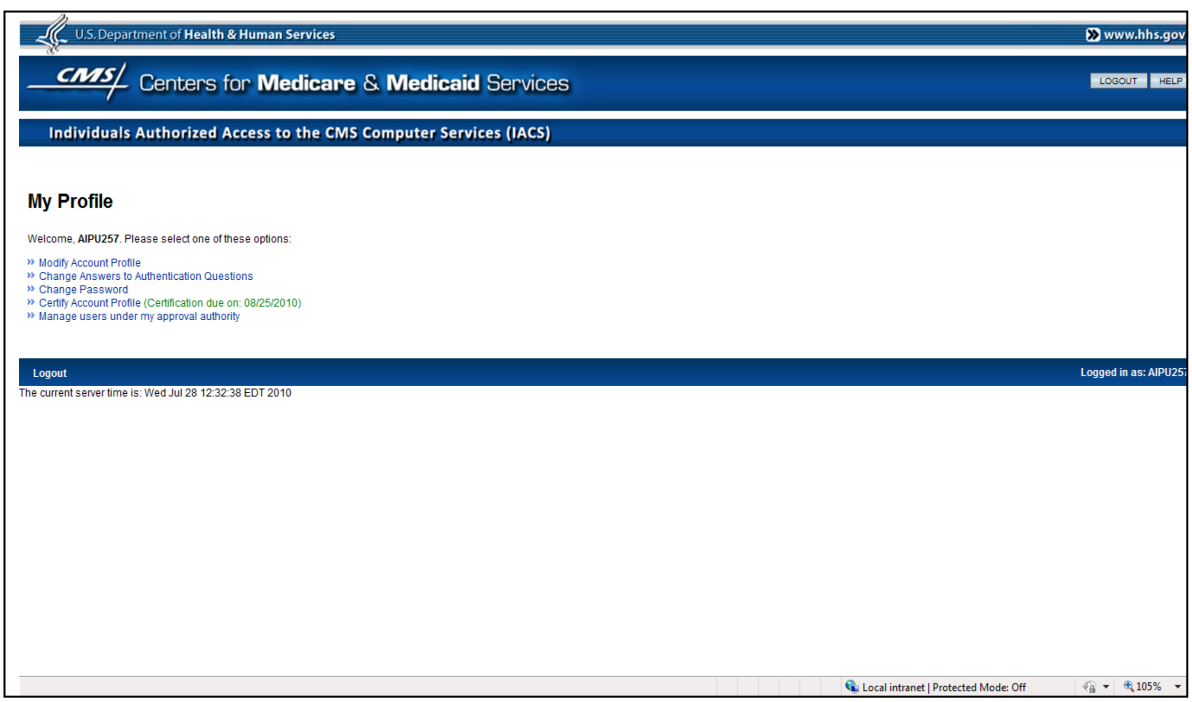


Figure 24: My Profile Screen: Certify Account Profile Hyperlink

The Annual Certification process will be a three-step process**. Step1: Review Account Profile Information** screen will display showing the user's profile as illustrated in Figure 25.

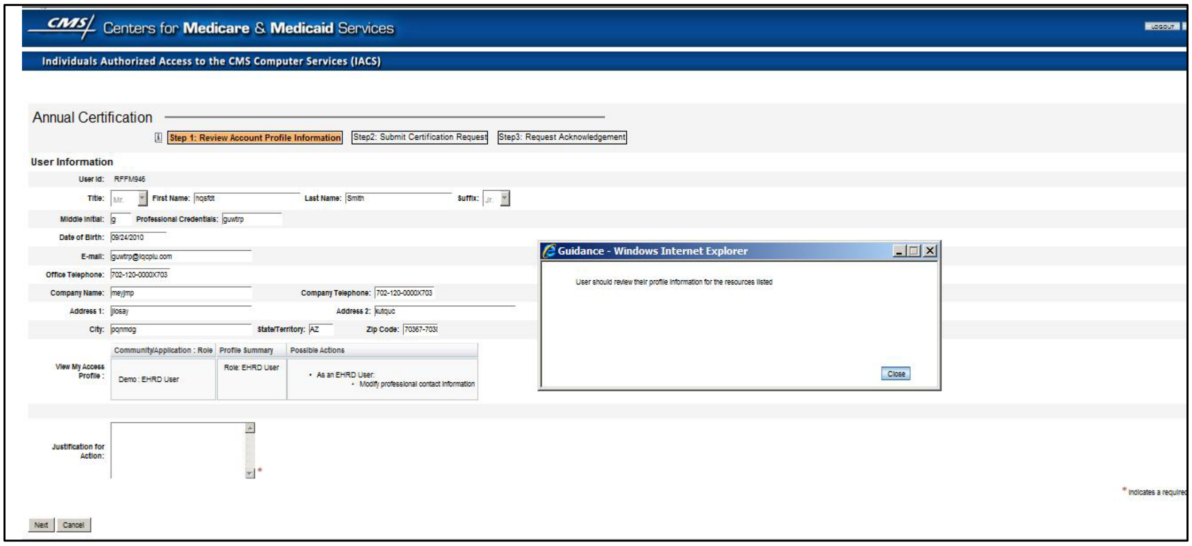


Figure 25: Annual Certification: Review Account Profile Screen

Action: 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 or call centers assigned to their account, IACS will display a message at the top of the page, 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 the appropriate Approver(s) or EPOC(s), or all of them if his request requires multiple 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 IACS requests requiring the Approver's attention. The following are the actions that an Approver takes:

- 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.

Some Helpdesks are at the top of the chain of trust and function as Authorizers of users with Approver roles. The Helpdesks of the applications listed in Table 2 follow this standard and approve the new users' registration, profile modification, and annual certification requests of the users under their approval authority.

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
ECRS	ECRS HelpDesk	EDI Help Desk
GENTRAN	Gentran Helpdesk	IACS Administration
HETS UI	MEIC Helpdesk	MCARE Help Desk
HPG	MEIC Helpdesk	MCARE Help Desk
Internet Server	Internet Server Help Desk	IACS Administration
MDR	Helpdesk	MAPD Help Desk
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
VMS Client Letter	VMS Help Desk	VMS Help Desk

Table 2: Applications and the corresponding Helpdesks with Approval Authority

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 30.

Note: The MA/MA-PD/PDP/CC Application screens will be used to illustrate this search function and other Approver functions. Approval procedures for the PQRS/eRx will be explained in Section 12.1.1.

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

The Approver's **Inbox** screen will display as illustrated in Figure 26. The pending approval requests for New User Registration and account profile modification will be displayed as hyperlinks in a table. The Approver can also search for requests by selecting the Search Request hyperlink. Section 12.1.2 provides details on the search function.

Figure 26: Approver Inbox Screen

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

When the Approver has selected a Pending Approval request to work on, the **Approve / Reject Request** screen will display as illustrated in Figure 27.

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 will be defaulted to the ***Defer*** radio button for all individual items in the request.

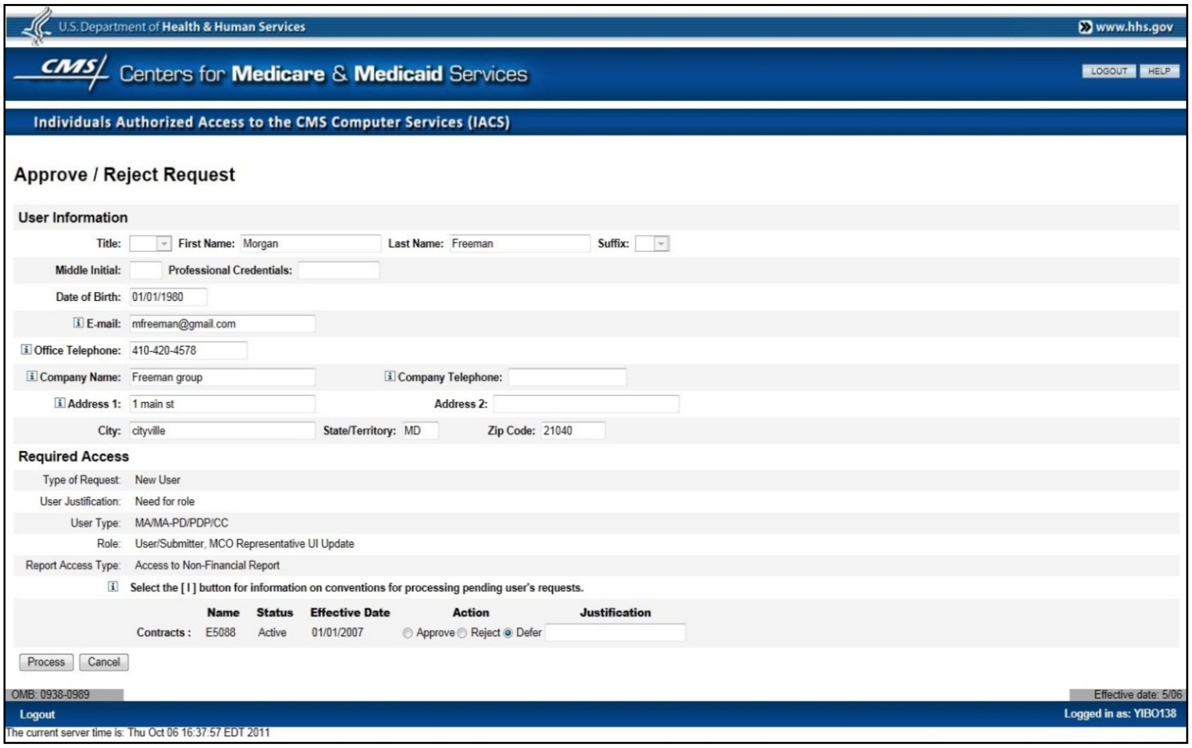


Figure 27: Approve/Reject Request Screen: Required Access Area – Grouped Pending Items

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

Action: Determine, by individual item (*Contracts*), the action you will take.

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 A - Request Timeout Days.

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

If the user selects the ***Cancel*** button at any point during the approval process, a confirmation screen will display to confirm the action. If the ***OK*** button is selected to confirm the cancellation, any action taken will be lost and the user will be returned to the **Inbox** screen. If the ***Cancel*** button is selected from the confirmation screen, any action taken will not be lost and the user will be returned to the **Approve / Reject Request** screen.

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.
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 28.

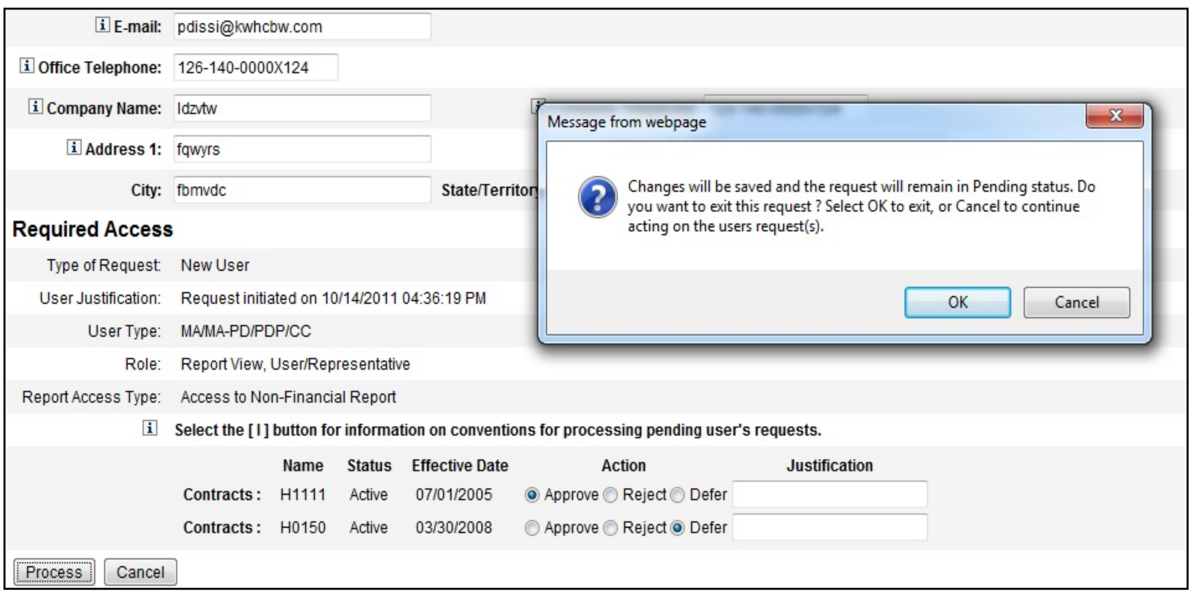


Figure 28: Confirm Action Dialogue box with Deferred Items

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

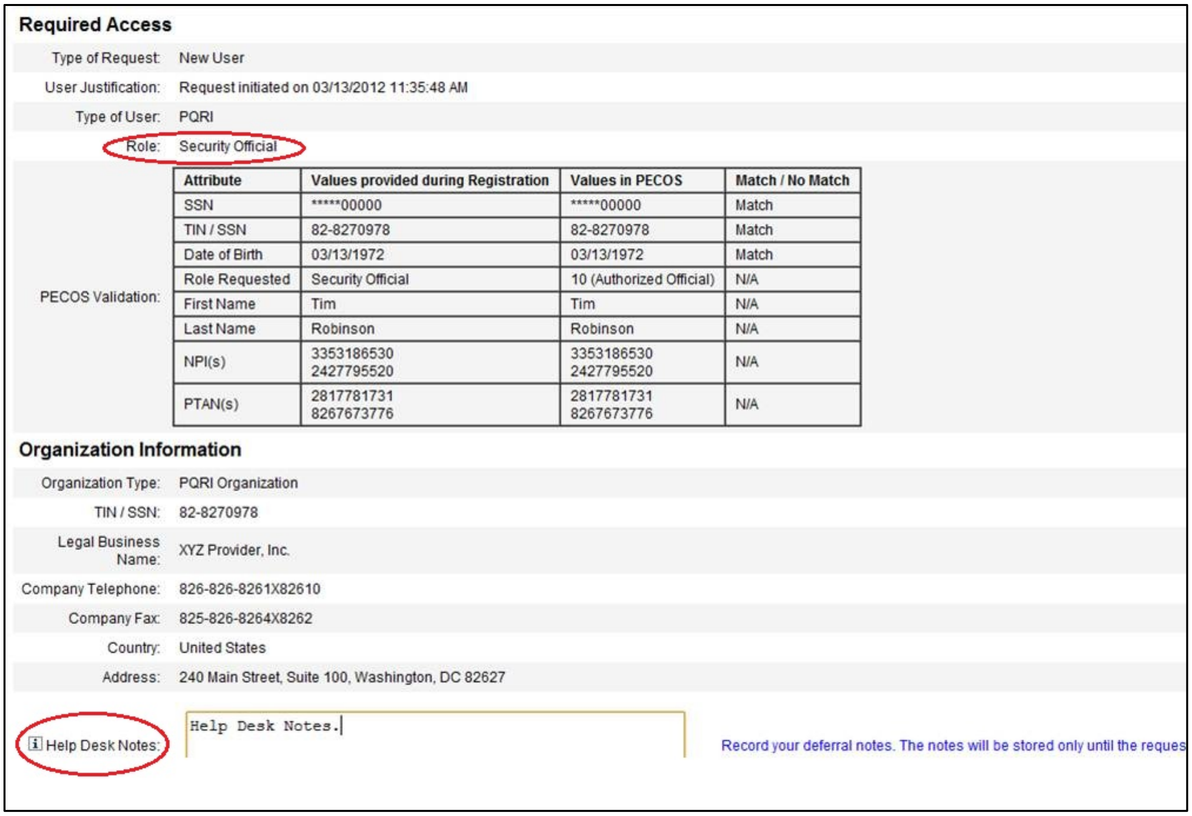
This section describes the **Approve / Reject Request** screen for those registering for the following roles during New User Registration or as a new role for an existing IACS user with no PQRS/eRx role:

- Security Official
- Backup Security Official
- 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 29. This figure represents the SO and BSO approval. The validation table will display the values and the comparison results for SSN, TIN, DOB, Legal Business Name, role requested, first name, and last name. The NPI and PTAN 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 SSN, DOB, first name, last name, NPI, and PTAN.



Required Access

Type of Request: New User

User Justification: Request initiated on 03/13/2012 11:35:48 AM

Type of User: PQRI

Role: Security Official

PECOS Validation:

Attribute	Values provided during Registration	Values in PECOS	Match / No Match
SSN	*****00000	*****00000	Match
TIN / SSN	82-8270978	82-8270978	Match
Date of Birth	03/13/1972	03/13/1972	Match
Role Requested	Security Official	10 (Authorized Official)	N/A
First Name	Tim	Tim	N/A
Last Name	Robinson	Robinson	N/A
NPI(s)	3353186530 2427795520	3353186530 2427795520	N/A
PTAN(s)	2817781731 8267673776	2817781731 8267673776	N/A

Organization Information

Organization Type: PQRI Organization

TIN / SSN: 82-8270978

Legal Business Name: XYZ Provider, Inc.

Company Telephone: 826-826-8261X82610

Company Fax: 825-826-8264X8262

Country: United States

Address: 240 Main Street, Suite 100, Washington, DC 82627

Help Desk Notes: Help Desk Notes.

Record your deferral notes. The notes will be stored only until the reques

Figure 29: 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 to all PQRI Helpdesk users while the request is pending action. Once the request is approved or rejected, the request will be removed from the helpdesk 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(s) function to search for a specific request by providing the search criteria.

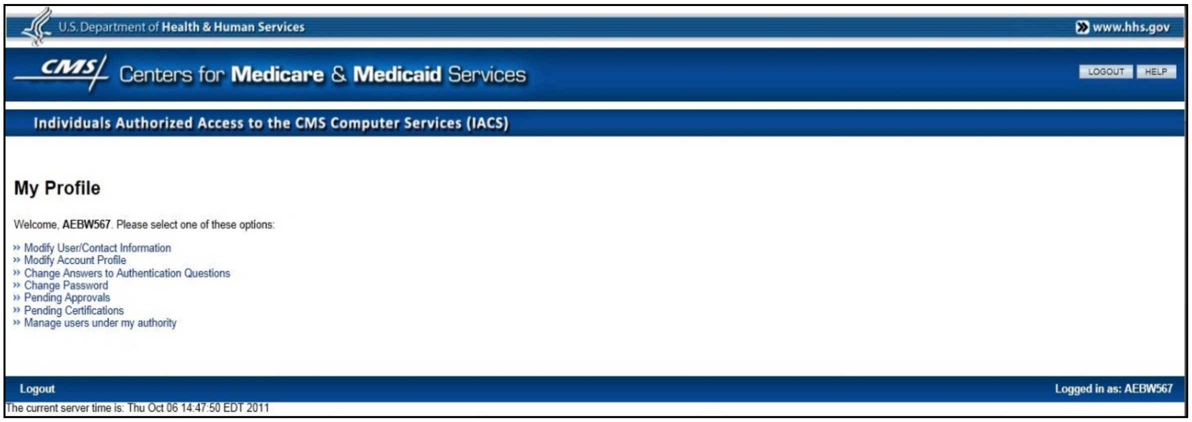


Figure 30: My Profile Screen

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

The Approver **Inbox** screen will display as illustrated in Figure 31. 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.

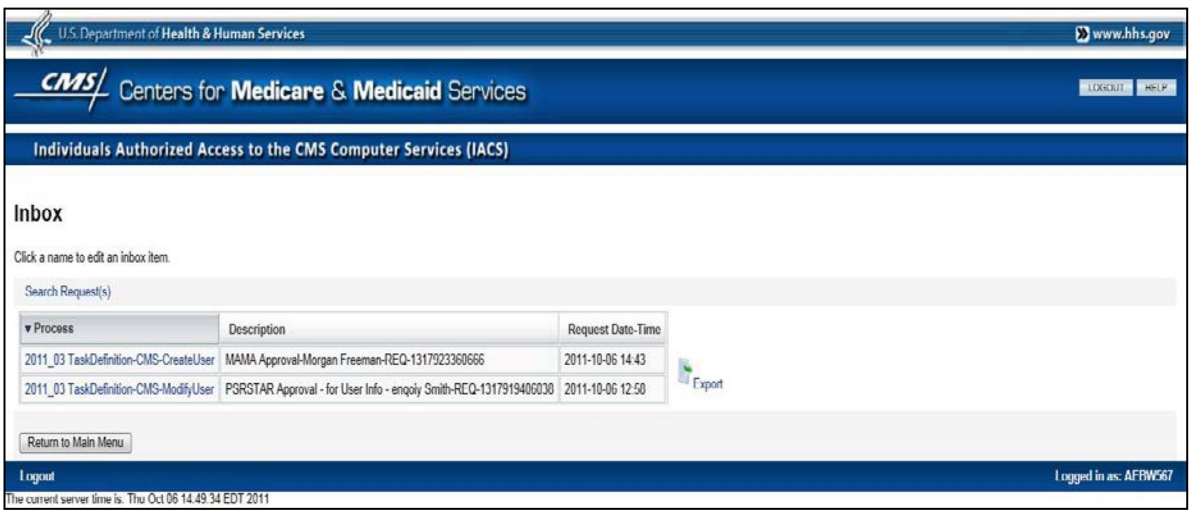


Figure 31: Approver Inbox Screen: Search Request(s) Hyperlink

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 32.

> **Note:** This function is currently only available for the MA/MA-PD/PDP/CC, CSP-HSTP, CSP-MCSIS, ECRS, Gentran, Internet Server, MDR, MED, Novitasphere, PS&R/STAR, and VMS Client Letter applications.

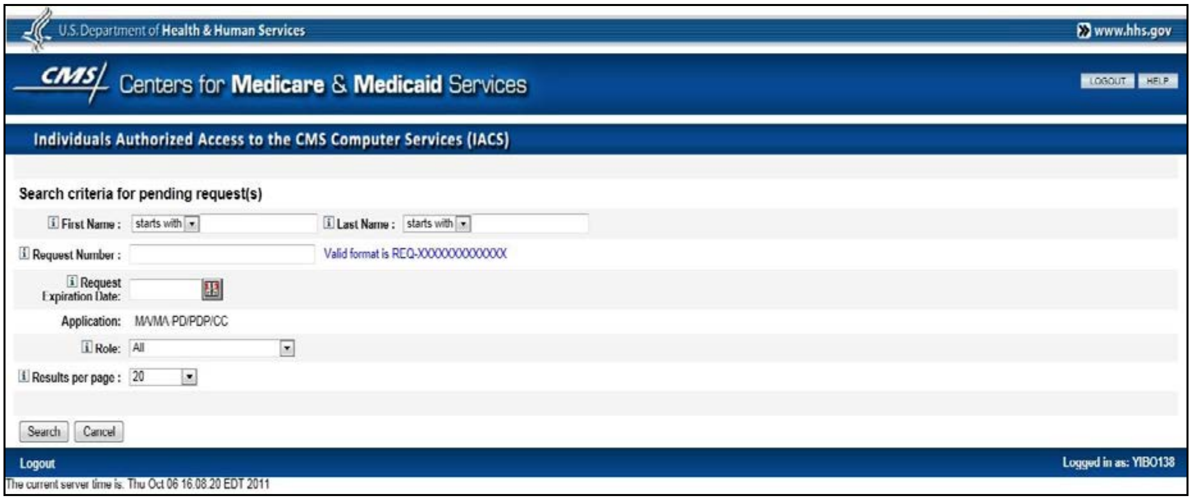


Figure 32: Search Criteria for Pending Request(s) Screen

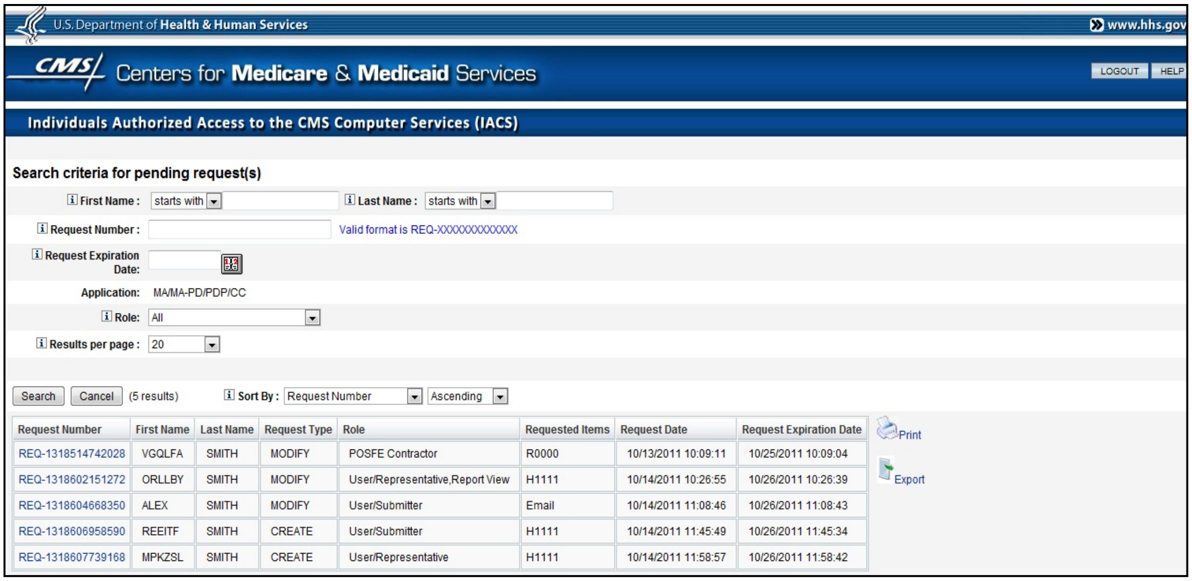
Action: Select the desired search criteria by entering the appropriate data in the search fields or selecting from the available drop-down lists.

Note:

- 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 when you have finished selecting your search criteria.

The screen will refresh and the search results will display at the bottom of the screen as illustrated in Figure 33.



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 33: Search Criteria for Pending Request(s) Screen: Search Results

Action: Select the hyperlink of the pending approval request you want 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 MA/MA-PD/PDP/CC, CSP-HSTP, CSP-MCSIS, ECRS, Gentran, Internet Server, MDR, MED, Novitasphere, PS&R/STAR, 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 Requests

The Search and View (only Pending Requests) hyperlink is available to the PQRI Help Desk, PS&R Help Desk, and MCARE (MEIC) Help Desk to search pending requests by the Request Tracking Number.

Enter the pending request tracking number and select the ***Search*** button. If the request is found, the user will be able to process 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 Authorizers will receive an E-mail advising him when an approver, under his authority, fails to perform annual certification. This E-mail will be sent to the Authorizers 14 days, 7 days, and one day before the certification due date unless the approver submits certification. This E-mail is sent to Authorizers if an approver has any 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 Approver(s) or EPOC(s), or all of them if his request requires multiple 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 in Section 12.3.1.

The certification request from the top of the chain users will be sent to the corresponding Business Owners who will open a Service Request (SR) with an IACS Administrator advising their approval/rejection decision on 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 30.

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 34.

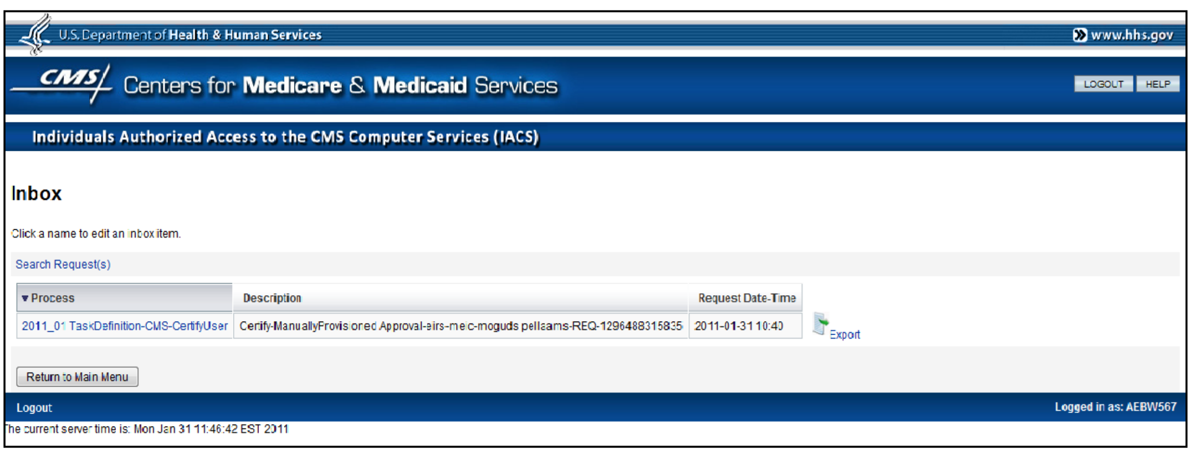


Figure 34: Inbox listing Pending Certification

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

The **Approve / Reject Request** screen will display as shown below in Figure 35.

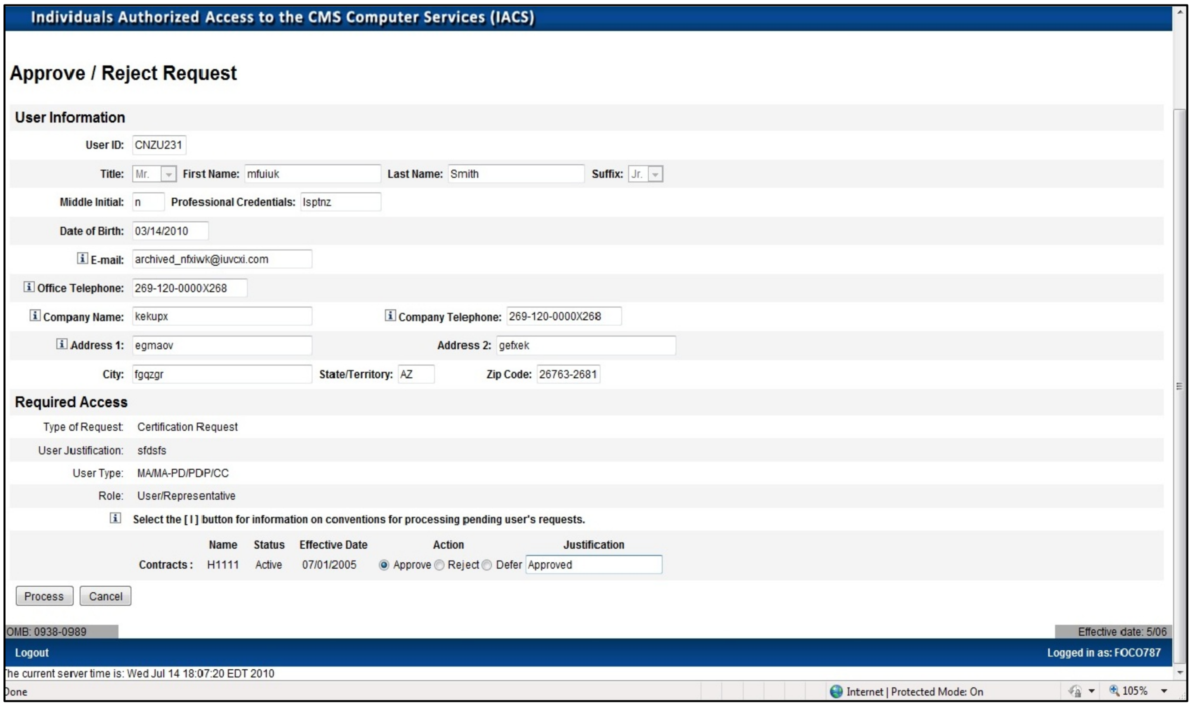


Figure 35: Approve / Reject Request Screen: Certification Request

Action: Review the requestor's information.

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

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

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 AO, SO, EPOC, and Helpdesk users with the 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 as 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	MEIC Helpdesk	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, 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 user 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 30.

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 36. The appropriate *Search criteria* will display based on the Approver's approval authority and the application.

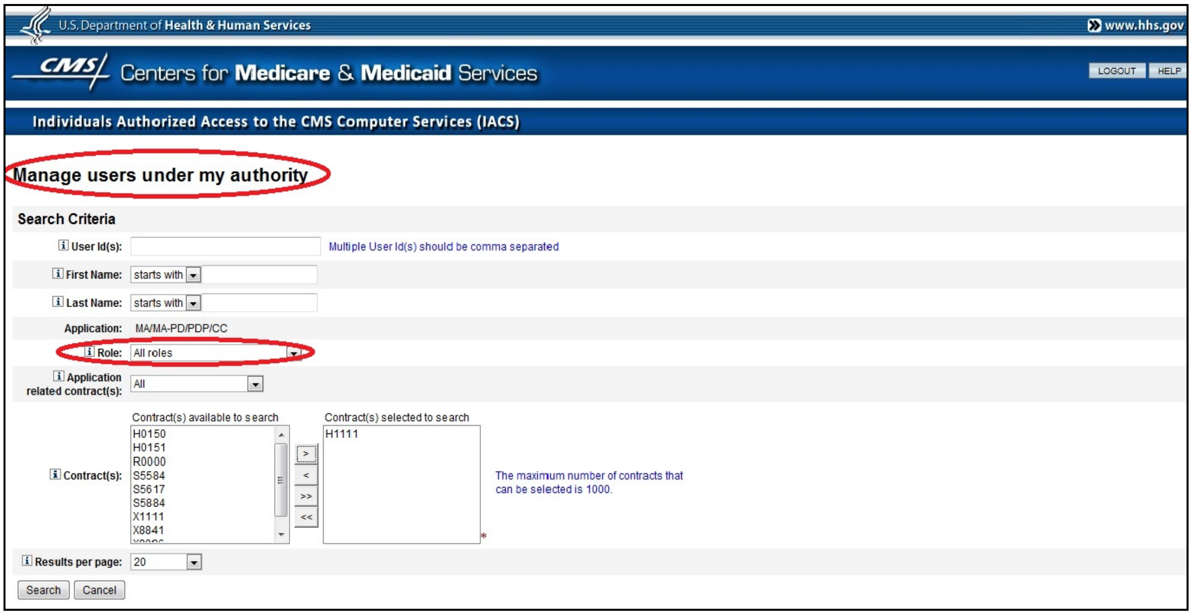


Figure 36: Manage user under my authority – Search Criteria

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

Action: Select the ***Search*** button when you have finished selecting your search criteria.

The screen will refresh and the search results will display in a table under the ***Search Criteria*** area as illustrated in Figure 37.

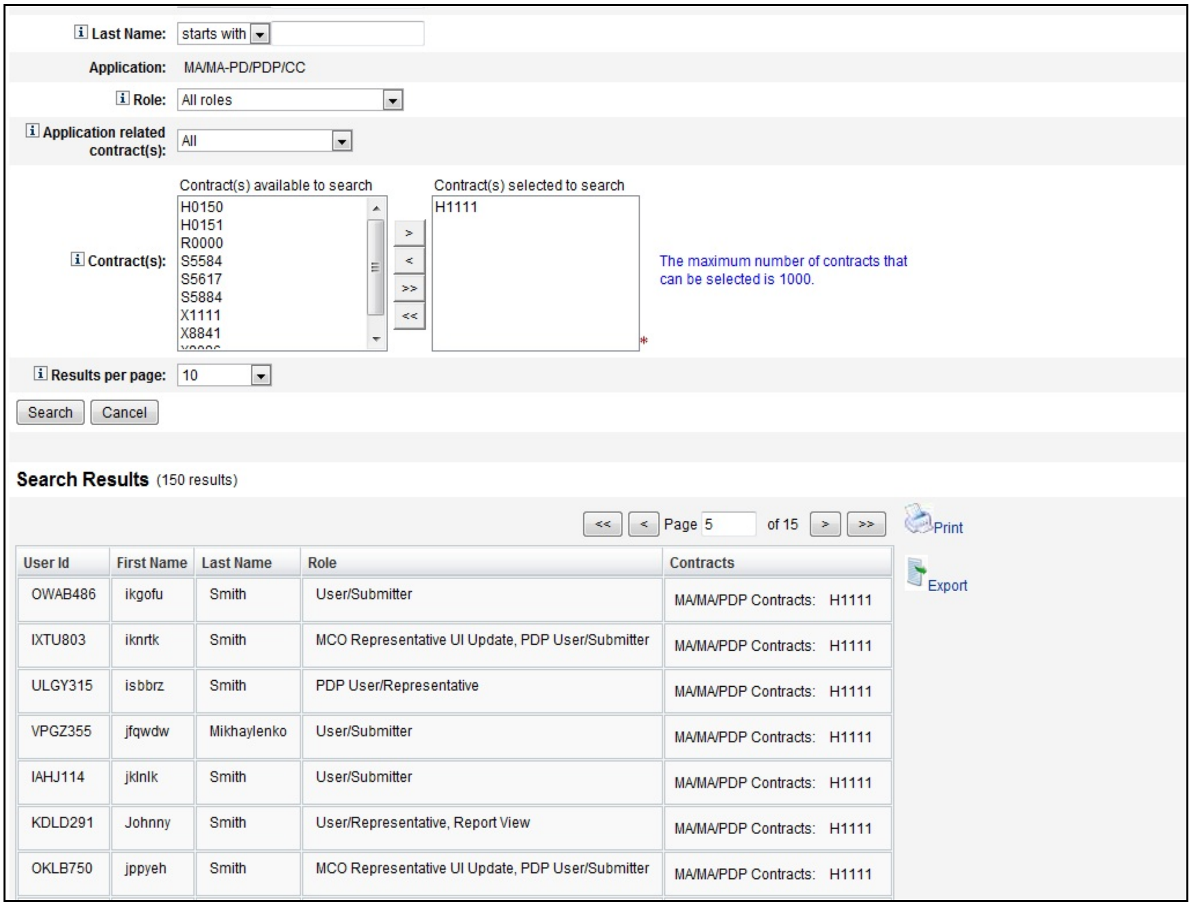
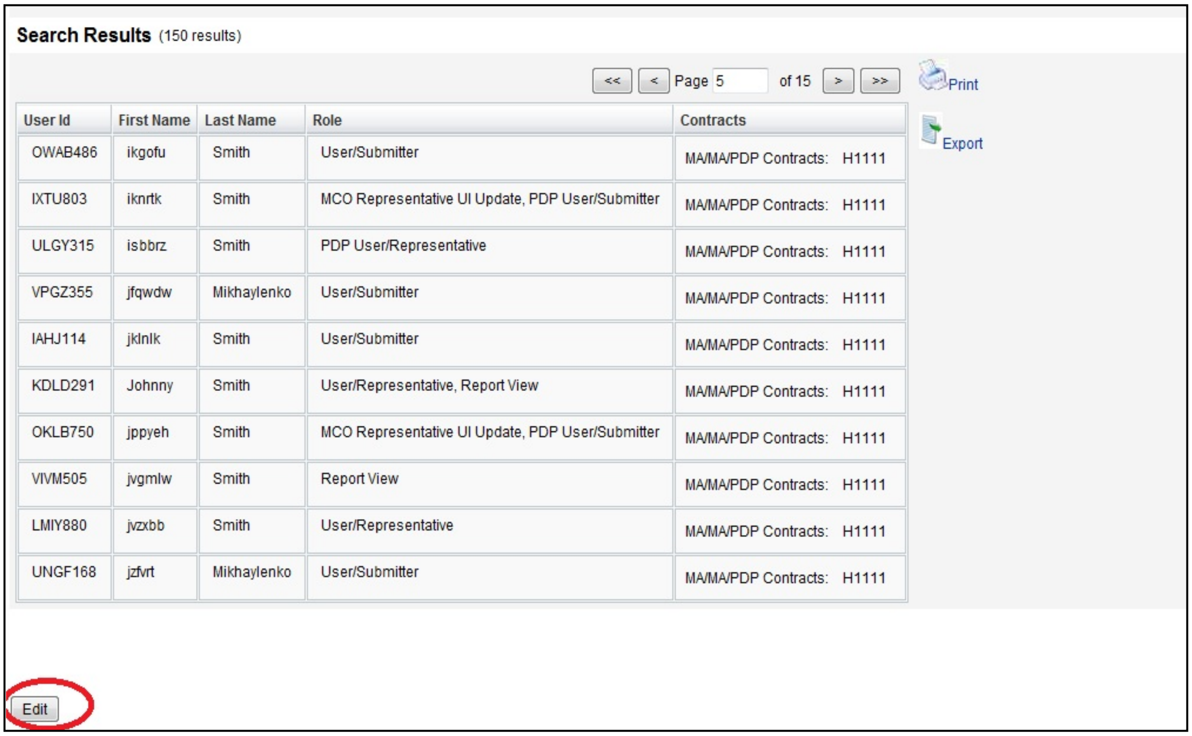


Figure 37: Manage users under my authority Screen – Search Results Area

Action: Depending on the number of results, you may need to scroll through the screens of the ***Search Results*** table until you find the appropriate user(s).

- If the Approver wants to print the search results, he should select the ***Print*** icon to the right of the ***Search Results*** table.
- If the Approver wants to export the search results into an Excel file format, he should select the ***Export*** icon to the right of the ***Search Results*** table.

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 critieria 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)

<< < Page 5 of 15 > >> Print Export

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

Edit

Figure 38: Manage users under my authority Screen Search Results Area – Edit Button Selection

Action: If you want to edit the search results select the ***Edit*** button at the bottom of the screen as illustrated in Figure 38.

The ***Search Results*** table will be converted into an editable format as illustrated in Figure 39.

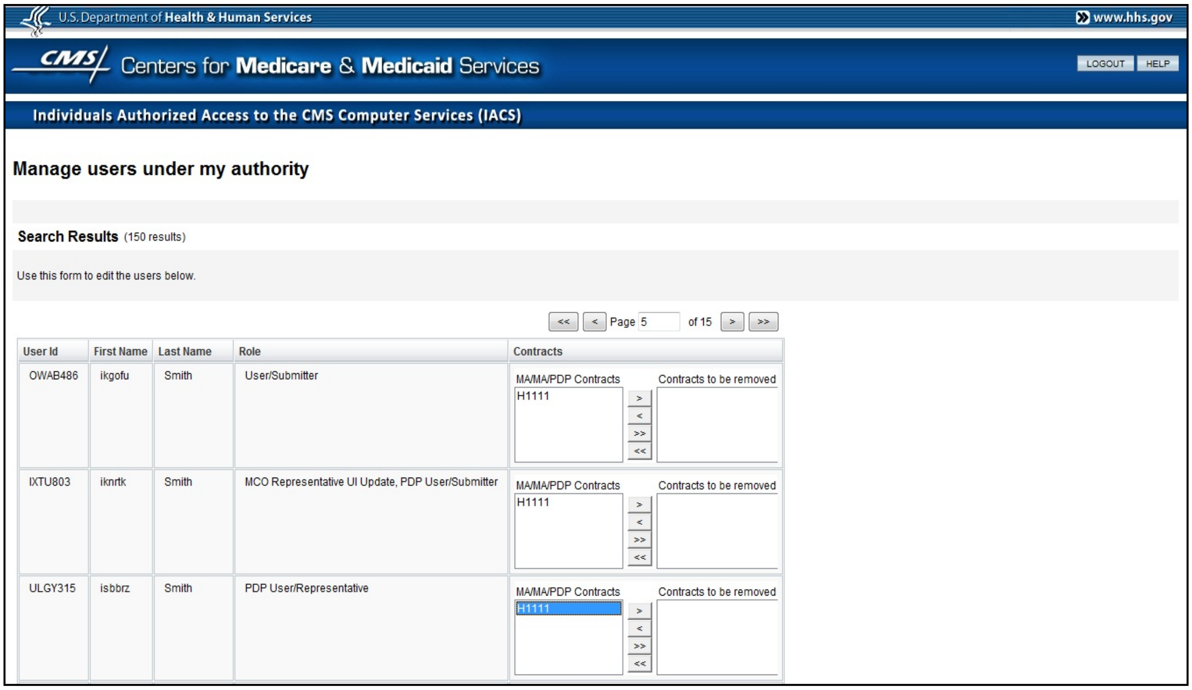


Figure 39: Manage users under my authority Screen: Search Results Area – Editable Search Results

Action: Edit the search results as desired.

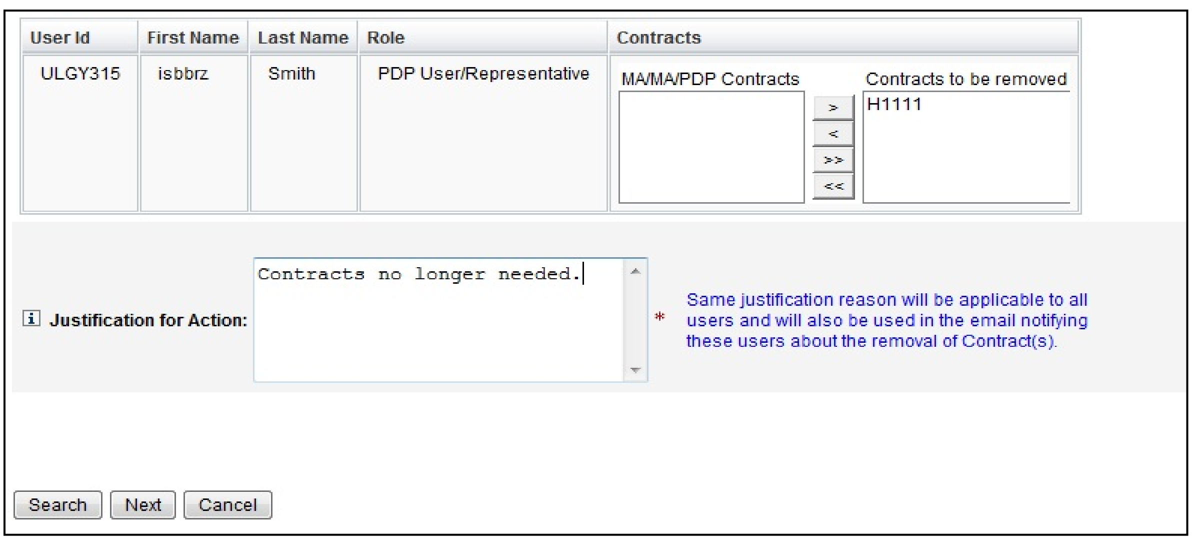


Figure 40: Manage users under my authority Screen: Search Results Area – Single Justification for Action

Action: Enter a single justification for your edits in the *Justification for Action* field, as illustrated in Figure 40.

Action: Select the ***Next*** button when you are done.

The screen will refresh and the **Review Details** screen will be displayed as illustrated in Figure 41.

If the Approver wants to discard these search results and conduct a new search, he should select the ***Search*** button, and the system will return him to the **Manage users under my authority** - ***Search Criteria*** screen, as illustrated in Figure 36.

If the Approver wants to cancel his edits, he should select the ***Cancel*** button and the system will discard his edits and return him to the **My Profile** screen as illustrated in Figure 30.

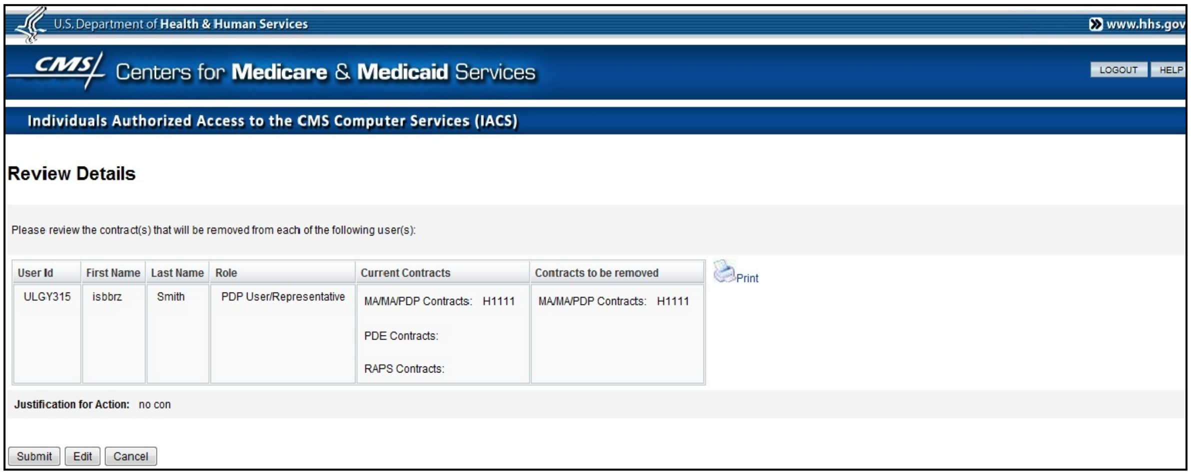


Figure 41: Review Details Screen

Action: Select the ***Submit*** button when you have reviewed your edits and are ready to finalize them. The screen will refresh and return you to the **My Profile** screen as illustrated in Figure 30.

If the Approver wants to make changes to his edits, he should select the ***Edit*** button and the system will return him to the editable ***Search Results*** section as illustrated in Figure 39.

If the Approver wants to cancel his edits, he should select the ***Cancel*** button and the system will discard his edits and return him to the **My Profile** screen as illustrated in Figure 30.

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 helpdesks 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
COB	COB Helpdesk	MAPD 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
GENTRAN	Gentran Helpdesk	IACS Administration
HETS UI	MEIC Helpdesk	MCARE Help Desk
HPG	MEIC Helpdesk	MCARE Help Desk
Internet Server	Internet Server Help Desk	IACS Administration
MA/MA-PD/PDP/CC	MAPD Helpdesk MAPD Helpdesk Admin	MAPD Help Desk
MDR	Helpdesk	MAPD Help Desk
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
VMS Client Letter	VMS Help Desk	VMS Help Desk

Table 4: Applications and Help Desk Roles using Manage users under my authority Help Desk Functions

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 42 illustrates the **My Profile** screen after a successful login by an ECRS HelpDesk user.

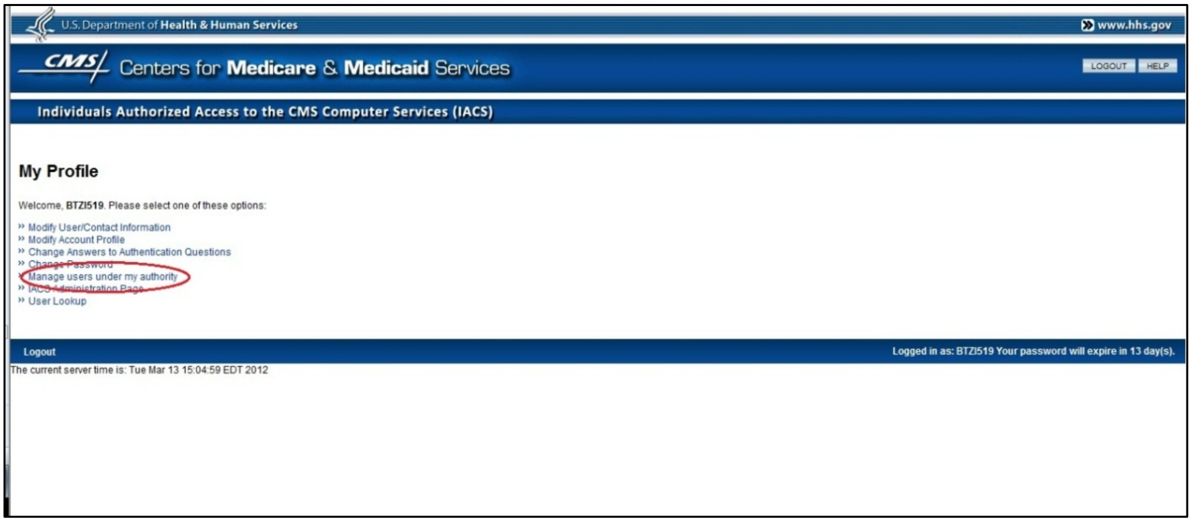


Figure 42: My Profile Screen

Action: Select the Manage users under my authority hyperlink.

The **Manage users under my authority** screen with multiple ***Search Criteria*** options will display. 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 help desk user will select one of the radio buttons to search.

The following applications will display the *Search By* radio buttons for *Archived users, User Status, and Role:*

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 43 displays the Search options for MA/MA-PD/PDP/CC helpdesks.

The following applications will display the *User Status* and *Role* selection as drop-down list:

CSP-MSCIS, CSP-HSTP, ECRS, Gentran, Internet Server, MDR, MED, Novitasphere, PS&R/STAR, and VMS Client Letter

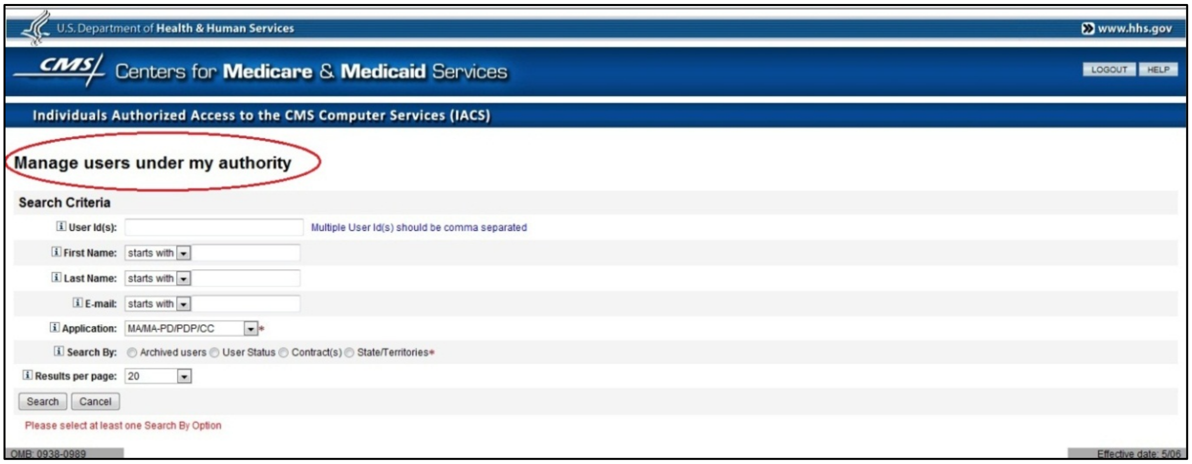


Figure 43: Manage users under my authority Screen - MA/MA-PD/PDP/CC

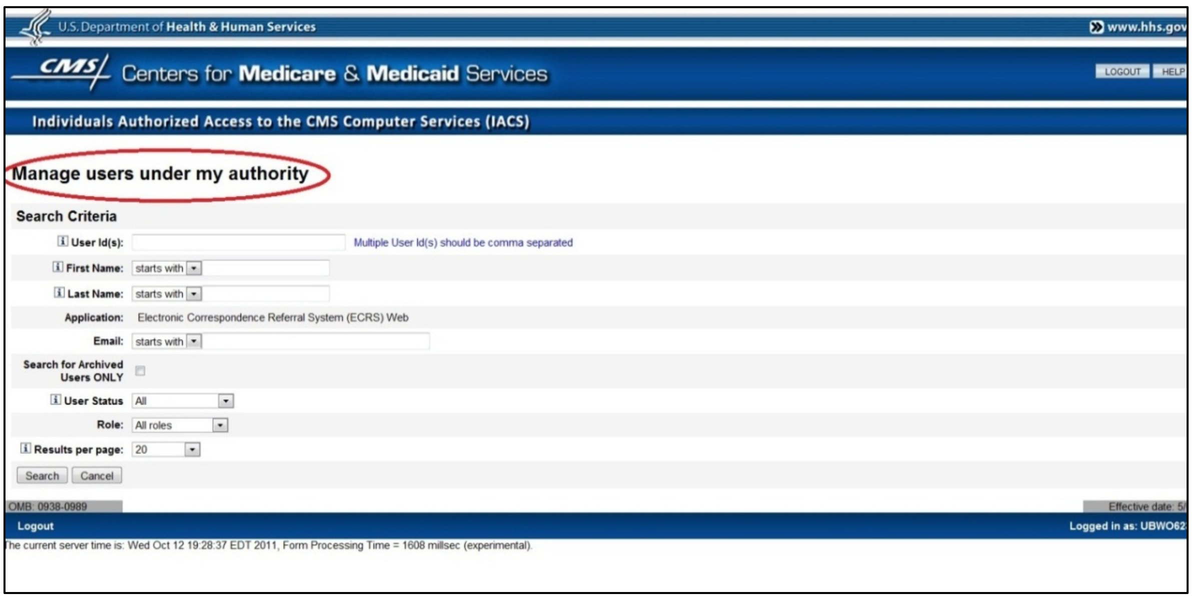


Figure 44: Manage users under my authority Screen - ECRS

13.4 Searching for User Accounts

Helpdesks can view the users of their corresponding application(s) using the Manage users under my authority function, as illustrated in Figure 43 or Figure 44. 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**.**

Note:

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

- The *Search By* field is a collection of radio buttons that when selected refreshes the screen and displays other drop-downs to select. For instance, when the MAPD Helpdesk selects the *Contract(s)* radio button the screen will refresh and the Contracts multi-select boxes will display.
- If the Helpdesk supports multiple CMS applications, then an application should be selected from the application drop-down list in order to continue with the search.
- DMEPOS search limitations:
    - The *Role* drop-down will not display when searching by *User Status*. The search results will not include the *Role* column.
    - *Role Search by* results will include archived and disassociated users. If the user selected has been archived the help desk function buttons will be disabled. The helpdesk user will not be able to identify a user that has disassociated from a role. Therefore, the helpdesk user should use the View feature to confirm that the user has a role before taking an action. The View tab will display the role as "DMEPOS User". If the user has disassociated from a DMEPOS role, the role will not display.
    - A user with a DMEPOS Authorizer1 or DMEPOS Authorizer2 role will not be found using the *Role Search By* option. The helpdesk user should use the *User Status Search By* option, along with the *User Id(s)* search criteria to locate the user.
    - *Archived users Search by* results will display “DMEPOS” as the role name for all users except DMEPOS Authorizer1 and DMEPOS Authorizer2.

Action: Select the ***Search*** button when you have finished selecting your search criteria.

The screen will refresh and the ***Search Results*** will display in a table under the ***Search Criteria*** area, as illustrated in Figure 45.

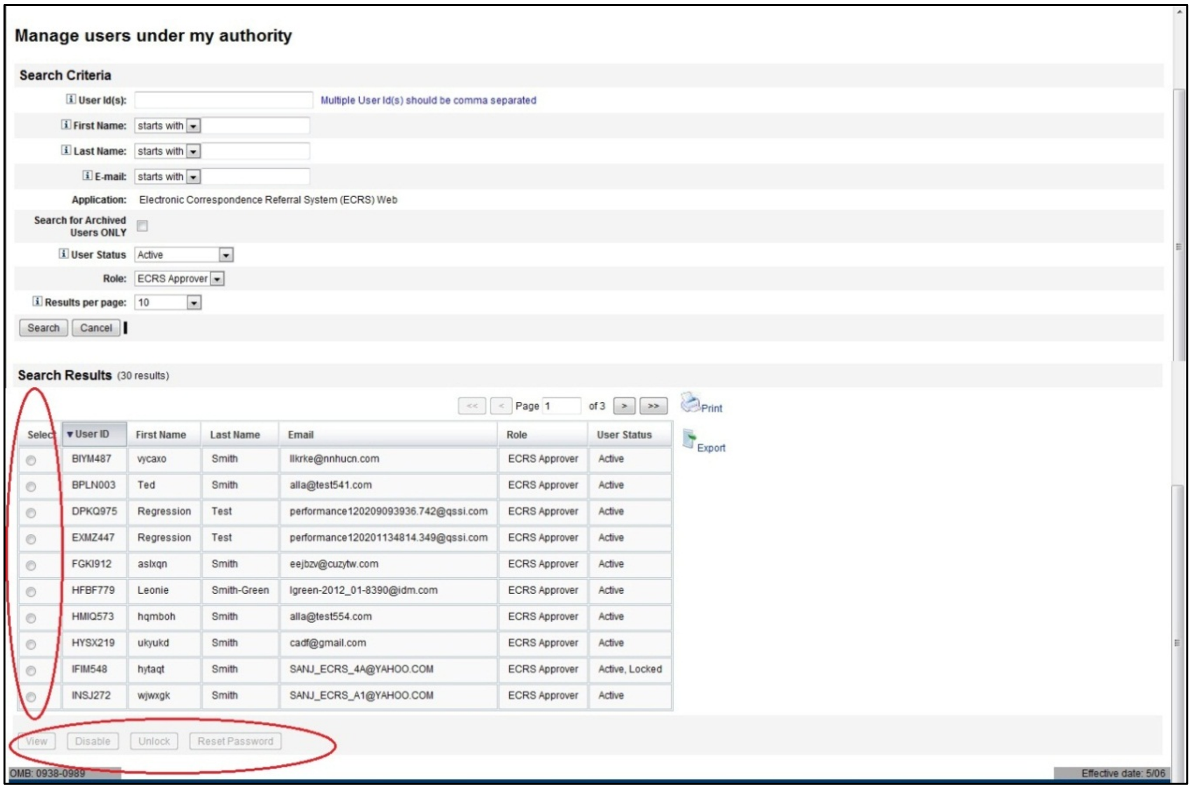


Figure 45: Manage users under my authority Screen – Search Results

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 page, as illustrated in Figure 45:

- View
- Disable
- Unlock
- Reset Password

Note:

- The help desk function buttons will be inactive until the Helpdesk selects a user record. Once the radio button is selected, the 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 46.

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

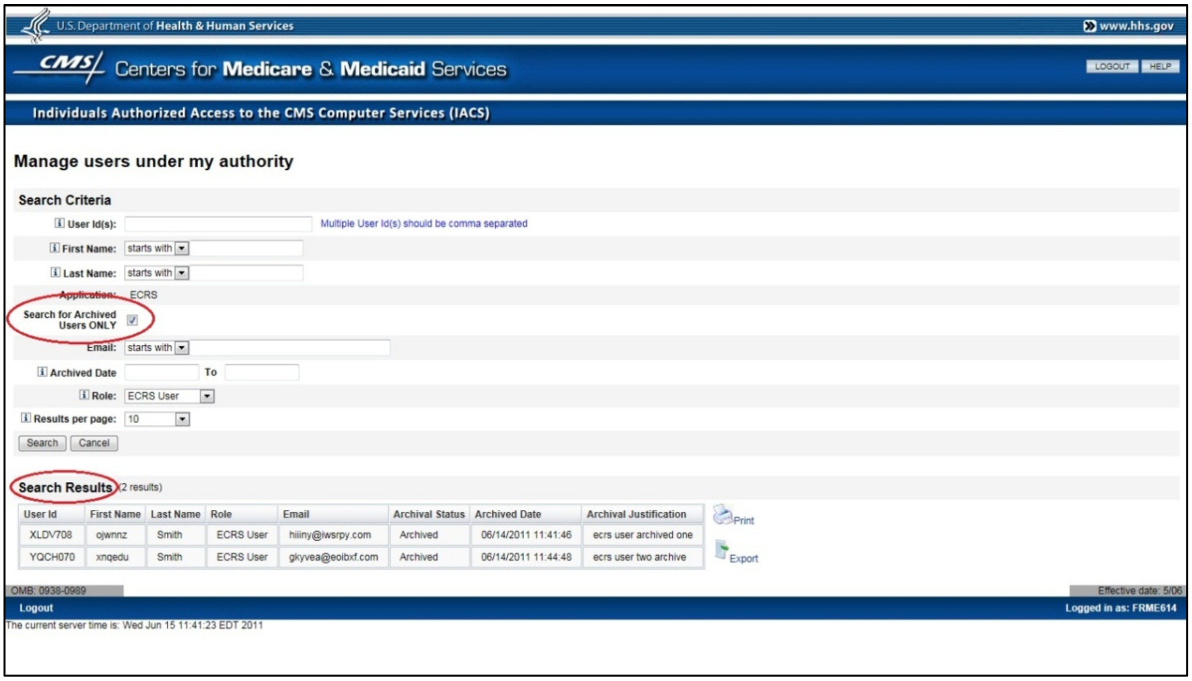


Figure 46: Manage users under my authority Screen – Search Results (Archived Users)

Action: Select the desired ***Search Criteria*** by entering the appropriate data in the search fields or selecting 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 when you have finished selecting your search criteria.

The screen will refresh and the ***Search Results*** will display in a table under the ***Search Criteria*** area, as illustrated in Figure 46.

Note:

- If the ***Search*** button is selected with no search criteria, 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

As part of the view capability, the Helpdesk can view the account information of the users under their scope of responsibility for identifying the users for any account maintenance activity.

Action: Select the radio button shown to the left of a user record, as illustrated in Figure 47.

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.

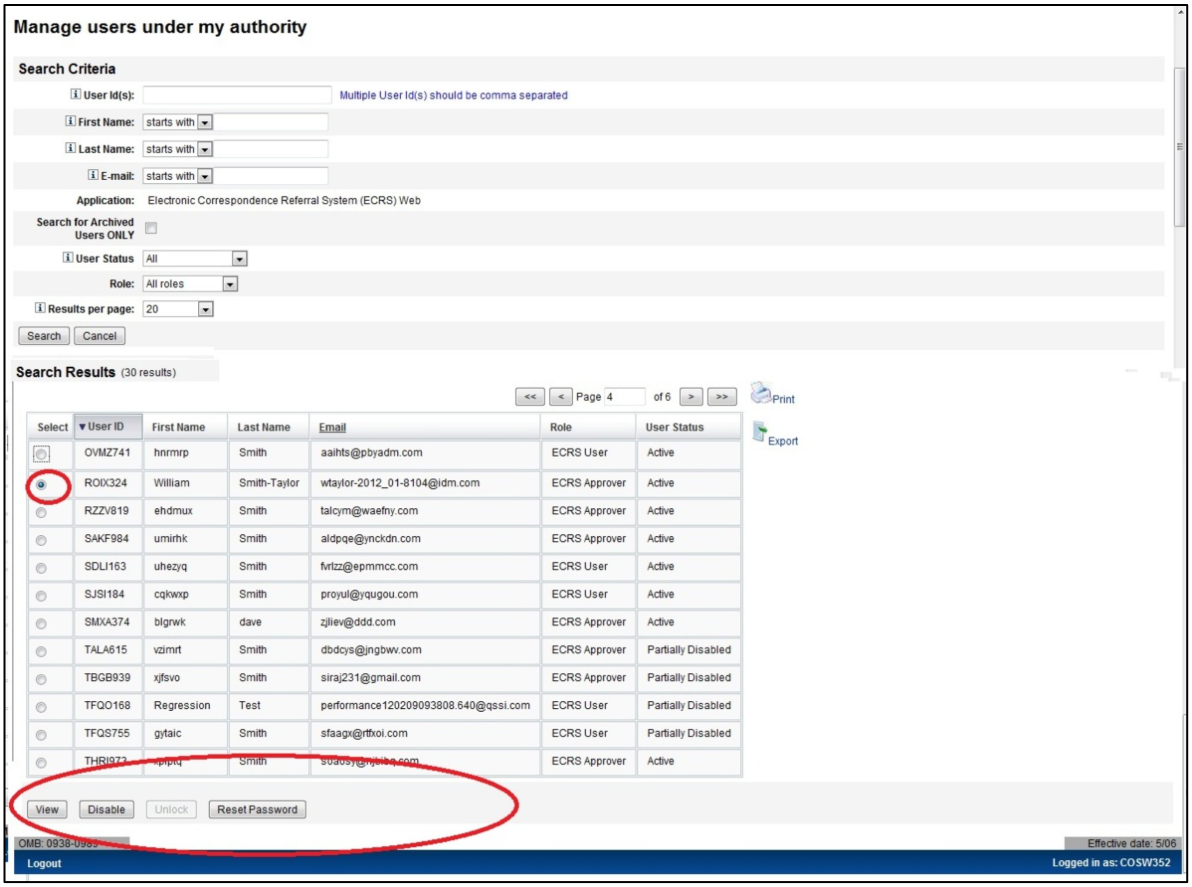


Figure 47: Manage users under my authority Screen – Help Desk Function Buttons Enabled

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

The **View Profile** screen will display which includes the navigation tabs as illustrated in Figure 48.

The tabs on the **View Profile** screen are as follows:

- 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 48.

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.

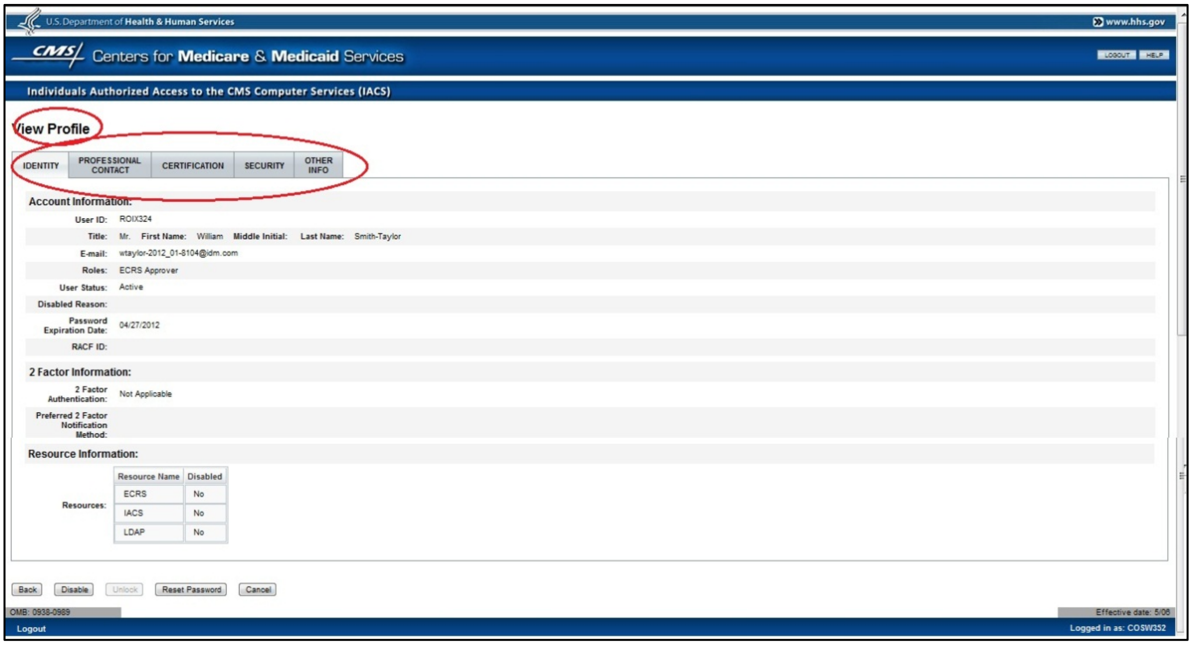


Figure 48: View Profile Screen – Identity Tab

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

The Professional Credentials and Company information will display as illustrated in Figure 49.

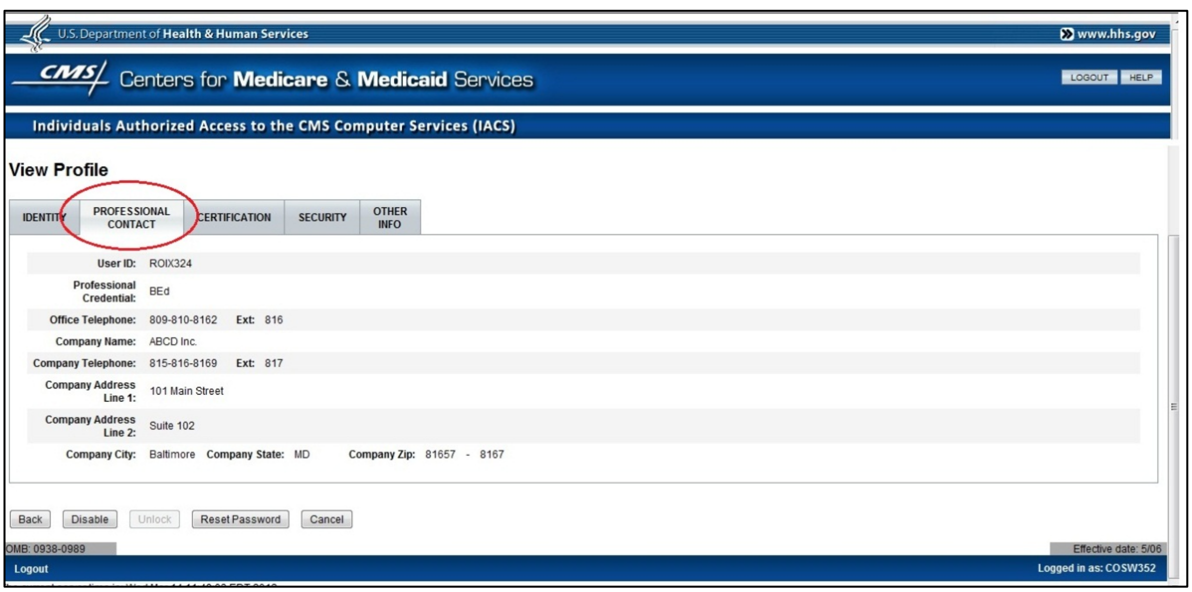


Figure 49: View Profile Screen – Professional Contact Tab

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

The user's Certification information will display as illustrated in Figure 50.

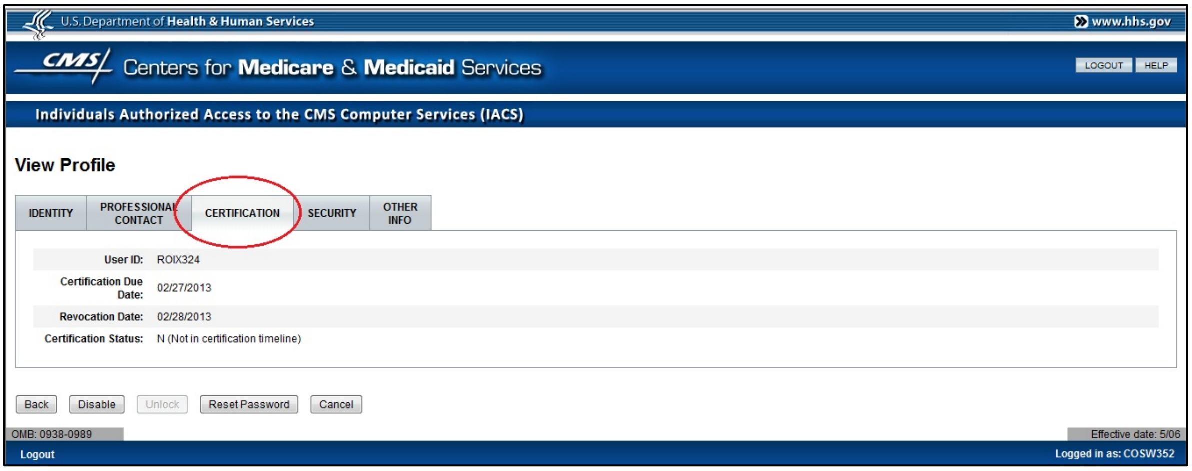


Figure 50: View Profile Screen – Certification Tab

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

The user's security information, authentication questions, and answers will display as illustrated in Figure 51.

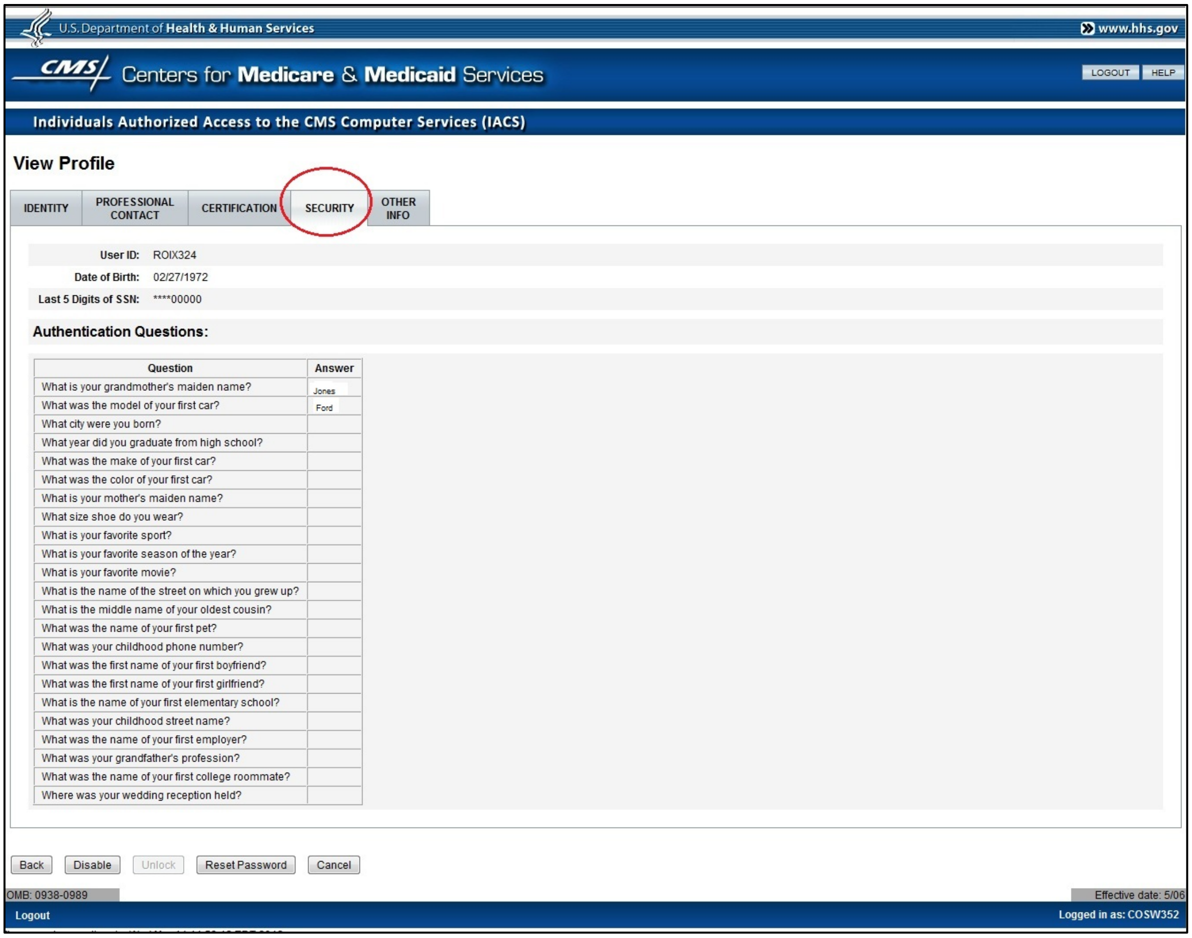


Figure 51: View Profile Screen – Security Tab

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 the application specific user information, for example, organization Information. Application specific information will not be applicable to all applications or to some roles within an application. ECRS Application does not have any application specific user information to be displayed. PS&R/STAR Helpdesk will be able to view the organization information and CMS Certification Number (CCN), or Medicare Contractor ID as appropriate.

13.4.2 Disable User Account

Helpdesks can disable user accounts within their scope of responsibility 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 52.

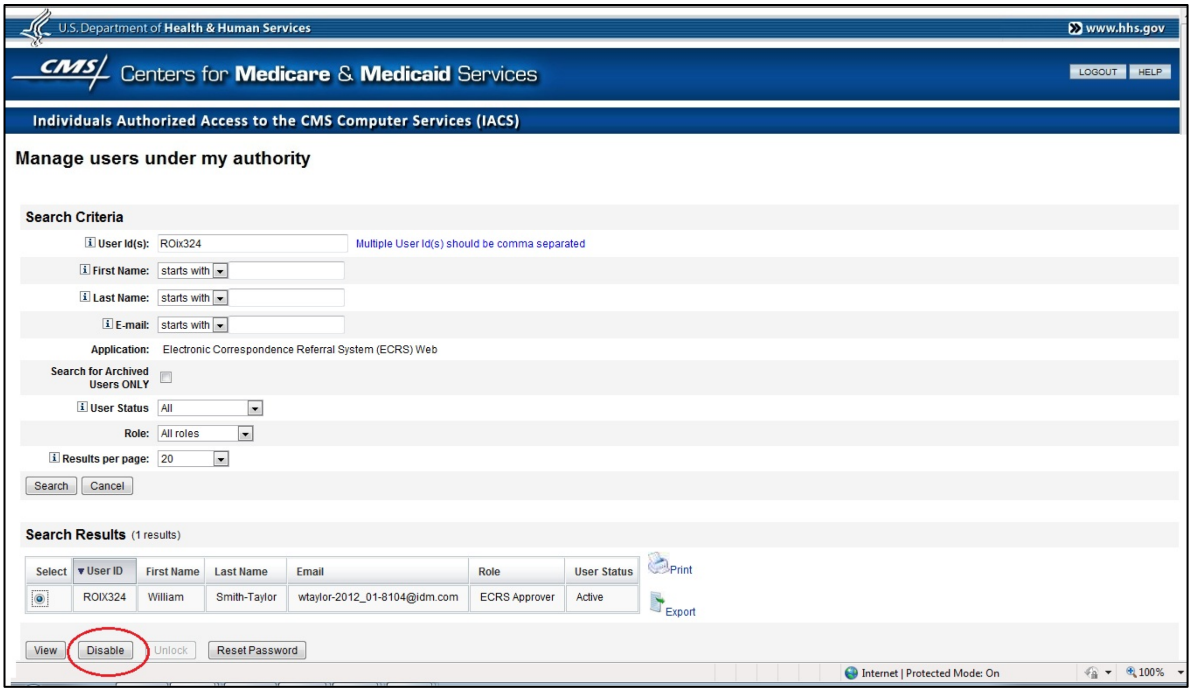


Figure 52: Manage users under my authority Screen –Disable Option

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

The **Disable Account** screen will display as illustrated in Figure 53.

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

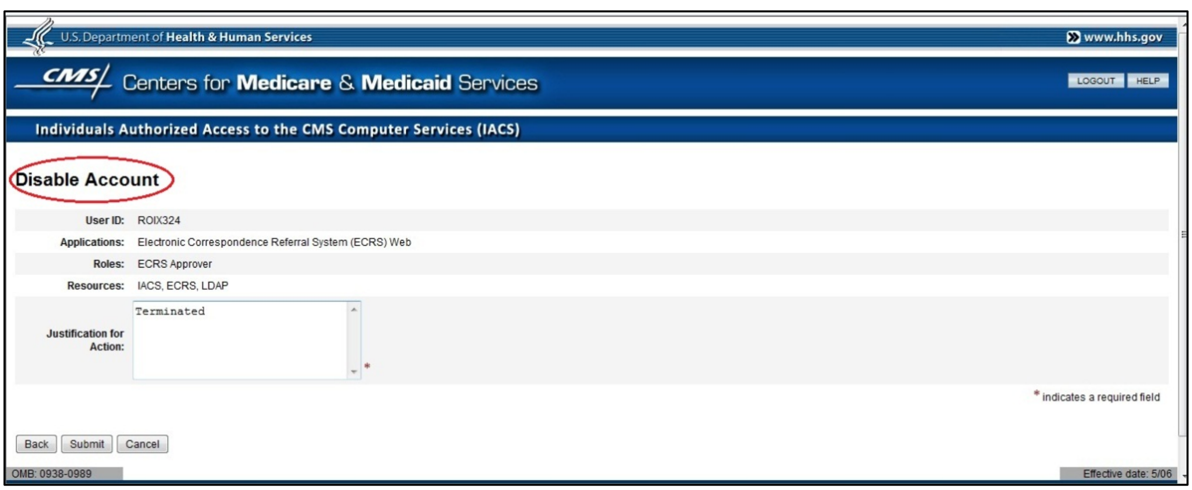


Figure 53: Disable Account Screen

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 54.

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.

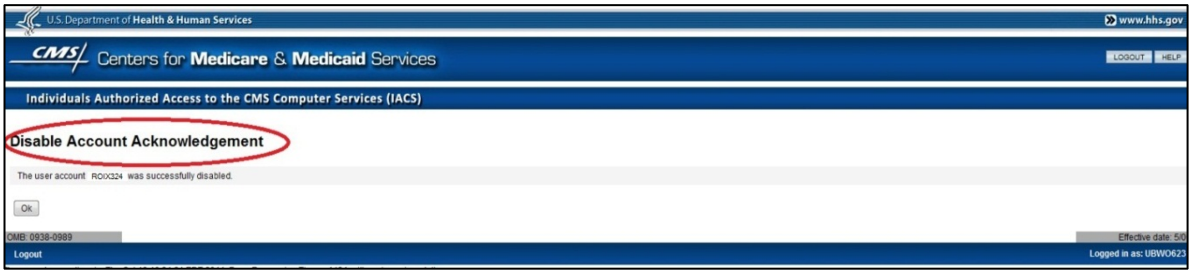


Figure 54: Disable Account Acknowledgement Screen

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.

The Helpdesk will be returned 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 55.

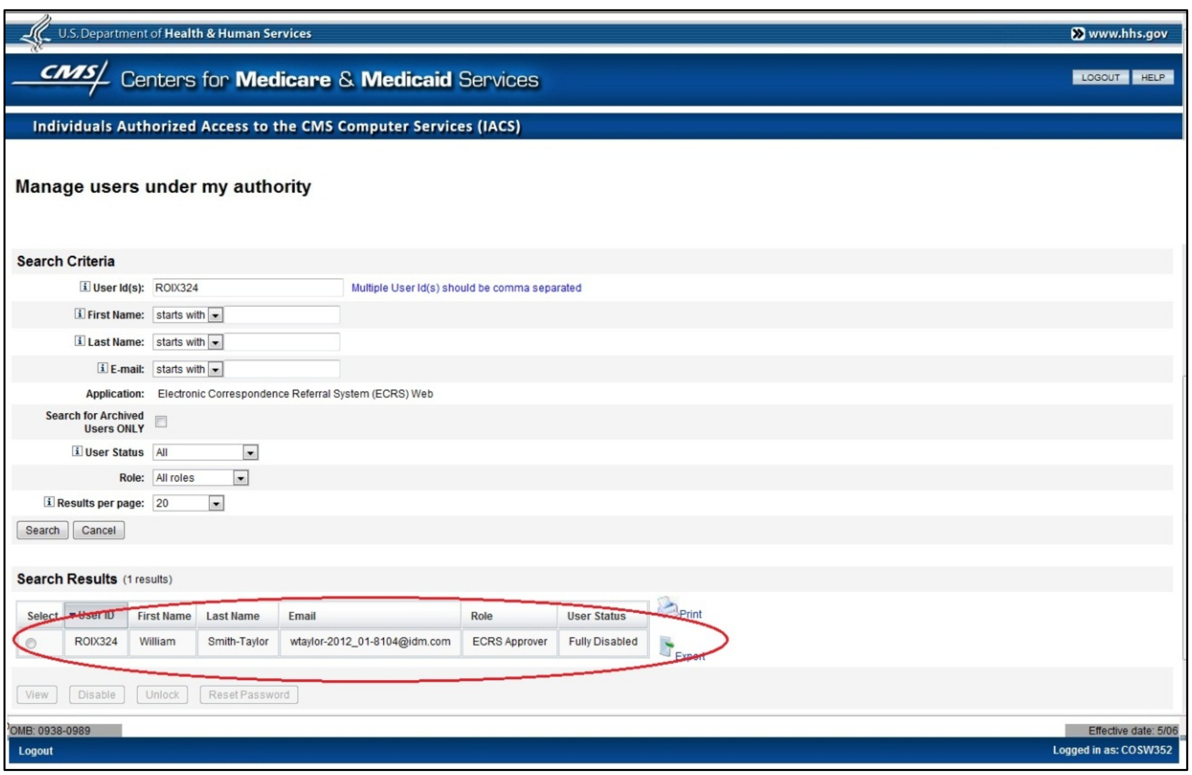


Figure 55: Manage users under my authority Screen – Shows User (Fully Disabled)

13.4.3 Reset User Password

Helpdesks can reset the password for user accounts within their scope of responsibility 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 a one-time password. IACS requires the user to change the temporary password at the time of login.

Figure 56: Manage users under my authority Screen – Reset Password Option

Action: From the **Manage users under my authority** screen, select the radio button to the left of the user account to reset the password, as illustrated in Figure 56.

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

The **Reset Account Password** screen will display as illustrated in Figure 57.

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

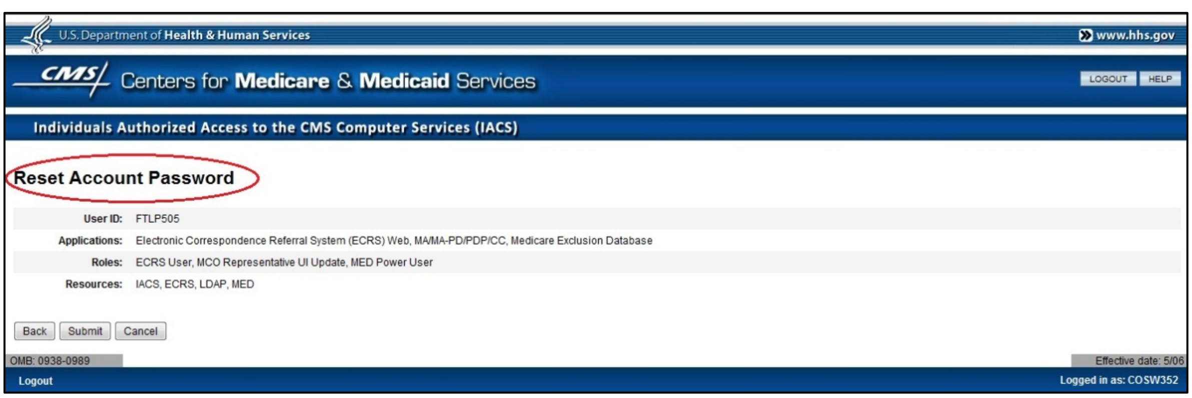


Figure 57: Reset User Password Screen

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 58 .

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.

Figure 58: 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 a random one-time password once the password reset process completes.

The Helpdesk will be returned to the search results on the **Manage users under my authority** screen, as illustrated in Figure 56.

13.4.4 Unlock User Account

Helpdesks can unlock a user's account within their scope of responsibility 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 59.

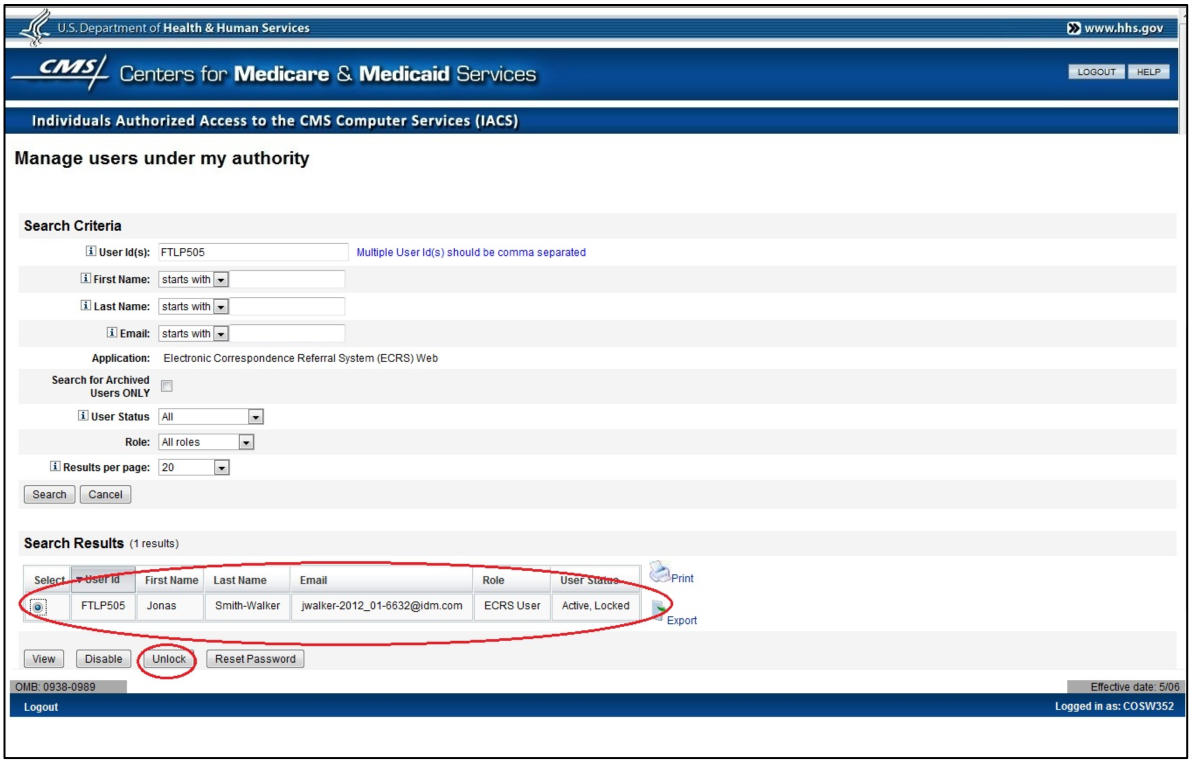


Figure 59: Manage users under my authority Screen – Unlock Option

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 60.

> **Note:** The ***Unlock*** button will not be active when the user status is not 'Locked' or 'Fully Disabled'.

Figure 60: 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.

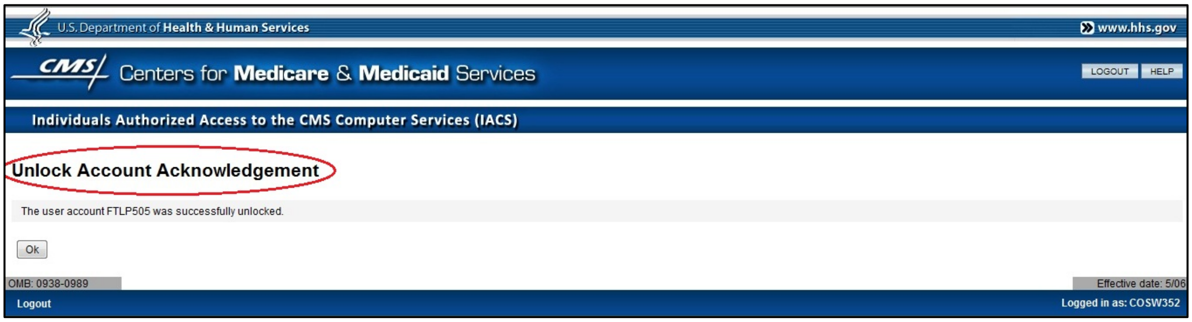


Figure 61: Unlock Account Acknowledgement Screen

The **Unlock Account Acknowledgement** screen will display a message that the account was unlocked successfully, as illustrated in Figure 61.

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

The Helpdesk will be returned 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 62.

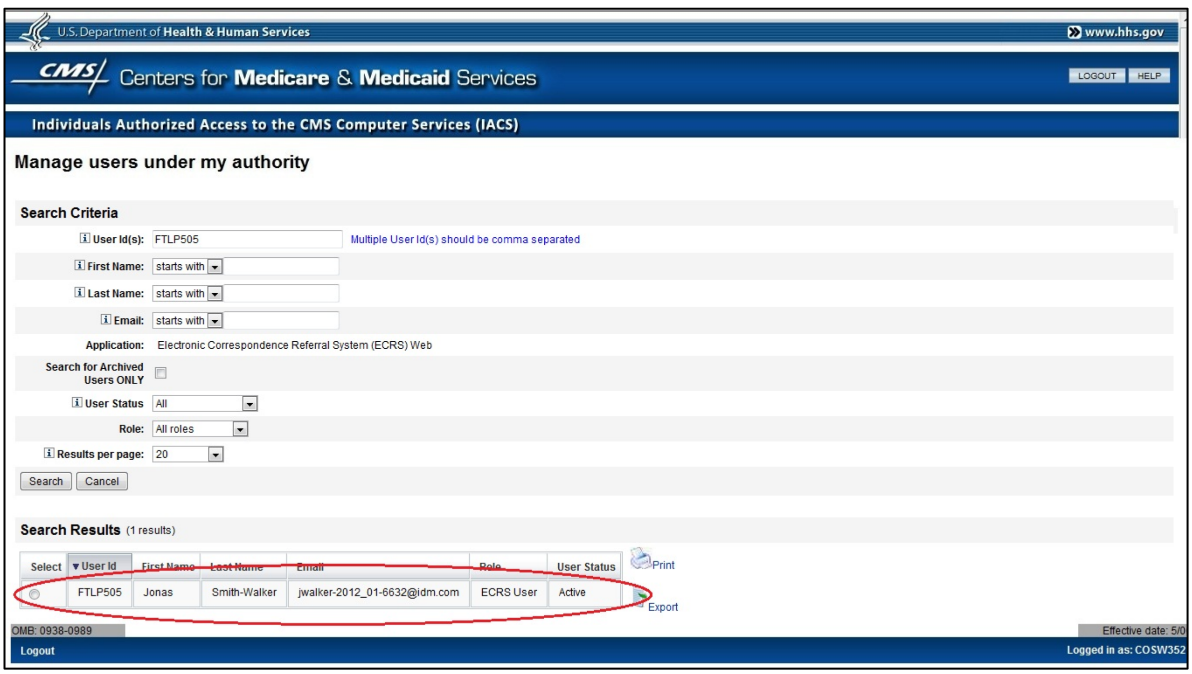


Figure 62: Manage users under my authority Screen – Shows User (Active)

14.0 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 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 63.

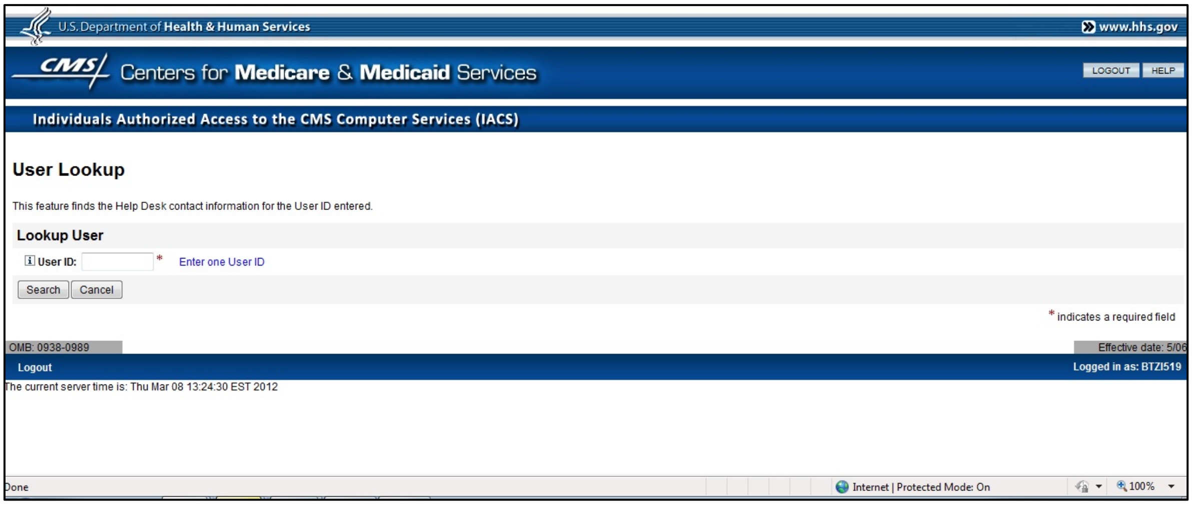


Figure 63: User Lookup Screen

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 64.

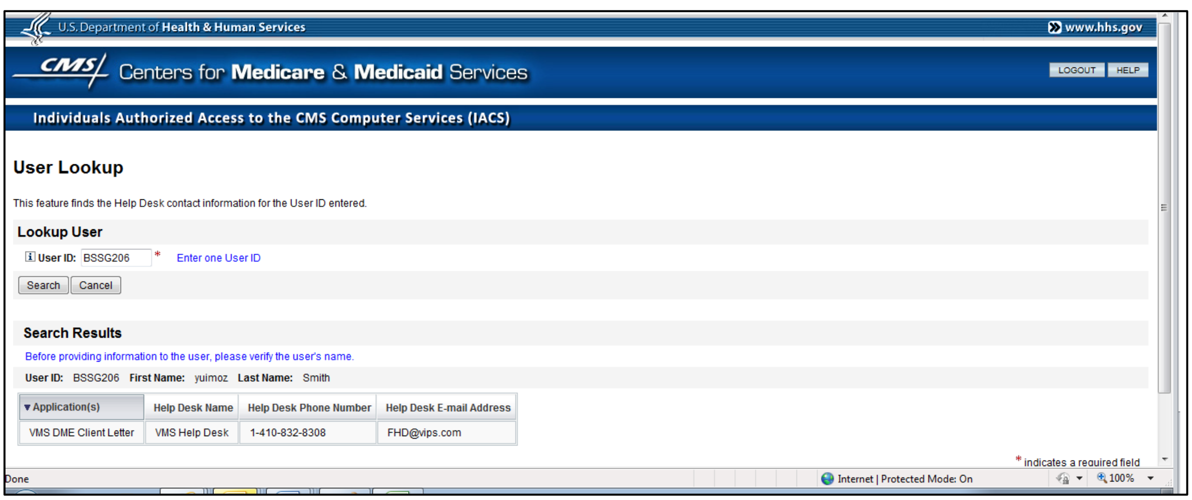


Figure 64: User Lookup Search Results

Note:

- 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 with no 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 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 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 the next time he logs in. If the user has not changed the password in over 180 days, the account will be disabled. Section 8.4 describes the procedures to re-active the account.

15.2 180 Day Partial Disable

In compliance with CMS security policy, IACS automatically disables any user that has not logged into IACS for 180 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 8.4 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 archived as described in the sections below.

15.3.1 Certification Failure

All IACS users are required to certify annually 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 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.

Note:

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

15.3.2 MA/MA-PD/PDP/CC Users without Contracts for 60 days

Users with the following MA/MA-PD/PDP/CC Application roles will have their IACS user account archived if they have no contracts associated with their profile for 60 days or longer and they do not have any other IACS roles:

- MA Submitter
- PDP Submitter
- MA Representative
- PDP Representative
- EPOC
- POSFE Contractor
- 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.

16.0 Troubleshooting & Support

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 section illustrates one type of error message and instructions to the user. The examples are of the error messages and instructions that will appear for validation failures.

16.2 Validation Failure

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 65.

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.

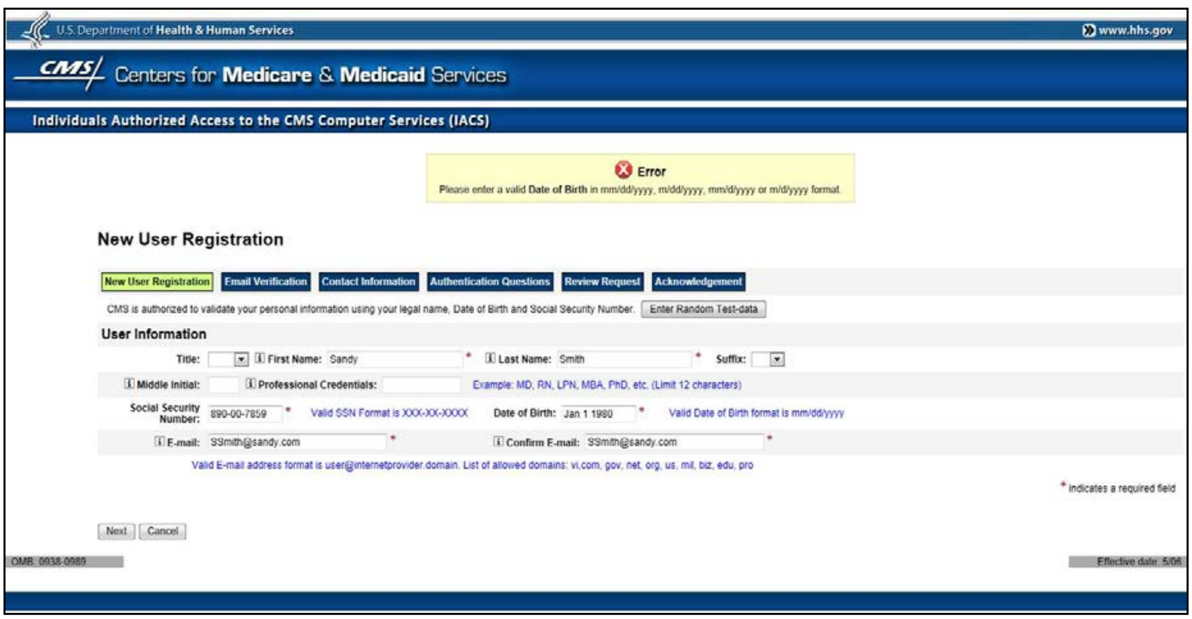


Figure 65: New User Registration Screen: Validation Failure Message

Action: Review the user information you have entered for correctness.

Action: Make any needed changes to your user information.

Action: Select the ***Next*** button when you are done.

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 **E-mail Address Verification** 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 listed below.

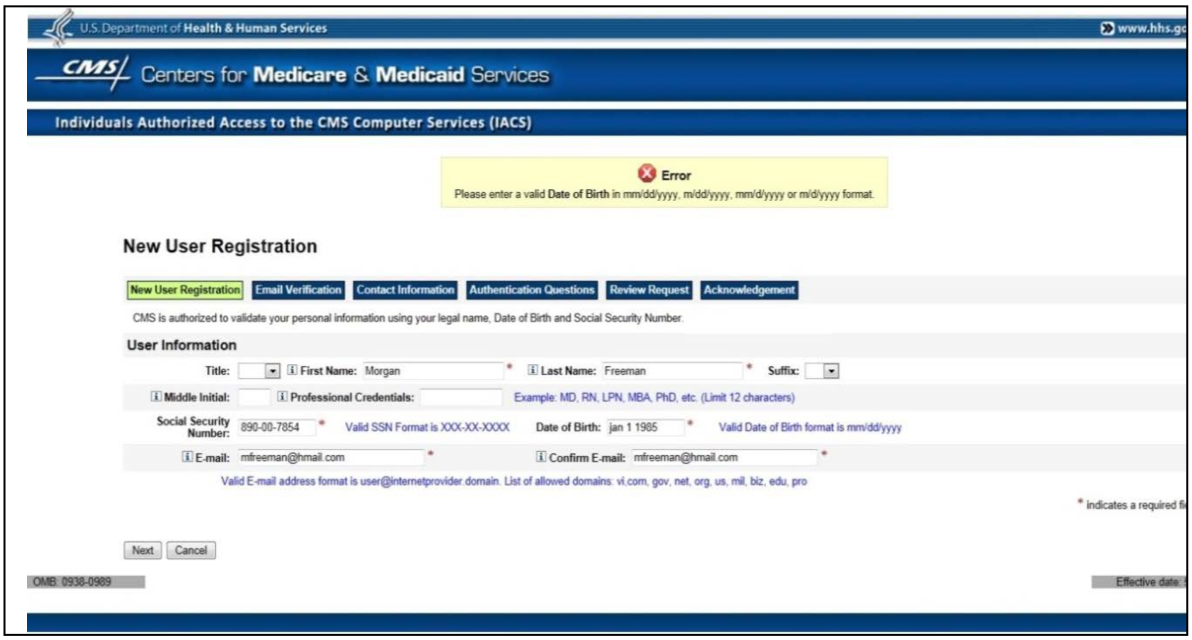


Figure 66: Warning Message

The message shown in Figure 66 notifies the user that the *Date of Birth* (DOB) field failed and the expected input is shown.

Figure 67: Information Message

The message shown in Figure 67 notifies the user that the option selected cannot currently be used.

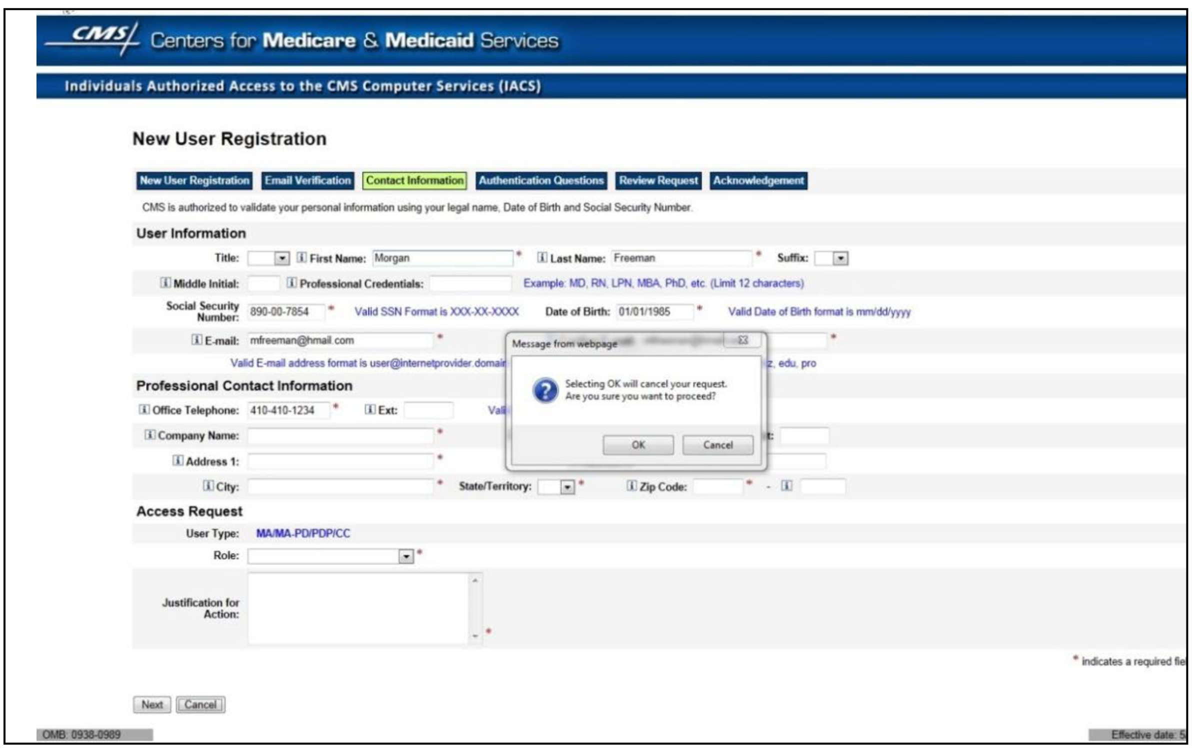


Figure 68: Caution Message

The message shown in Figure 68 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.

16.3 Frequently Asked Questions

1. *I registered and was approved as a PQRS Submitter for the PQRS/eRx application without associating with an organization. How can I add the organization to my profile?*

   To associate with 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 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, should open a Service Request directed to the IACS Administrators to modify the Submitter ID. Refer to Section 16.4 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 directed to the IACS Administrator to modify your personal information. Refer to Section 16.4 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 directed 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 get certified?*

   You are seeing a warning message because, you have one or more role(s) in PQRS/eRx or PS&R/STAR Applications in your user profile and there are no approvers defined in the system for one or more of those role(s). Therefore, IACS will not have a way to route your certification request for approval. Thus, your request for certification will remain unprocessed. Please contact your Help Desk for further instructions. Refer to Section 16.4 for Help Desk contact details.

   Note: In the case of a user having multiple roles in PQRS/eRx or PS&R/STAR Applications and only one of the roles not having an Approver; the certification request will remain unprocessed for all the roles.

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 because there are no contracts associated with your role. To retain your IACS account you will need to request a contract and be approved for that 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 role(s) in IACS will be archived by the system by the 61st day. Since you are a MA Submitter, you could have been archived for not having contracts associated with your profile and no other IACS application roles for 60 days. Once archived, you will have to go through New User Registration to establish a new IACS account. Refer to Section 15.3.2 for more details.

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 role(s) 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 for not having contracts associated with your role for 60 days. You will have to request the MA Submitter role again using the Modify Account Profile function. Refer to Section 15.3.2 for more details.

15. *As a PS&R Security Official, how do I modify the CCNs associated with my organization?*

    PS&R Security Official can modify CMS Certification Number(s) (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.
    2. From the *My Current Access Profile* table select the View/Edit Organization details option from the *Action* drop-down.
    3. The **Organization Information** with the *CMS Certification Number* field will display.

4. Modify the *CMS Certification Number* field entry as desired. Input a 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 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 help desk user will receive a warning notice that the user will be disabled.

The Manage users under my authority help desk function warns the 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 180 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-active 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. The 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 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 his temporary password.

    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 role(s) and contract(s)

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 notice the Edit feature of the Manage users function does not display the same users as in the search results. Why is this?*

As a Security Official for the PS&R/STAR or PQRS/eRx applications, you have the capability to disassociate users in your organization. The SO role, also allows you to view the users of other organizations. When you select the search criteria as, *All Organizations* and then select the ***Edit*** button, the page 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. A*fter 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 gets 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.

16.4 Support

This section provides the Help Desk contact information for IACS supported applications.

Note: For a more recent list of Help Desk contact information, refer to the Help Resources area of the **Account Management** screen on the CMS website.

Application	Supporting Help Desk	Phone Number	E-mail Address
COB	MAPD Help Desk	1-800-927-8069	mapdhelp@cms.hhs.gov
CSR	MAPD Help Desk	1-800-927-8069	mapdhelp@cms.hhs.gov
DMEPOS Bidding System (DBidS)	CBIC Help Desk	1-877-577-5331	CBIC.admin@palmettogba.com
ECRS Web	EDI Help Desk	1-646-458-6740	ecrshelp@hmedicare.com
GENTRAN	IACS Administrator	N/A	iacs_admin@cms.hhs.gov
Health System Tracking Project (HSTP)	HSTP Help Desk	1-410-786-6693	HSTP_Application_Support@cms.hhs.gov
HETS UI	MCARE Help Desk	1-866-440-3805, Fax: 1-615-238-0822	mcare@cms.hhs.gov
HPG	MCARE Help Desk	1-866-440-3805, Fax: 1-615-238-0822	mcare@cms.hhs.gov

Application	Supporting Help Desk	Phone Number	E-mail Address
Internet Server	IACS Administrator	N/A	iacs_admin@cms.hhs.gov
MCSIS	MCSIS Help Desk	1-410-786-4727	MCSIS_Application_Support@cms.hhs.gov
MDR State Exchange	MAPD Help Desk	1-800-927-8069	mapdhelp@cms.hhs.gov
MED	External User Services (EUS) Help Desk	1-866-484-8049 TTY/TDD: 1-866-523-4759	EUSSupport@cgi.com
Medicare Advantage/Prescription Drug Plans	MAPD Help Desk	1-800-927-8069	mapdhelp@cms.hhs.gov
Novitasphere	Novitasphere Help Desk	1-877-235-8073	websiteEDI@highmark.com
PQRS/eRx	QualityNet Help Desk	1-866-288-8912	qnetsupport@sdps.org
PS&R/STAR	External User Services (EUS) Help Desk	1-866-484-8049 TTY/TDD: 1-866-523-4759	EUSSupport@cgi.com
VMS Client Letter	VMS Help Desk	1-410-832-8308	FHD@vips.com

17.0 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.
DMEPOS	Durable Medical Equipment, Prosthetics, Orthotics & Supplies

Term	Definition
ECRS	Electronic Correspondence Referral System - 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.
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, or 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.
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 contact 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.

Term	Definition
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 180 days. A 'Partially Disabled' user cannot log into 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.

18.0 Acronyms

This section defines acronyms used or referenced in this document.

Acronym	Definition
AO	Authorized Official
BAO	Backup Authorized Official

Acronym	Definition
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
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
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)
EST	Eastern Standard Time
EUS	External User Services
FI/Carrier/MAC	Fiscal Intermediary/Carrier/Medicare Administration Contract
GUI	Graphical User Interface
HETS UI	HIPAA Eligibility Transaction System User Interface
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act

Acronym	Definition
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
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 Contract
MA-PD	Medicare Advantage – Prescription Drug
MCARE	Medicare Customer Assistance Regarding Eligibility
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
NIST	National Institute of Standards and Technology
NPI	National Provider Identifier
PDE	Prescription Drug Event
PDP	Prescription Drug Plan
PII	Personally Identifiable Information
PTAN	Provider Transaction Access Number
POSFE	Point-of-Sale Facilitated Enrollment
PQRI	Physician Quality Reporting Initiative

Acronym	Definition
PQRS/eRX	Physician Quality Reporting System and E-Prescribing Incentive Programs
PS&R/STAR	Provider Statistical and Reimbursement / System Tracking for Audit and Reimbursement
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
TIN	Taxpayer Identification Number
VMS	ViPS Medicare System

Appendices

Appendix A - 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 had 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 had 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
Registry End User	12
EHR Vendor	12
PQRI Admin	12
Individual Practitioner	60
PQRI Maintainer	12
PQRS Submitter	12
PQRS Representative	12

Index

A

Annual Certification Process
- Certify Annually ... 58, 59
- Submitting Certification Request ... 58, 59

C

CMS Application
- CMS Applications ... 3

CMS Application Registration
- COB ... 32
- CSR ... 32
- DMEPOS ... 32
- Gentran ... 32
- HETS UI ... 33
- HPG ... 33
- Internet Server ... 33
- MA/MA-PD/PDP/CC ... 33
- MED ... 35
- Novitasphere ... 35
- PQRS/eRx ... 36
- PS&R/STAR ... 38
- VMS Client Letter ... 39

F

Frequently Asked Questions
- Organization ... 99

I

IACS Account
- Definition ... 3

IACS Account Life Cycle
- 180 Partial Disable ... 94
- Archiving Accounts ... 94
- Certification Failure ... 94
- Password Expiration ... 94

L

Log in to IACS
- IACS User ID ... 40
- Terms and Conditions ... 40
- User Profile ... 40

M

Modify Account
- Add Applications ... 48, 50
- Contracts ... 51
- Disassociate from a Role ... 52
- Modify Report Access ... 12, 27, 34, 35, 49, 53, 54, 55, 56, 57

Modify User/Contact Information
- Change E-mail ... 42, 46, 99

O

Other Application Modifications
- HPG ... 56
- MA/MA-PD/PDP/CC ... 56
- PQRS/eRx ... 56
- PS&R/STAR ... 56

R

Roles
- COB ... 4
- CSP - HSTP ... 5
- CSP - MCSIS ... 5
- DMEPOS ... 6
- ECRS ... 8
- Gentran Gentran ... 8
- HETS UI ... 8
- HPG ... 9
- Internet Server ... 9
- MA/MA-PD/PDP/CC ... 10
- MDR ... 13
- Medicare Exclusion Database ... 13
- Novitasphere ... 14
- PQRS/eRx ... 15
- PS&R/STAR ... 18
- VMS Client Letter ... 19

T

Troubleshooting & Support
- Validation Failure ... 96