Individuals Authorized Access to the CMS Computer Services

(IACS)

User Guide for CMS Applications

Document Version 4.0

July 2011

Document No.: IACS.UG.4.0
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
07/30/2010	1.0	Initial Release	QSSI
11/08/2010	2.0	Revisions for IACS November 2010 Release(2010.03)	QSSI
04/01/2011	3.0	Revisions for IACS April 2011 Release (2011.01)	QSSI
06/07/2011	4.0	Revisions for IACS July 2011 Release (2011.02)	QSSI

CONTENTS

FIGURES

TABLES

1.0 Introduction

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

- Identify themselves
- 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).

This **IACS User Guide for CMS Applications** establishes the procedures for registering and provisioning end-users, helpdesks, approvers, and authorizers 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)**
- **Gentran Application**
- **HIPAA Eligibility Transaction System User Interface (HETS UI)**
- **HIPAA Eligibility Transaction System Provider Graphical User Interface (HPG)**
- **Medicare Advantage/Medicare Advantage-Prescription Drug/Prescription Drug Plan/Cost Contracts (MA/MA-PD/PDP/CC)**
- **Medicare Drug Rebate (MDR)**
- **Medicare Exclusion Database (MED)**
- **Physician Quality Reporting System and E-Prescribing Incentive Programs (PQRS/eRx)**
- **Provider Statistical and Reimbursement / System Tracking for Audit and Reimbursement (PS&R/STAR)**

2.0 Referenced Documents

This **IACS User Guide for CMS Applications** and additional **IACS User Guides** include information regarding new and/or modified IACS screens and functionalities.

The following IACS help documentation has been added to the CMS IACS website (http://www.cms.gov/MAPDHelpDesk/07_IACS.asp#TopOfPage) to provide additional information and instructions for IACS users:

- **IACS User Guide for CMS Applications** – provides registration and account maintenance information for CMS Applications Users.
- **IACS User Guide for Approvers** – provides account maintenance information for IACS Approvers.
- **IACS User Guide for the Helpdesk** – provides account maintenance information for the HelpDesk staff supporting CMS applications integrated with IACS.

3.0 Overview

The sensitivity of CMS data and improved ability to access data combine to create substantial risk to CMS and Beneficiaries. Legislation, 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 the CMS uses to:

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

The **IACS User Guide for CMS Applications** provides procedural information and representative screens that are common to most users and includes:

- Registering as a New User for one of CMS's Applications
- Modifying user registration information after the initial registration has been approved
- Modifying IACS account profile information such as adding or removing Contracts, Call Centers, Organizations, and/or applications
- Certifying for IACS roles and resources annually

Procedural information that is particular to specific applications is noted for reference. IACS procedures are consistently user-friendly, and on-screen help and error messages will help guide users when completing procedures not illustrated in this User Guide.

3.1 Warnings and Reminder

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. This information is presented in the opening screen of the CMS Applications Portal as illustrated in Figure 1.

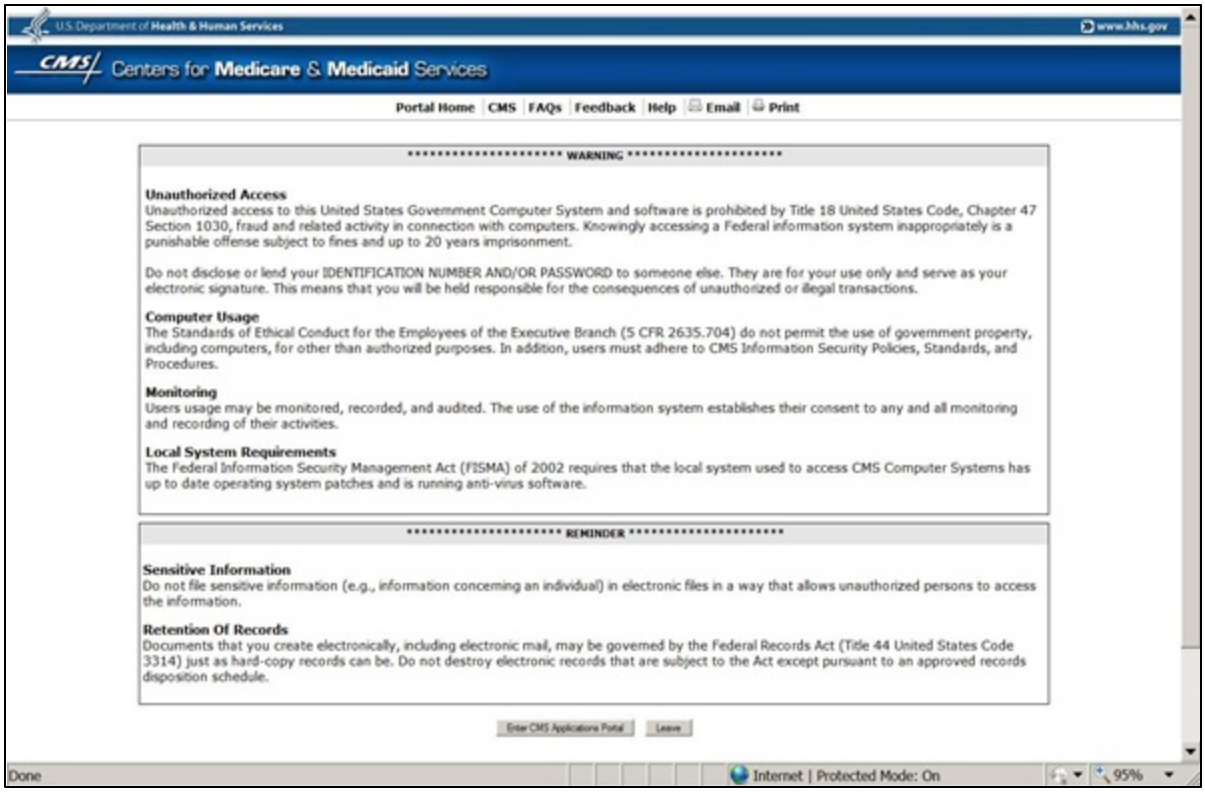

Figure 1: CMS Applications Portal WARNING/REMINDER Screen

All applicants to CMS Applications should read the important information on this screen and indicate their agreement by selecting the ***Enter CMS Applications Portal*** button.

If the user does not want to proceed any further, the user should indicate this by selecting the ***Leave*** button.

3.2 Terms and Conditions

In addition to the government warnings, there are specific CMS Computer Systems Security Requirements Terms and Conditions that potential IACS users need to know. During their registration process, the CMS **Terms and Conditions** screen will display as illustrated in Figure 2.

This screen contains the Privacy Act Statement and the Rules of Behavior which present the terms and conditions for accessing CMS computer systems.

IACS applicants must accept them to be authorized to access CMS systems and applications.

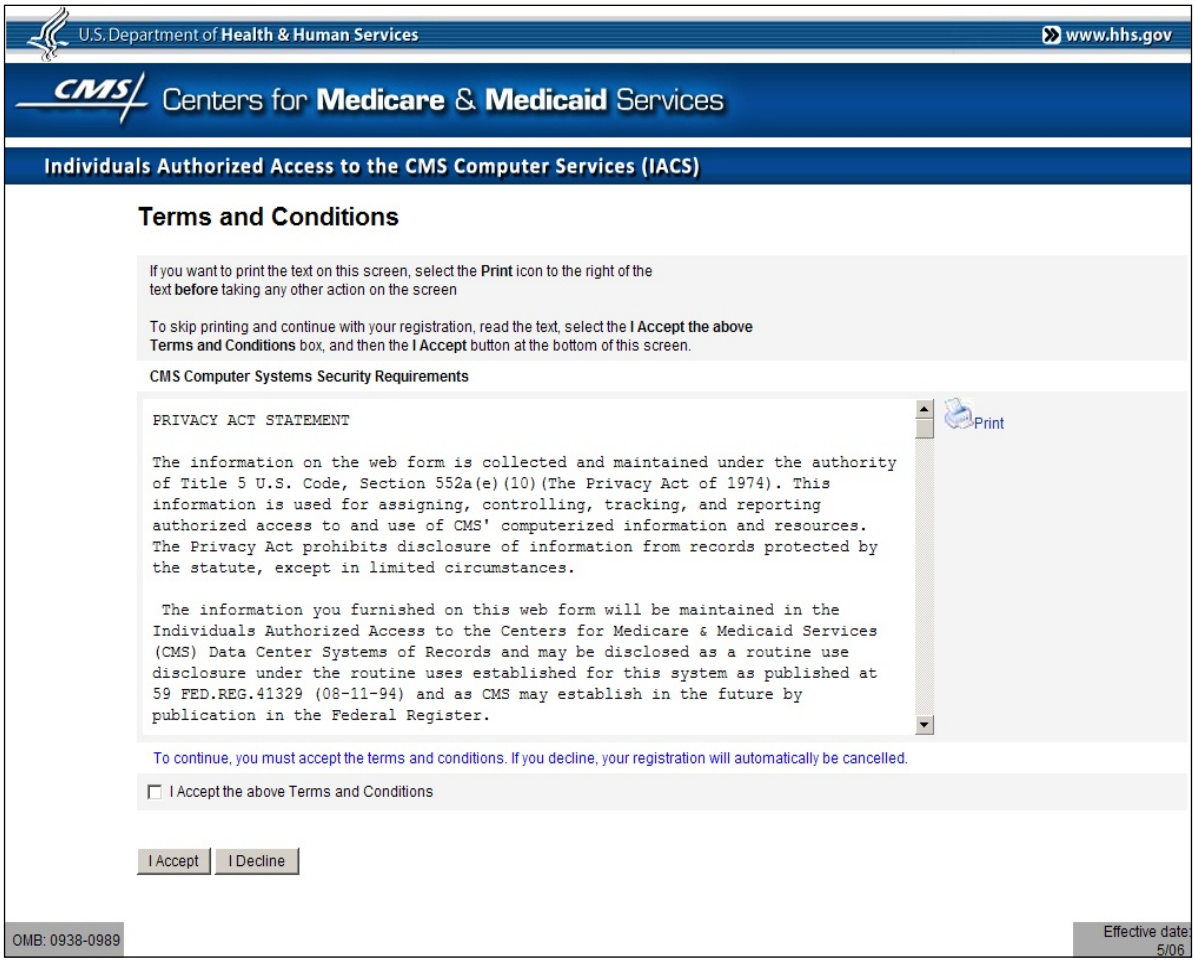

Figure 2: Terms and Conditions Screen

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

To accept, the user must select the ***I Accept the above Terms and Conditions*** check box and indicate their agreement by selecting 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 he confirms this, his IACS session is cancelled and a screen indicating this is displayed.

3.3 Conventions

This User Guide will present typical account registration and 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.

3.3.1 Formatting Conventions

The following formatting conventions have been used in this User Guide.

1. Screen names are indicated in **plain bold**.

   Example:

   The **CMS Applications Portal Introduction** screen will display as illustrated in Figure 6.

2. References to partial screens displayed or buttons to be acted upon are indicated in ***bold italics***.

   Examples:

   Available applications are listed in the ***New User Registration Menu for CMS Applications*** area of the **CMS Applications Menu** screen

   Or

   Select the ***Next*** button to continue.

3. References to hyperlinks are indicated in blue, underlined text.

   Example:

   Select the Modify Account Profile hyperlink.

4. References to figures and sections will take the user to that figure or section when selected.

   Examples:

   Go to Section 1.0 – *The number is the link. The user will be brought to that Section when the number is selected.*

   Or

   As illustrated in Figure 1 – *The combination of Figure and Number is the link. The user will be brought to that Figure when he selects either.*

5. When an action is required on the part of the reader, it is indicated by a line beginning with the word **Action:**

   Example:

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

6. Explanatory notes will be indicated with the word **Note:**

   Example:

Note: The name of the MEIC Helpdesk has been changed to the MCARE Helpdesk.

7. Input fields are indicated in *plain italics*.

   Example:

   Enter the last name in the *Last Name* field.

8. Required input fields are indicated by an asterisk to the right of the field. These fields must be completed.

9. Some fields have help icons to their left if the user needs help on completing an input field. This icon is displayed 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 not to reflect actual IACS Users and/or Accounts.

3.4 Cautions & Warnings

IACS provides on screen cautions and warnings to help guide users through procedures that require specific data formatting or are designed 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.

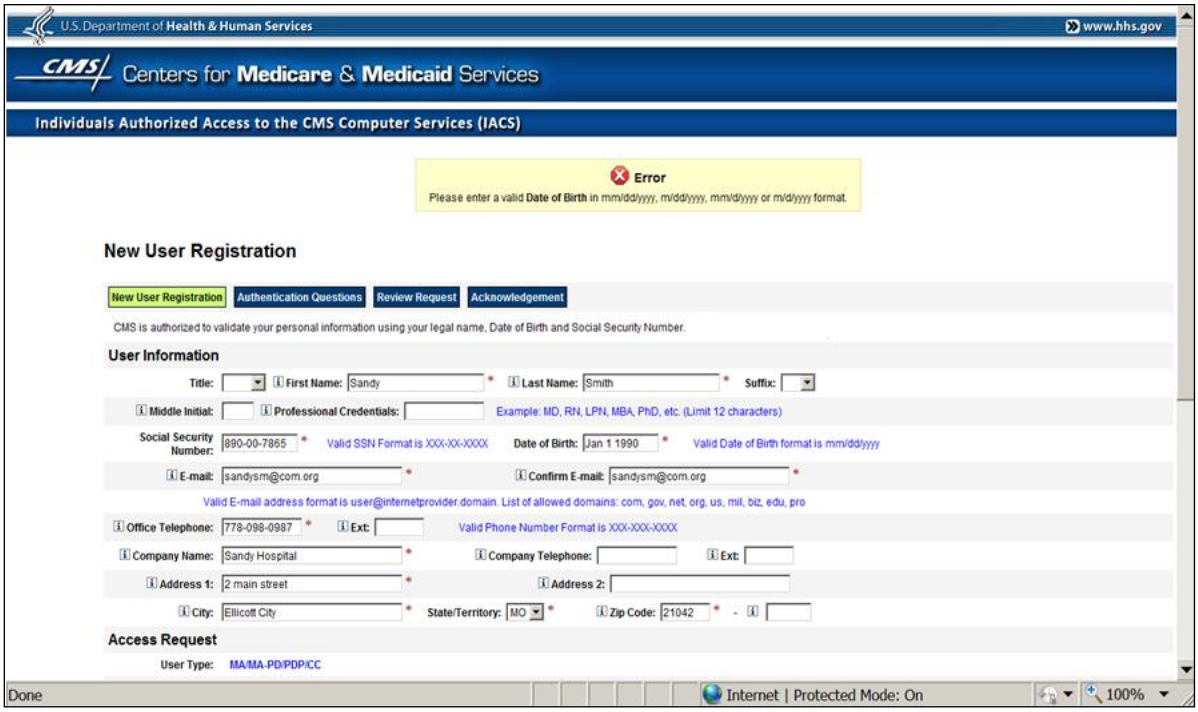

Figure 3: Warning Message

The message shown in Figure 3 notifies the user that an incorrect format has been used for Date of Birth (DOB) and also provides the correct format that the user should follow.

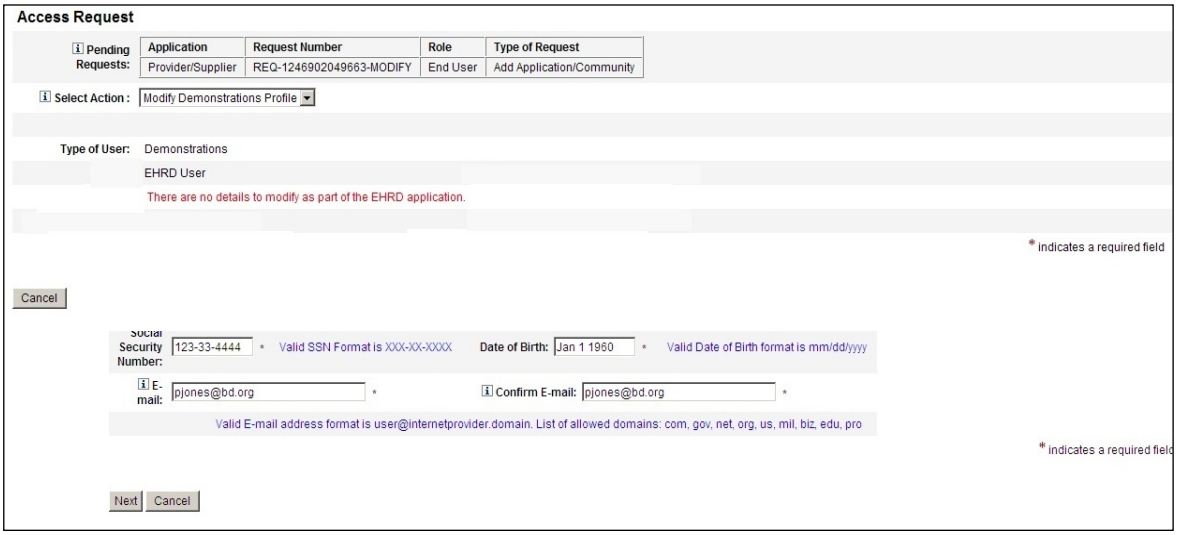

Figure 4: Information Message

The message shown in Figure 4 notifies the user that the option selected cannot currently be used.

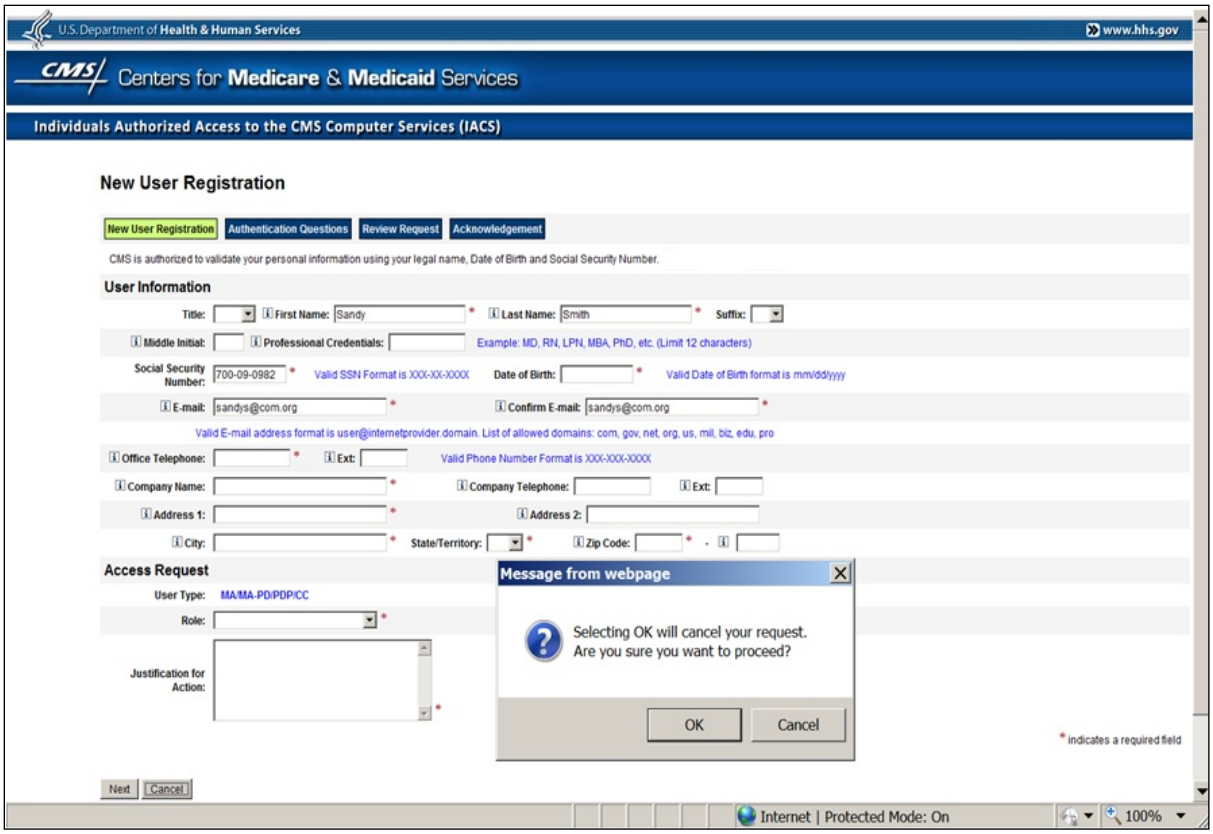

Figure 5: Caution Message

The message shown in Figure 5 cautions the user that the user's action will cancel the registration and allows the user to proceed by selecting the ***OK*** button or to stop by selecting the ***Cancel*** button.

4.0 Getting Started – New User Registration

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 is installed on the PC.

4. **Pop-up Blockers:** Disable pop-up blockers prior to attempting to access the CMS Applications Portal.

The user should contact the Helpdesk if he has questions about any of the above criteria. For Helpdesk contact information, see Section 9.2.

4.1 Available 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
- Approvers are approved by Authorizers (for some applications, the Help Desk 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:

Coordination of Benefits

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

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 Help Desk User**
  - The HSTP Help Desk User is the top of the chain user who will provide helpdesk assistance to CSP - HSTP Application users. The HSTP Help Desk 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 HSTP Approver role.
- **HSTP Approver**
  - The HSTP Approver is trusted with approving new user creation requests, requests for Modify user profile, and re-certification for HSTP End Users.
- **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 Help Desk User**
  - The MCSIS Help Desk user is the top of the chain user who will provide helpdesk assistance to CSP - MCSIS Application Users. The MCSIS Help Desk 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 MCSIS Approver role.
- **MCSIS Approver**
  - The MCSIS Approver is trusted with approving new user creation requests, requests for Modify user profile and re-certification for MCSIS End Users.
- **MCSIS End User**
  - The MCSIS End User is a staff member who is trusted to perform Medicare business for the Application.

CSR Application:

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 will provide helpdesk assistance to CSR Application Users. The LSA role is an end user role that does not have approval authority.

DMEPOS Bidding System (DBidS) Application:

Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) Competitive Bidding System - The DMEPOS Competitive Bidding System is for suppliers submitting a bid for selected products in a particular Competitive Bidding Area (CBA).

- **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 and DMEPOS IT Administrator roles.

- **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.

- **Authorized Official (AO)**
  - The AO is an appointed official to whom the organization has granted the legal authority to enroll it in the Medicare program and to commit the organization to fully 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 it in the Medicare program and to commit the organization to fully 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.

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

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

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

- **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 Authorized Official, AO, and/or Backup Authorized Official, 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. Through this web application, users may submit CWF Assistance Requests, MSP Inquiries, PDC Inquiries, and Workload Tracking Reports.

- **ECRS HelpDesk**
  - The ECRS HelpDesk is the top of the chain user who will provide helpdesk assistance for the ECRS Application Users. The ECRS Help Desk 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**
  - 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 the application to get access to their Gentran mailbox.

- **Gentran Helpdesk**
  - The Gentran Helpdesk is the top of the chain user who will provide helpdesk 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.

- **MCARE Helpdesk**

- The MCARE Helpdesk (formerly called the MEIC Helpdesk) is the top of the chain user who will provide helpdesk assistance for the CMS Medicare Eligibility Integration Contractor (MEIC) and approve HPG Users. If the User Approver does not exist, the request is routed to the MCARE Helpdesk.

- **Security Official(SO)**
  - The Security Official represents the organization or facility in IACS. There can be two Security Officials at a facility or organization.

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

- **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, except for P-type submitters, is automatically associated to a Gentran mailbox.

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

MA/MA-PD/PDP/CC Application:

Medicare Advantage/Medicare Advantage - Prescription Drug/Prescription Drug Plan/Cost Contracts/ Medicaid State Agency

- **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 (Integrated User Interface) Help Desk and IUI Administrator role.

- **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.

- **Approver**
  - The Approver, also known as the EPOC, is trusted with approving new user creation requests, requests for Modify user profile and re-certification for the users with Submitter, Representative, and Contractor 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.

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

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

- **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 automatically associated to a Gentran mailbox.

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 and related data through the MARx online user interface (MARx UI).
  - This role will not have access to Gentran Mailbox.

- **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 automatically associated to a Gentran mailbox.

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 automatically associated to a Gentran mailbox.

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.

- **MAPD Helpdesk**
  - The MAPD Helpdesk User is an authorized representative of CMS who will provide helpdesk assistance to MA/MA-PD/PDP/CC Application Users.

- **MAPD Helpdesk Admin**
  - The MAPD Helpdesk Admin User is an authorized representative of CMS who will provide administrative helpdesk assistance to MA/MA-PD/PDP/CC Application Users information.

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; 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 helpdesk 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**
  - State Technical Contact is a staff member who is trusted to perform Medicare business for the Application.

MED Application:

The Medicare Exclusion Database, MED, is updated monthly with sanction and reinstatement information on excluded providers, and is made available to approved entities only.

- **MED Help Desk User**
  - The MED Help Desk User is the top of the chain user who will provide helpdesk 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 automatically associated to 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 automatically associated to 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 automatically associated to a Gentran mailbox.

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

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 is the top of the chain user who is an authorized representative at the QualityNet Help Desk that will provide helpdesk assistance for the PQRS/eRx Application Users.

- The PQRI Help Desk 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), Individual Practitioner (IP), Registry End User, EHR Vendor, PQRI Maintainer, and PQRI Admin roles.

- **Security Official**
  - The Security Official is the authorized representative of his/her 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).

- **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 also 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 Users Registration.

- **Individual Practitioner**
  - An Individual Practitioner is a solo practitioner enrolled in Medicare reporting with a single NPI.

- **Individual Practitioner with 2-FactorAuthentication**
  - An Individual Practitioner is a solo practitioner enrolled in Medicare reporting with a single NPI. If the Individual Practitioner would like to Submit EHR / PII data, they must select the "Request EHR Submission (2 factor) role" radio button within their Individual Practitioner IACS Profile.

- **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).

- **Registry End User**
  - A Registry End User is part of the Registry Organization and can also 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.
- **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.
- **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.

Provider Statistical and Reimbursement / System Tracking for Audit and Reimbursement Application:

This registration link is for users requesting access to PS&R and/or STAR application. During new user registration, users are required to select either FI/Carrier/MAC, Providers, CMS, or PS&R/STAR System Maintainer.

- **PS&R/STAR Helpdesk**
  - The PS&R/STAR Helpdesk is the top of the chain user who is an authorized representative that provides helpdesk assistance to the PS&R and STAR application users.
  - The PS&R/STAR Helpdesk approves Security Officials (SOs) that work for FI/Carrier/MAC and Medicare Providers.
- **PS&R/STAR Security Official**
  - The PS&R/STAR Security Official is the authorized representative of his/her 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/her 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 information in the Organization profile 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.

- **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.

4.2 Basic Registration Steps

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 document. Noteworthy differences for other roles will be identified in Section 4.3.

Prior to registering in IACS, the user should have received information on registration details from their Organization or CMS point of contact. This information may include:

- The role the user will register for in IACS
- The user (if registering as SO for HETS UI, PQRI and PS&R Provider Organizations) will be asked to supply additional information during registration such as Organization Legal Name, Taxpayer Identification Number, street address, etc.

Note: If the user has not received information on registering for IACS, the user needs to check with his Organization prior to registering for IACS.

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 as illustrated in Figure 1.

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 6.

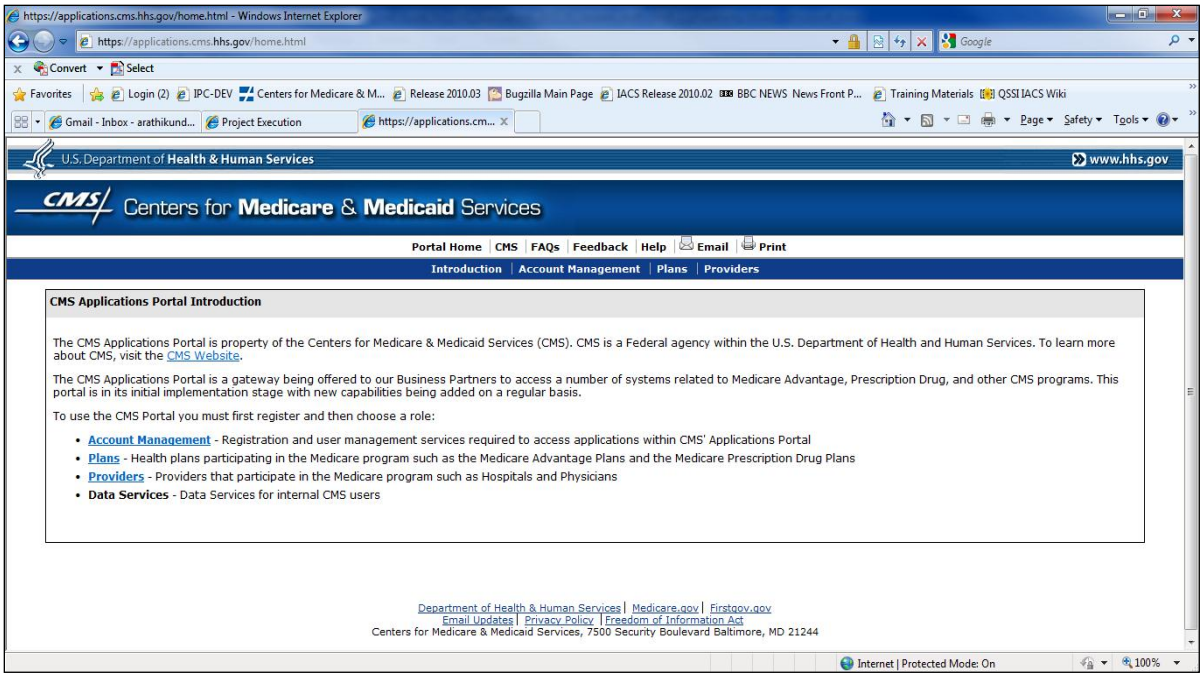

Figure 6: CMS Applications Portal Introduction Screen

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

The **Account Management** screen will display as illustrated in Figure 7.

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 Helpdesk contact information and E-mail hyperlinks.

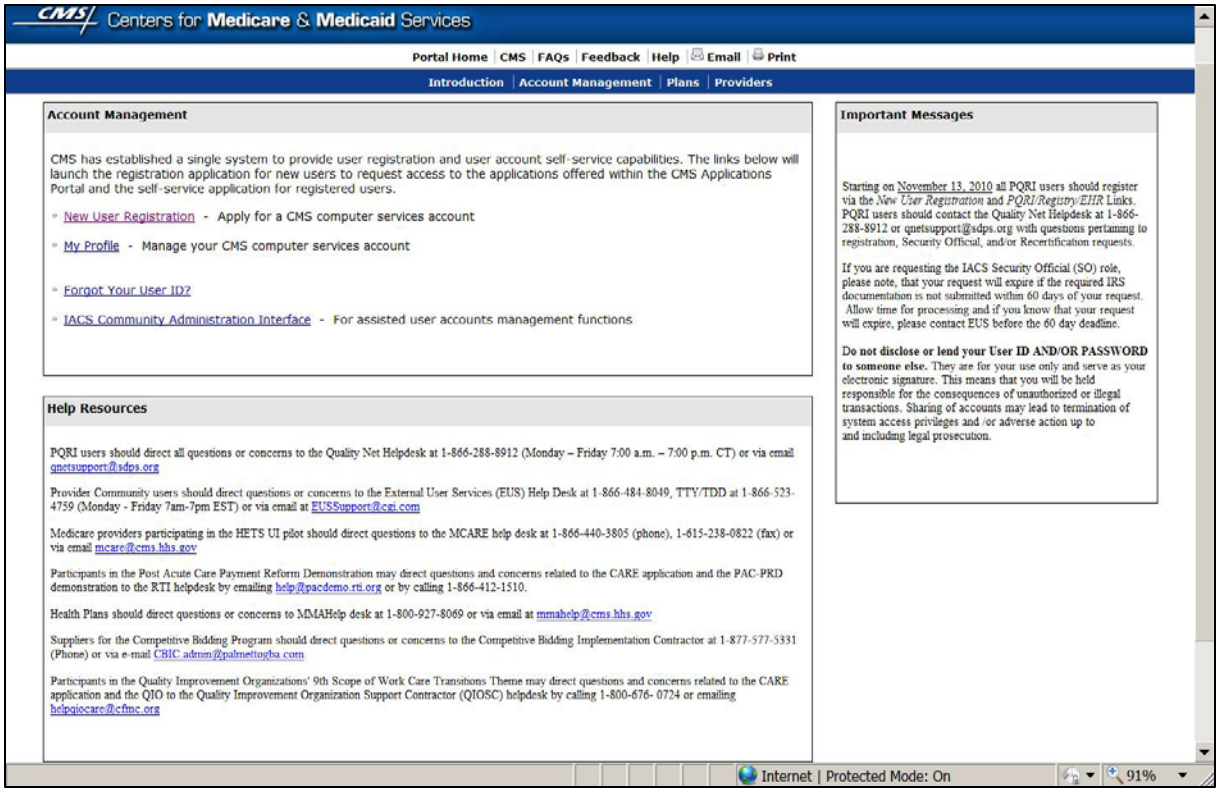

Figure 7: Account Management Screen

Action: Select the New User Registration hyperlink.

The **New User Registration Menu** screen will display as illustrated in Figure 8.

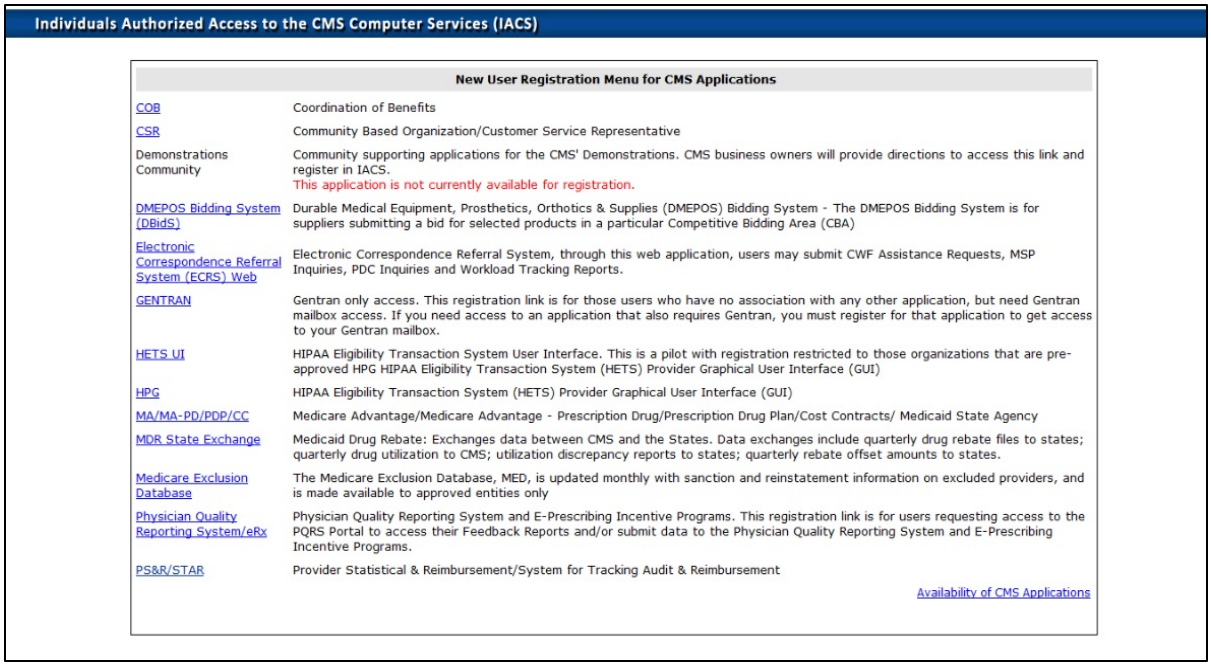

Figure 8: New User Registration Menu Screen

Note: When an application is not available for registration, the link will be "grayed out" and a message will be displayed in red stating that "***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 as illustrated in Figure 2.

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 9.

In the ***User Information*** area of the screen, the user will enter information needed by the system to identify the user and to 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.

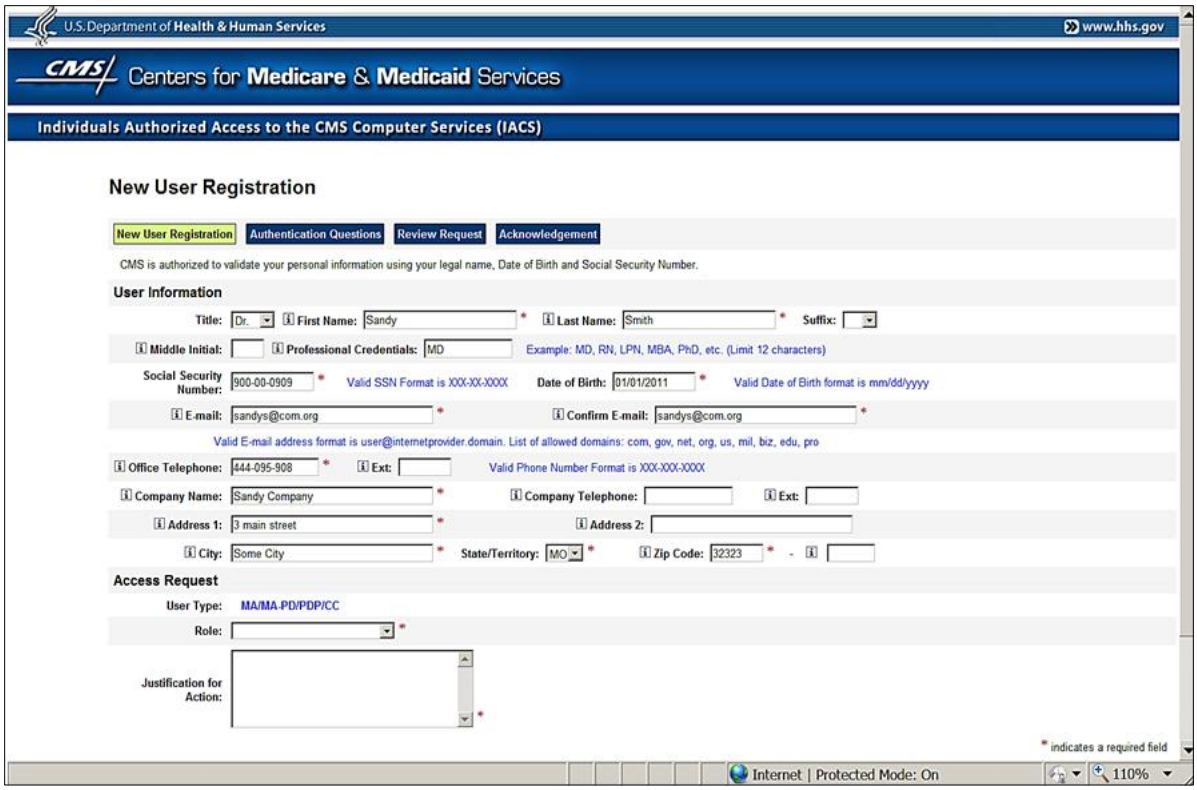

Figure 9: New User Registration Screen

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

Note: The information must be entered in the fields in the formats specified on the screen.

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. There are some minor differences in the information collected and the way the user will select/input this information for the various Applications.

The ***Access Request*** area, as illustrated in Figure 10, 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 10.

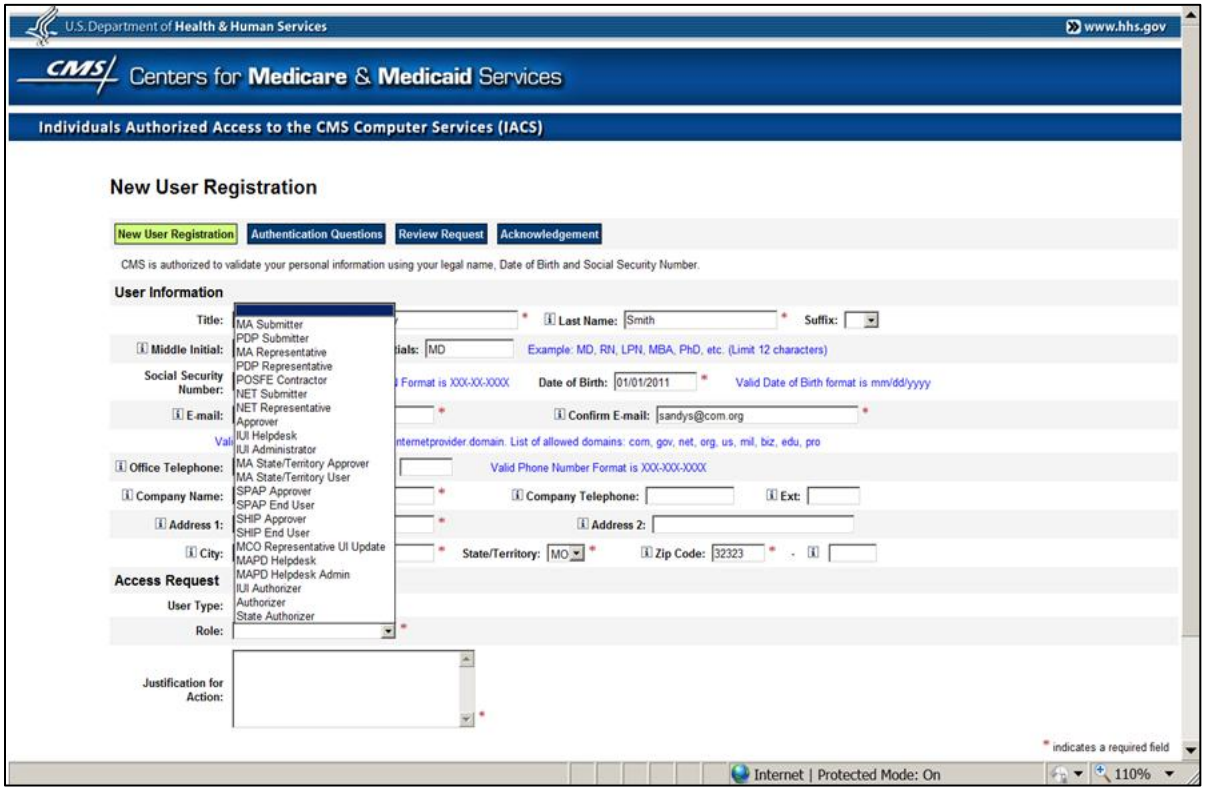

Figure 10: New User Registration Screen: Access Request Area, Role Drop-down

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.

If the user selects the role of MA Submitter, the screen will refresh and *Contract Number* fields will display as illustrated in Figure 11. The user may enter a Contract Number in the fields displaying, which are:

- *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.

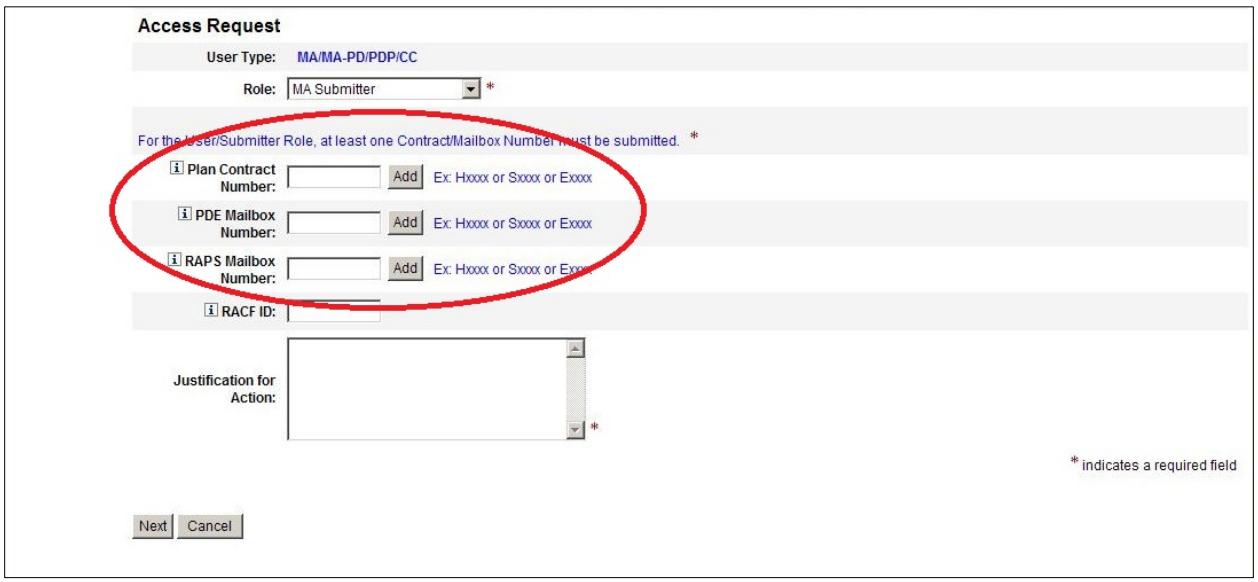

Figure 11: New User Registration Screen: Access Request Area, MA Submitter

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. This is illustrated in Figure 12.

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 Helpdesk 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 that he have one, the system will automatically assign him a *RACF ID* once his request is approved.

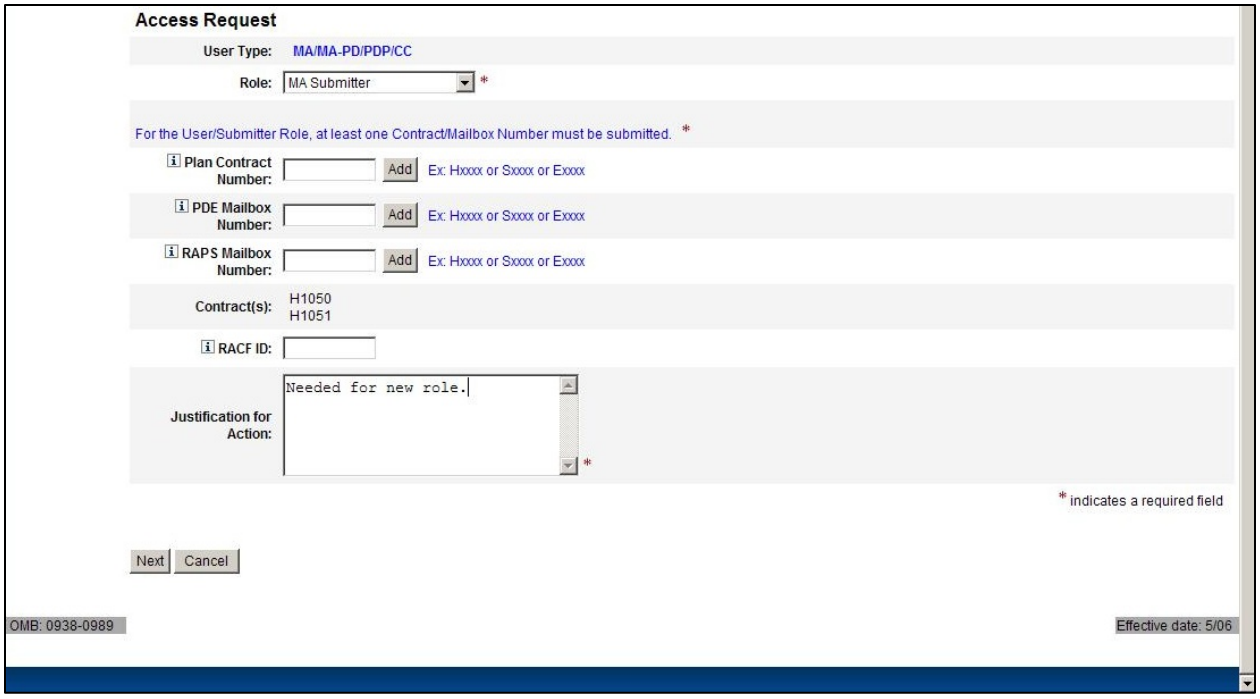

Figure 12: New User Registration Screen: Access Request Area, Contract Number & RACF ID Field – MA Submitter

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 the 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.

If the data is validated, the system will display the **Authentication Questions** screen as illustrated in Figure 13.

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 ***Forgot your User ID?*** or ***Forgot your password?*** features.

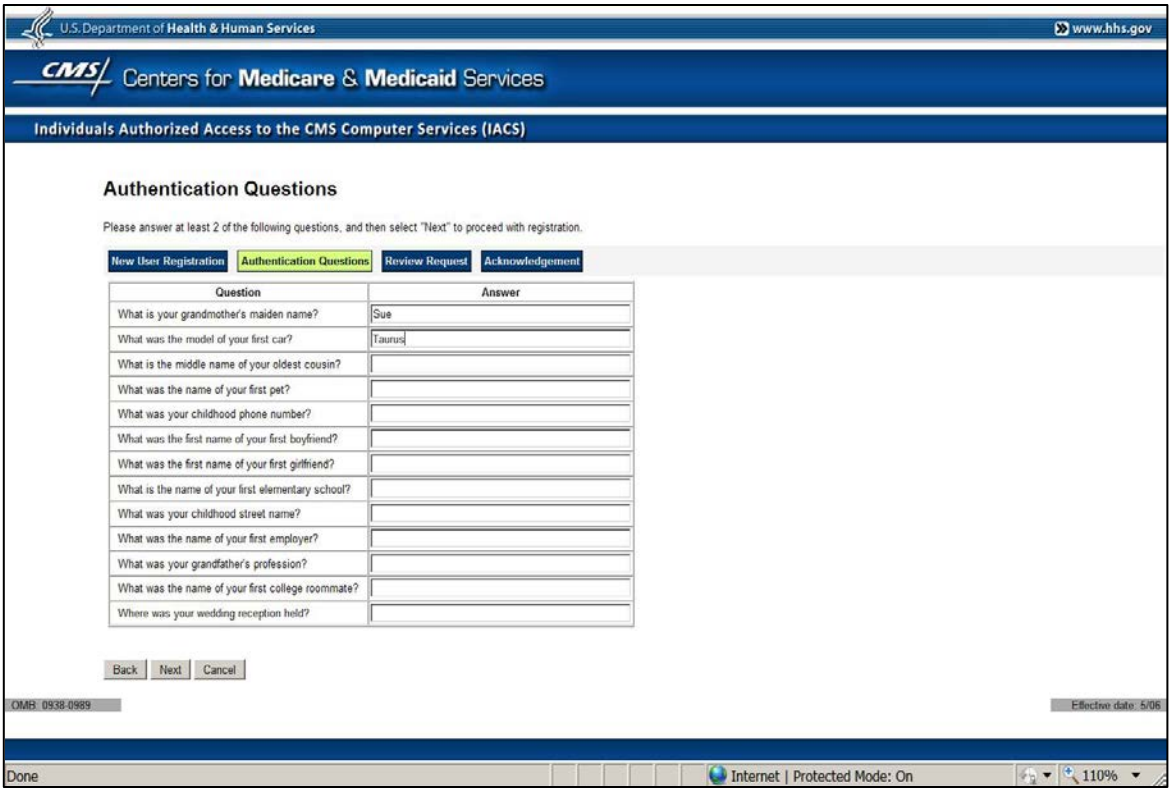

Figure 13: Authentication Questions Screen

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 14. The User Guide information for this screen and Figure 15 needs to be reviewed to see how to complete the ***New User Registration*** process.

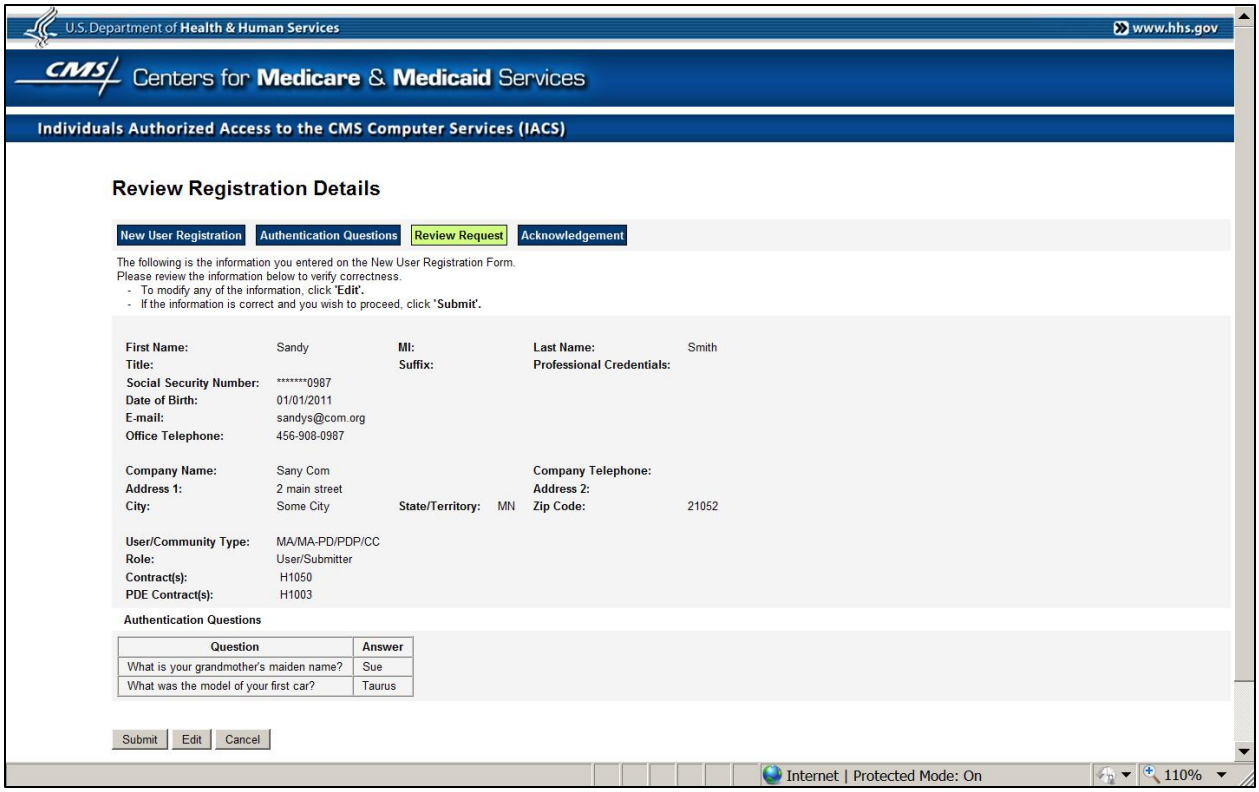

Figure 14: Review Registration Details Screen

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

The ***Edit*** button must be selected if there are any modifications that are to be made to the registration information. The **New User Registration** screens will be redisplayed with all the information populated in the appropriate fields. The user may modify the information that he wants and, when finished, he should select the ***Next*** button. He will again be presented with the **Review Registration Details** screen.

If he selects the ***Cancel*** button, the application request is cancelled and all the 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. A **Registration Acknowledgement** screen will display as illustrated in the example in Figure 15.

The **Registration Acknowledgement** screen indicates that the registration request has been successfully submitted and provides a tracking number for the request. 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.

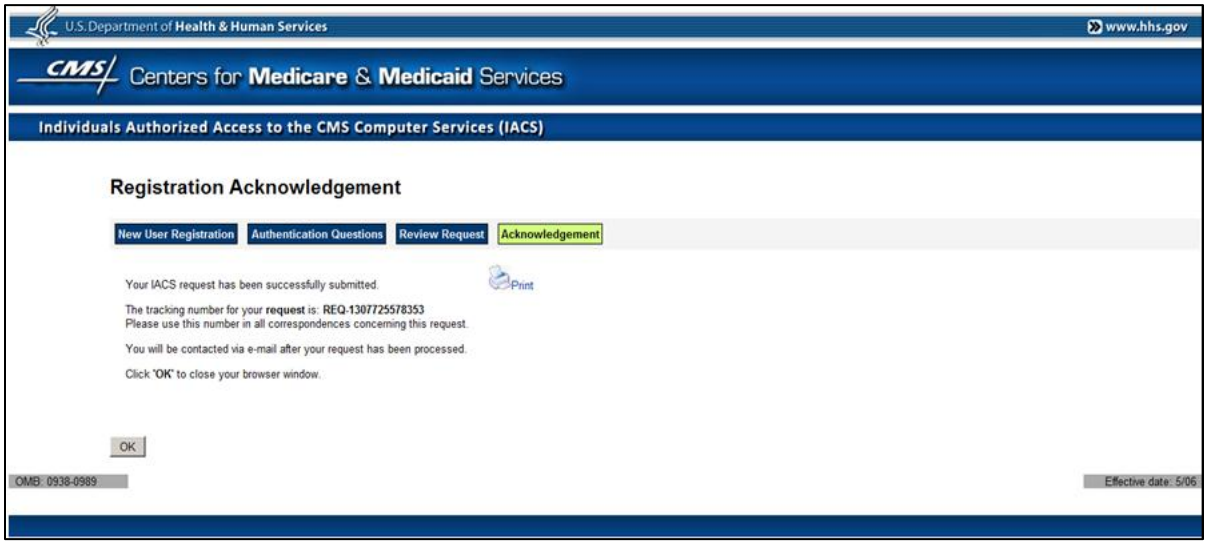

Figure 15: Registration Acknowledgement Screen

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.

After the user completes the IACS New User Registration, he will be sent an E-mail confirming that IACS has received his request and providing him with a Request Number. The user should use that request number if he needs to contact the Helpdesk regarding his request.

Note: If the E-mail notification has not been received within 24 hours after the user registers, he will need to contact his Helpdesk. See Section 9.2 for Helpdesk contact information.

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

Once the Approver or EPOC 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 receive an E-mail informing him that his request has been denied. The E-mail will also provide 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 automatically and the user will receive an E-mail notification to this effect. The user will then have to go to the **New User Registration** screen, re-enter the information, and resubmit the registration request.

Note: Table 1 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

Table 1: Role Type and Request Timeout Days

4.3 Exceptions to Basic Registration Steps

4.3.1 Exceptions to COB Application Registration

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

Note: A User who registers as an approver for COB will have the approval authority for all users of all organizations under COB.

4.3.2 Exceptions to CSR Application 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.

4.3.3 Exceptions to DMEPOS Registration

- All Users registering into 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.

- After selecting "DMEPOS Bidding System (DBidS)" from the New User Registration Menu page, users registering for the DMEPOS Application 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 a bidder with access to the DBidS Application.
    - I want to register for the CBIC-Tier1, CBIC-Tier1, CBIC-Input, DMEPOS-IT Administrator, DMEPOS-IT Help Desk, DMEPOS Authorizer1 or DMEPOS Authorizer2 role for the DBidS Application.

Note: A User Group Administrator role does not exist for DMEPOS.

4.3.4 Exceptions to 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 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 automatically associate the new User ID with the appropriate Gentran mailbox.

4.3.5 Exceptions to HETS UI Application 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.

Note: At least one Contractor Name and Associated Billing NPI are required.

4.3.6 Exceptions to HPG Application Registration

- The User registering as a HPG User will have to enter the Submitter ID.

Note: Submitter ID starting with 'P' will not have access to the Gentran Mailbox.

4.3.7 Exceptions to MA/MA-PD/PDP/CC Application Registration

MA Representative and MA Submitter:

- A user registering as an MAMA Submitter can only enter Contracts starting with ‘H’, ‘E’, ‘S’ and ‘9’.

MA State Territory Approver and User:

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

MCO Representative UI Update:

- A user registering as a MCO Representative UI Update can only enter Contracts starting with ‘H’, ‘E’, ‘S’ and ‘9’.

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.

PDP Submitter and PDP Representative:

- A User registering as a PDP Submitter can only enter contracts starting with ‘S’, ‘E’ and ‘9’.
- The user will have access to a Gentran Mailbox.

POSFE Contractor:

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

SHIP Approver and User:

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

SPAP Approver and User:

- A User registering as a SPAP Approver / User will have to select a State from a list of all states

4.3.8 Exceptions to PQRS/eRx Registration

Security Official:

- A user registering as a Security Official may either choose 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.

Backup Security Official:

- The user will be required to search and associate to an existing PQRI Organization during the self-registration process.
- A user registering as a Backup Security Official will have the option to select the 2-Factor Authentication Approver Role.

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 in that Organization selected by the user.
- The user will be able to choose the Preferred 2nd factor pass code notification method by selecting either 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.
- 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 either 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.
- 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.

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 to the system 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 either 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.

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.

PQRS/eRx Request timeout days:
IACS follows an application specific request timeout process for PQRS/eRx application which differs from the standard request timeout followed by most of the applications as illustrated in Table 1.

Table 2 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 days
Security Official	60 days
Backup Security Official	60 days
End User	60 days
EHR Submitter Registry End User	60 days 12 days
EHR Vendor	12 days
PQRI Admin Individual Practitioner	12 days 60 days
PQRI Maintainer	12 days
PQRS Submitter PQRS Representative	12 days 12 days

Table 2: PQRS/eRx Role Type and Request Timeout Days

4.3.9 Exceptions to PS&R/STAR User Registration

After selecting "PS&R/STAR" from the New User Registration Menu page, users registering for the PS&R and STAR Applications will have to select one of the four radio buttons to proceed. The text of the radio buttons is shown below.

- 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 either choose 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.

4.3.10 Exceptions to 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 Help Desk Users in certain Applications). Thus, the top of the chain user is either the Authorizer or the Help Desk User. He is the last user in the chain that is expected to have an IACS User ID.

Registration, profile modification, and annual certification requests for top of the chain users are routed and approved using E-mail. An E-mail is sent to the corresponding Business Owner (or designee) with 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.

Refer to Section 4.1 Available Roles for the top of the chain roles in each application

5.0 Login

When the user logs into IACS, he needs 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. Refer to Figure 1 for an illustration of this screen.

The **CMS Applications Portal Introduction** screen will display as illustrated in Figure 6.

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 7.

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

The **Terms and Conditions** screen will display as illustrated in Figure 2.

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 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 this, 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 16.

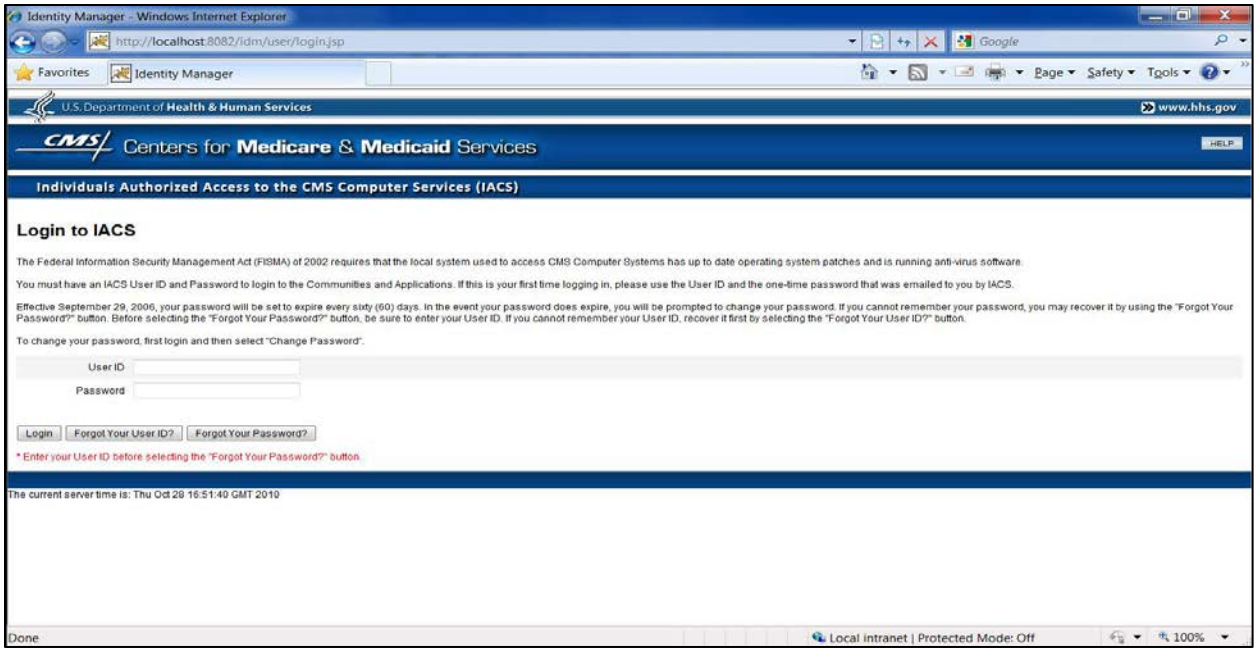

Figure 16: Login to IACS Screen

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

Action: Enter your ***Password.***

Action: Select the ***Login*** button.

The system will display the **My Profile** screen as illustrated in Figure 17.

Note: If this is the first time that the user is logging into IACS, he will be prompted to change his temporary, one time password. After the user has successfully changed his temporary password, the system will display the **My Profile** screen.

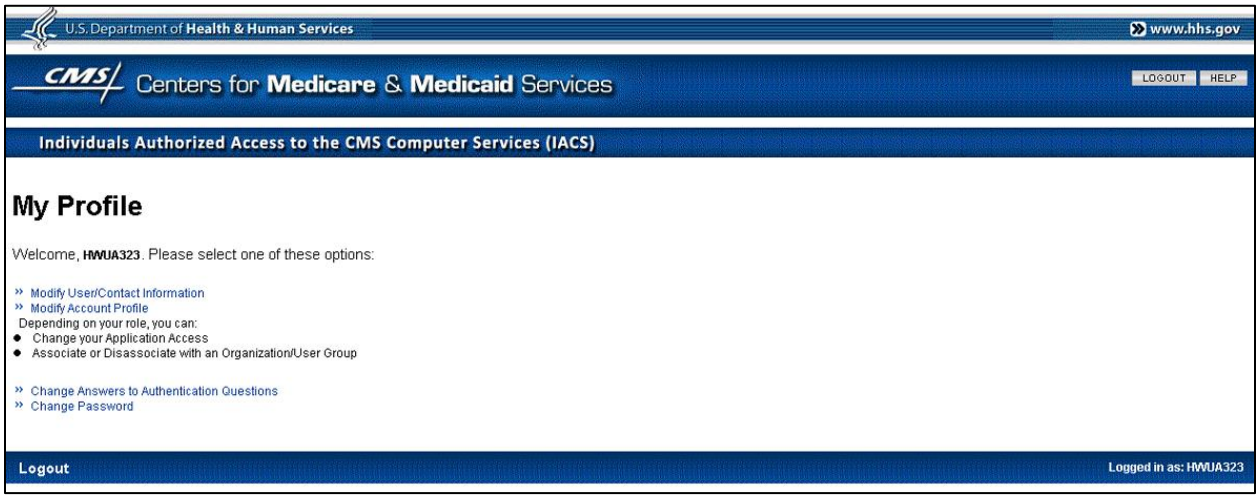

Figure 17: My Profile Screen: MA/MA-PD/PDP/CC Application Users

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

6.0 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 8 characters long.
- Passwords 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 4 consecutive characters of any of the previous 6 passwords.
- The password must be different from the previous 6 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

6.1 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 login 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.

6.2 Disabled Accounts

CMS requires that 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 he will be unable to access any applications.

The user needs to follow the steps below to re-enable the user's 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 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. Login 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 his Helpdesk.

6.3 E-mail Notifications

The following E-mail notifications are sent to all IACS users notifying them to change their passwords prior to the 60 day password expiration policy:

- E-mail sent two weeks prior to 60 day password expiration
- E-mail sent one week prior to password expiration
- E-mail sent one day prior to password expiration

The following E-mail notifications are sent to IACS users notifying them that their accounts will be disabled due to 180 days of account inactivity:

- E-mail sent two weeks prior to disabling user account
- E-mail sent one week prior to disabling user account
- E-mail sent one day prior to disabling user account
- E-mail sent on 180th day since last successful login, notifying the user that their account has been disabled due to inactivity

6.4 Self Service Features

Self Service features can be used to retrieve the User ID and Password.

6.4.1 Retrieving User ID

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

1. From the Login page, select the ***Forgot Your User ID?*** button.
2. When prompted, enter the *First Name*, *Last Name*, *Date of Birth*, *SSN*, and *E-mail*.

Note: For Login instructions, Section 5.0 should be reviewed.

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*.

6.4.2 Retrieving Password

The user needs to follow the steps below to retrieve his Password from the Login Screen:

1. From the Login page, select the ***Forgot Your Password?*** button.
2. When prompted, answer the Security Questions and Authentication Questions, and Change the Password.

Alternatively, the user can also use the Account Management screen to retrieve the Password, 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 My Profile hyperlink in the **Account Management** screen.
4. Accept the Terms and Conditions.
5. Select the Forgot your Password? hyperlink.
6. When prompted, answer the Security Questions and Authentication Questions, and Change the Password.

7.0 Using the System – Managing Profiles

The following section provides the most common steps to modify a user's profile. These actions are available only for an existing user. As part of managing a user profile, the user can perform the following actions:

- **Modify** User and Professional Contact details pertaining to the user's IACS ***Access 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** to associate and/or disassociate with other Organizations within an Application

Note:

- The User may only request and have one role for a CMS application. PQRS/eRx and PS&R/STAR applications will be an exception to this by allowing end users to obtain more than one end user role.
- The User cannot be an approver and a user for the same application.

7.1 Modify the User and Professional Contact Information

To modify the IACS account profile the user must first login to IACS using his IACS User ID and password. The My Profile screen will display after successful login.

IACS provides the user with the option to modify the ***User Information*** and/or professional contact information he provided during his IACS registration or updated at a later time. If the user changes the telephone number or moves to a different address, he can update that information by selecting this hyperlink. These modifications are basic Modify Profile changes.

When the user selects the Modify User/Contact Information hyperlink, the **Modify User/Contact Information** screen will display as illustrated in Figure 18.

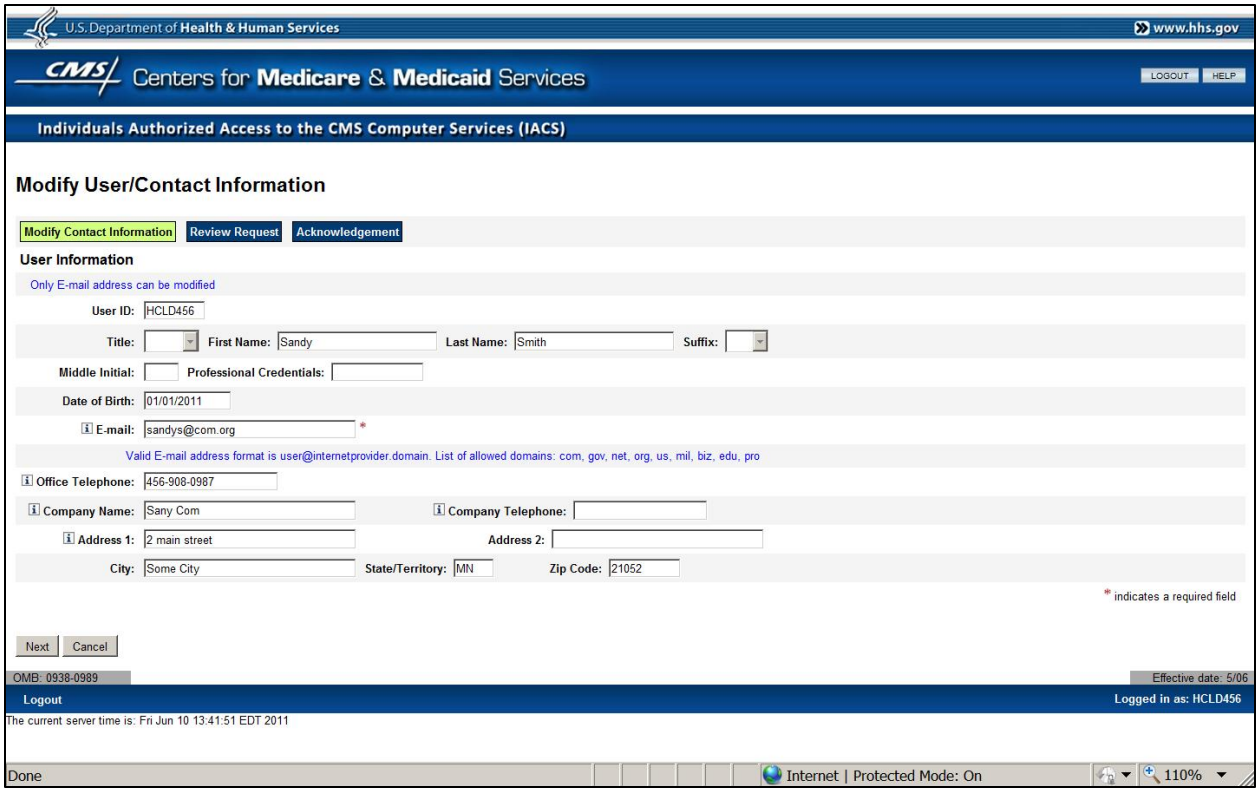

Figure 18: Modify User/Contact Information Screen

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 and proceed to the end of this Section for information on how to complete the changes.

When the user selects the ***Next*** button, the system will display the **Modify Request Confirmation** screen as illustrated in Figure 19.

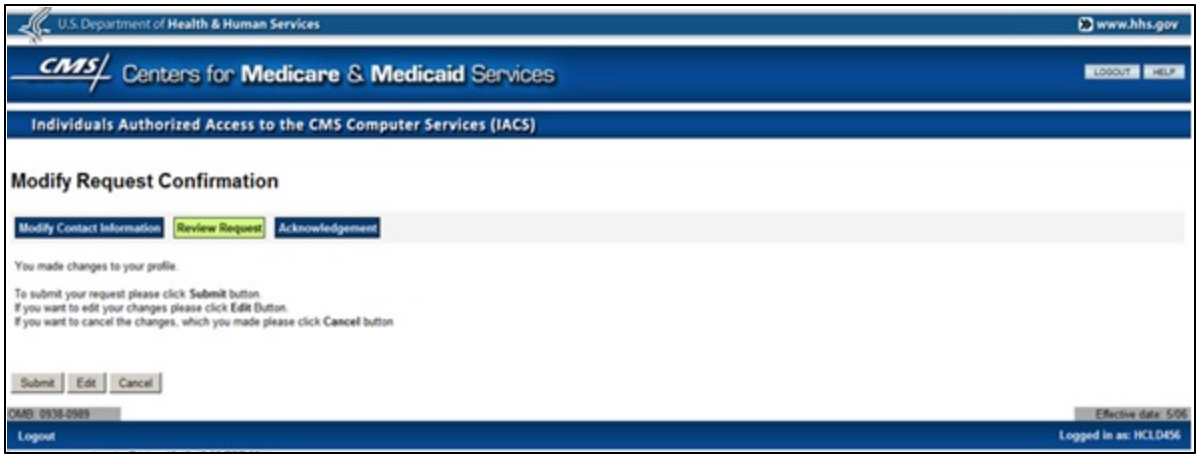

Figure 19: Modify Request Confirmation Screen

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

Note: The modifications will not be completed unless the ***Submit*** button is selected.

The ***Edit*** button should be selected to return and edit the changes.

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

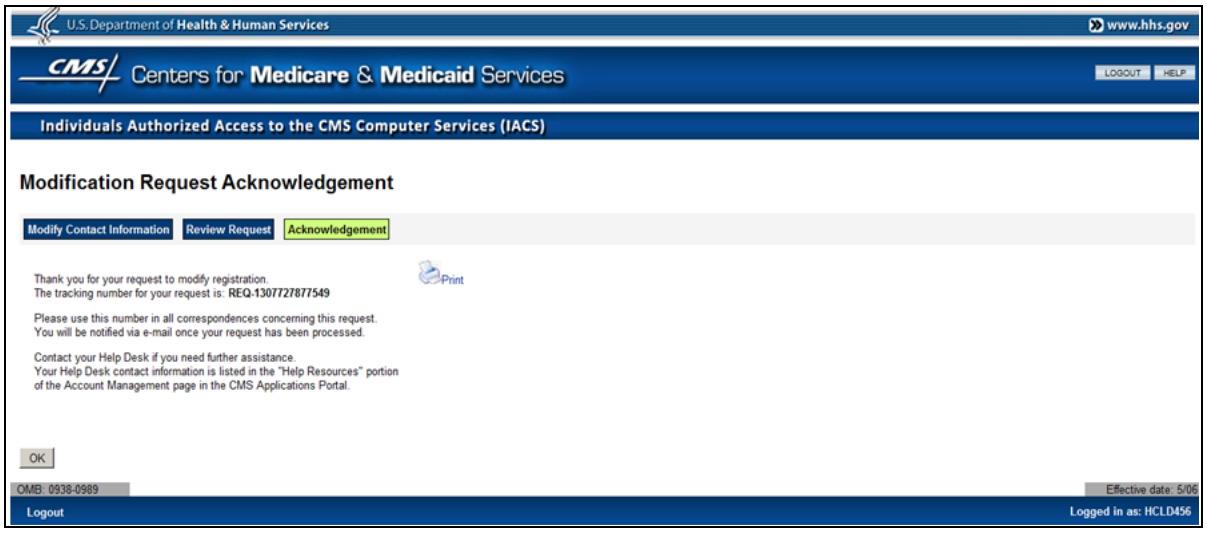

Figure 20: Modification Request Acknowledgement Screen

The **Modification Request Acknowledgement** screen indicates that the request has been successfully submitted and provides a tracking number for the request. 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 Helpdesk regarding the request. The user should also have the request number from the **Modification Request Acknowledgement** screen available for the Helpdesk.

If an E-mail notification is not received within 24 hours after the user modifies his profile, he will need to contact the Helpdesk. For information regarding Helpdesks, Section 9.2 should be reviewed.

7.2 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 21. 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 21.

Figure 21: Modify Account Profile Screen: Access Request Area – Select Action Drop-down

7.3 Adding CMS Applications

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 22. 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:

- The user may only request and have one role 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 22.

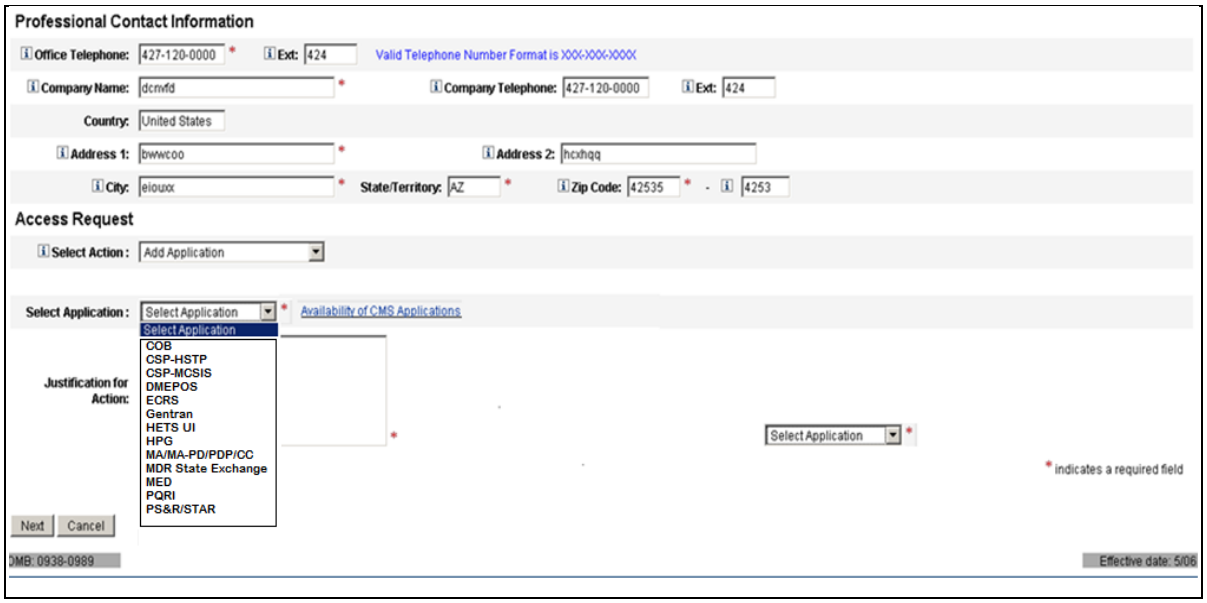

Figure 22: Modify Account Profile Screen: Access Request Area – Select Application Drop-down

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

7.4 Modify User's Profile

7.4.1 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 23.

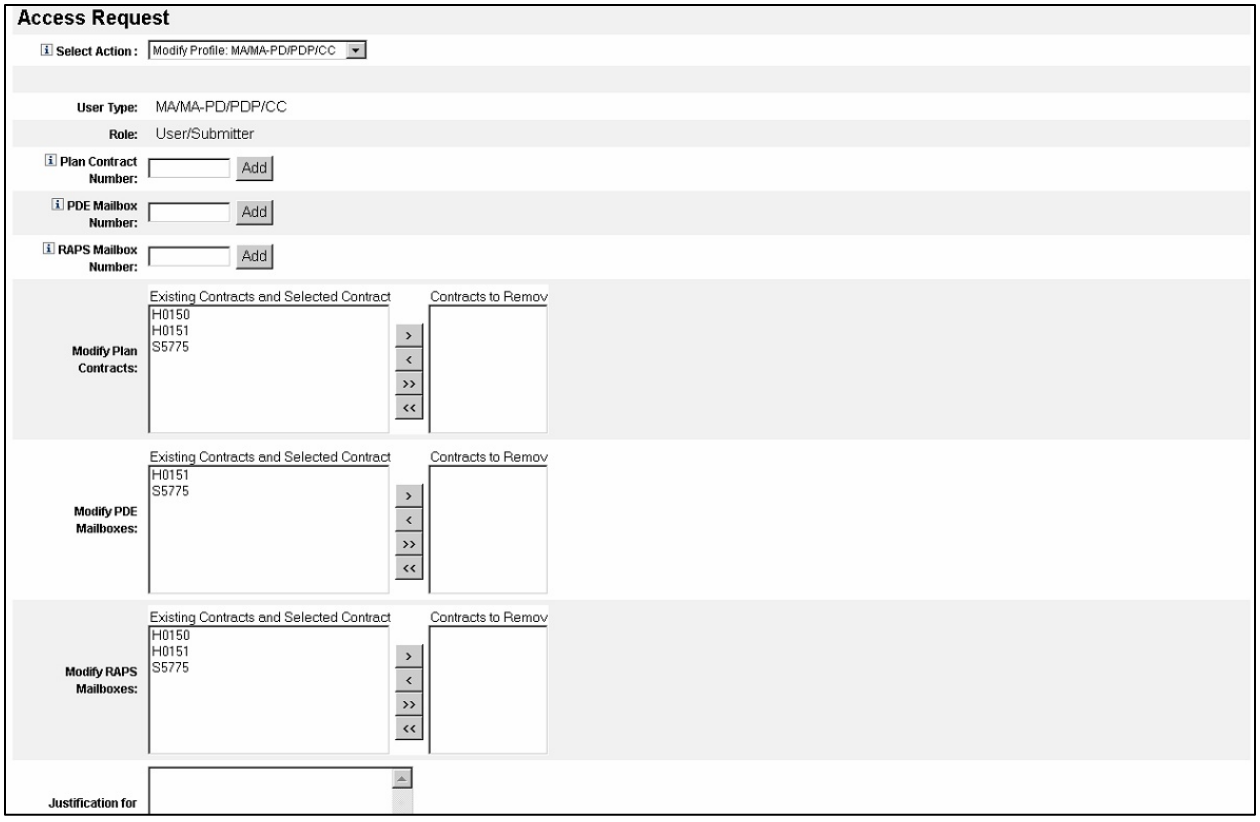

Figure 23: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC User/Submitter Add or Remove Contracts

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/Mailboxes* fields, within the *Existing Contracts and Selected Contracts* boxes, select the contract number that needs 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 needs to 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 19. The User Guide information for this screen and Figure 20 should be reviewed to see how to complete this ***Modify Account Profile*** process.

7.4.2 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 24.

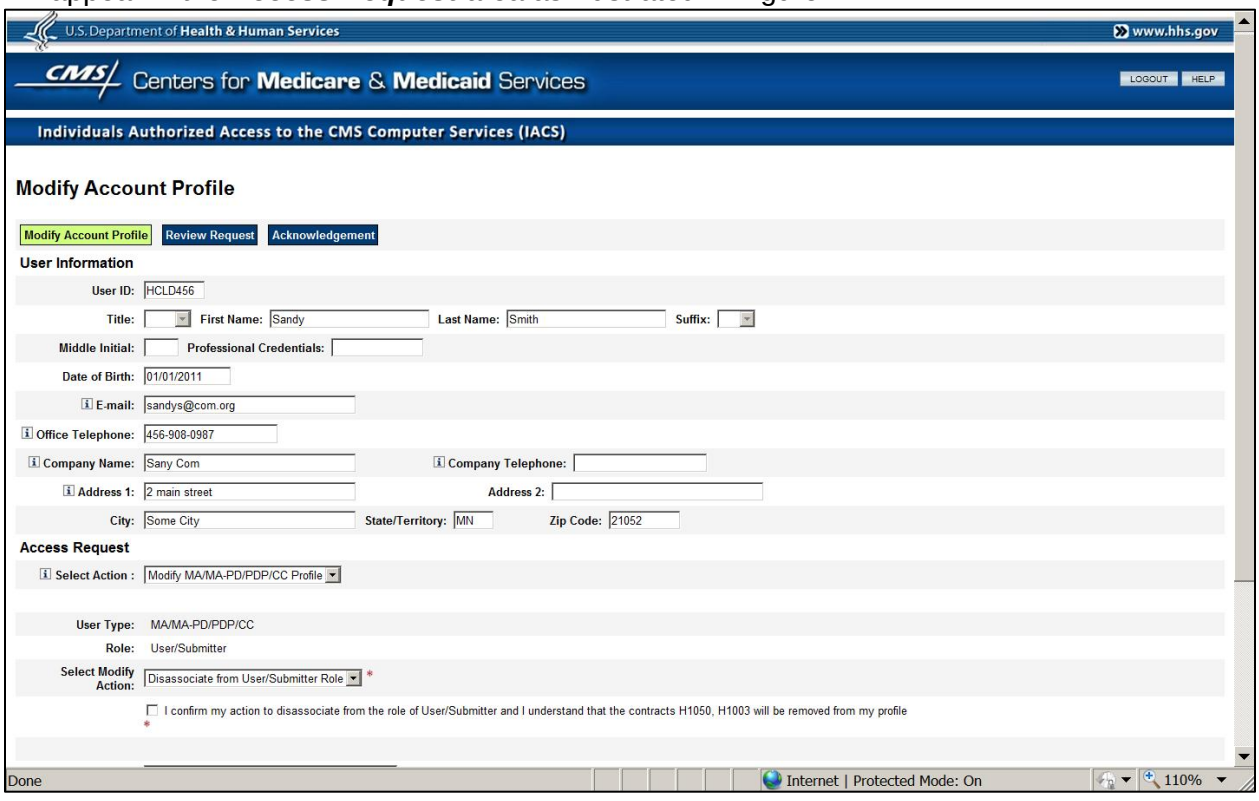

Figure 24: Modify Account Profile Screen, Access Request Area – MA/MA-PD/PDP/CC User/Submitter Disassociate from Role

Note: The message text will read, "*I confirm my action to disassociate from the role of <here the role name will be inserted> and I understand that the <here contract numbers will be inserted> will be removed from my profile."*

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 19. The User Guide information for this screen and Figure 20 should be reviewed to see how to complete this ***Modify Account Profile*** process.

7.4.3 Exceptions to Modify User Profile

Exceptions to Modify User Profile for COB Application

- COB users will not be able to disassociate from their current role.

Exceptions to Modify User Profile for CSR Application

- CSR users will not be able to disassociate from their current role.

Exceptions to Modify User Profile for MA/MA-PD/PDP/CC Application

- MA State Territory Users, SHIP Users and SPAP Users will not be able to remove the states that they have on their profile. They have to contact their approver to remove the states from their profile.

Exceptions to Modify User Profile for HETS UI Application

- A user registering as a Security Official cannot modify the Billing Provider NPI and Provider Type for his Organization.
- HETS UI users will not be able to disassociate from their current role.

Exceptions to Modify User Profile for HPG Application

- HPG users will not be able to disassociate from their current role.

Exceptions to Modify User Profile for PQRS/eRx Application

- A user registering 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

- A user registering 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 registering as an Individual Practitioner will have the option to modify his current selection of 2-Factor Authentication Role.
- All PQRS/eRx Users will be able to request for a new role under the PQRS/eRx application for an Organization that is different from their current Organization.
- A user will be able to request for one or more of the following roles within an organization and get the roles assigned upon appropriate approval.
    - EHR Submitter
    - End User
    - PQRS Submitter
    - PQRS Representative

Exceptions to Modify User Profile for PS&R/STAR Application

- A user will be able to request for 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
- A user will be able to request for 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
- A user registering as CMS and/or PS&R/STAR System Maintainer will be able to request for one or more roles and get the roles assigned upon appropriate approval.
    - PS&R User
    - PS&R Admin
    - STAR User 1 – STAR User 8

8.0 Annual Certification

Users registered through IACS for CMS Applications are required to certify annually their continued need for access to CMS systems. After November 15, 2010 IACS will begin enforcing the Annual Certification requirement for all Communities and Applications supported by IACS.

The certification due date corresponds to the anniversary of 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.

8.1 E-mail Notifications

E-mail Notifications - Users

Users will receive an advisory E-mail 45 days prior to their 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. The user will have until midnight on his Certification Date to submit the Certification Request.

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

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

E-mail Notifications – Approvers

An Approver will receive an E-mail informing him that a user under his authority has submitted a request for certification and that the request is waiting for his review and approval or rejection. 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 / 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.

Another type of E-mail that an Approver may receive is one that notifies him that a user under his authority hasn't submitted certification yet. An Approver is any user who has dependent users underneath him. For example, it can be an SO, EPOC, AO, their backups, a Help Desk or in some cases a Business Owner. When a user has taken no action to submit certification, an E-mail will be sent to the Approver advising them that the annual certification of a user directly under their authority is due. This E-mail will be sent to the Approvers 14 days, 7 days, and one day before the certification due date unless the user submits certification. This E-mail is not sent to users who do not have any dependent users under their authority.

8.2 Certifying

The **My Profile** screen will have a Certify Account Profile hyperlink as shown in Figure 25. When the user selects this hyperlink, he will be presented with the Terms and Conditions. After accepting the Terms and Conditions, the user will be presented with a screen showing his current access privileges.

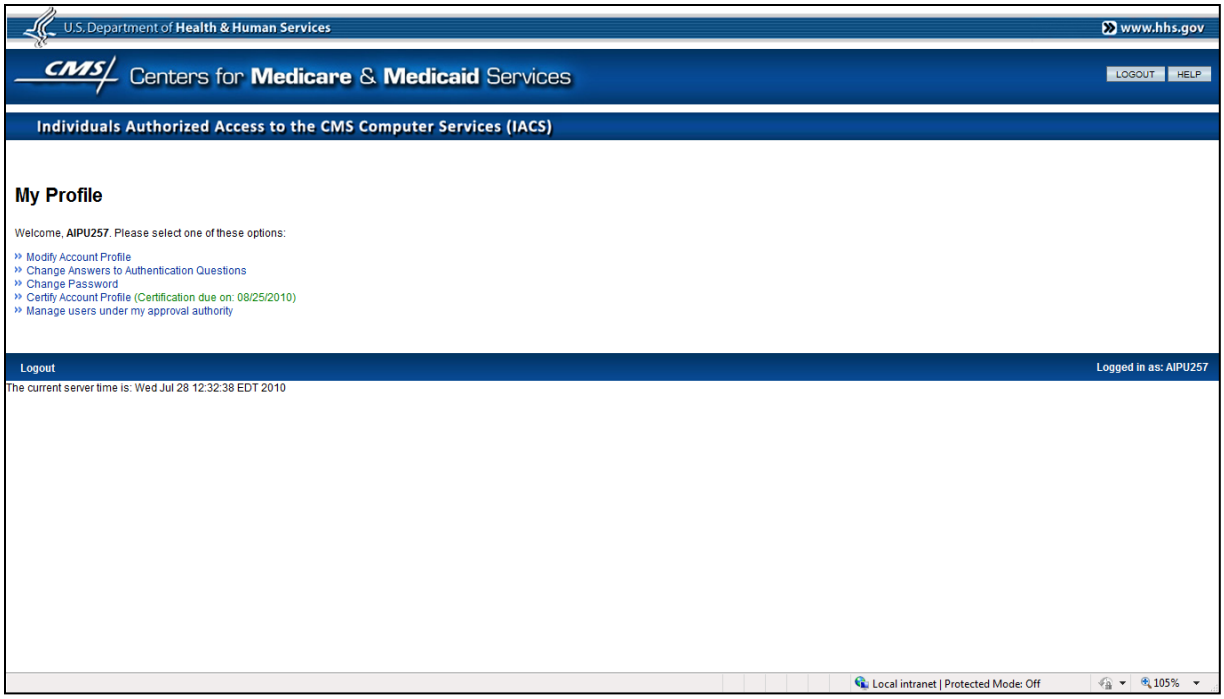

Figure 25: My Profile Screen: Certify Account Profile Hyperlink

When the user selects the Certify Account Profile hyperlink, the **Annual Certification – Step1: Review Account Profile Information** screen will display showing the user profile as illustrated in Figure 26.

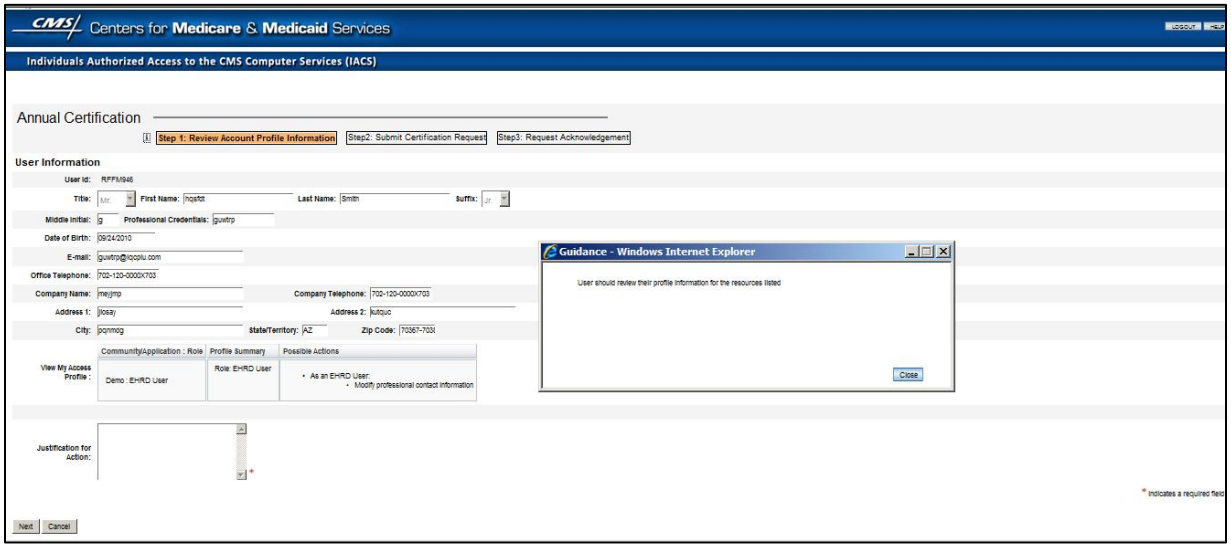

Figure 26: Annual Certification: Review Account Profile Screen

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:

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

- For users with no roles or resources assigned to their account, there is no Approver to whom the system can route the certification request, and such users will not be allowed to submit their certification. These users will be alerted by a message at the top of the page advising them to modify their profile and get a role assigned prior to their certification due date. These users will not be able to select the ***Next*** button to proceed with their certification request; but will have the sole option to select the ***Cancel*** button to cancel the certification process. If no action is taken by their certification due date, then the users' account will be archived.

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 Ack*now*ledgement** screen.

The **Annual Certi*fi*cation - Step 3: Certification Request Acknowledgement** screen indicates that the certification request has been successfully submitted and provides a request number to use for tracking the certification request.

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 describe 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, that will be treated the same as a rejected request and the user's account will be archived.

8.3 Archiving Accounts

Archiving is the process of removing a user's account information from the IACS system. A user's IACS account will be archived for failing Annual Certification. If the user attempts to login to IACS after his account has been archived, a message will appear on screen that his account cannot be found. If the user is not re-certified for any role or system resource by their Annual Certification due date, then the user's account will be archived.

Note:

- The user's account will only be archived if there are no approved resources assigned to the account. For a user with multiple resources, if even one resource is approved,

rejected resources will be removed from the user's profile, but 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.

9.0 Troubleshooting & Support

9.1 Error Messages

IACS provides a variety of on-screen error messages. These messages are self-explanatory and guide the user in how to remedy the error.

The following Sections illustrate 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.

9.1.1 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 27.

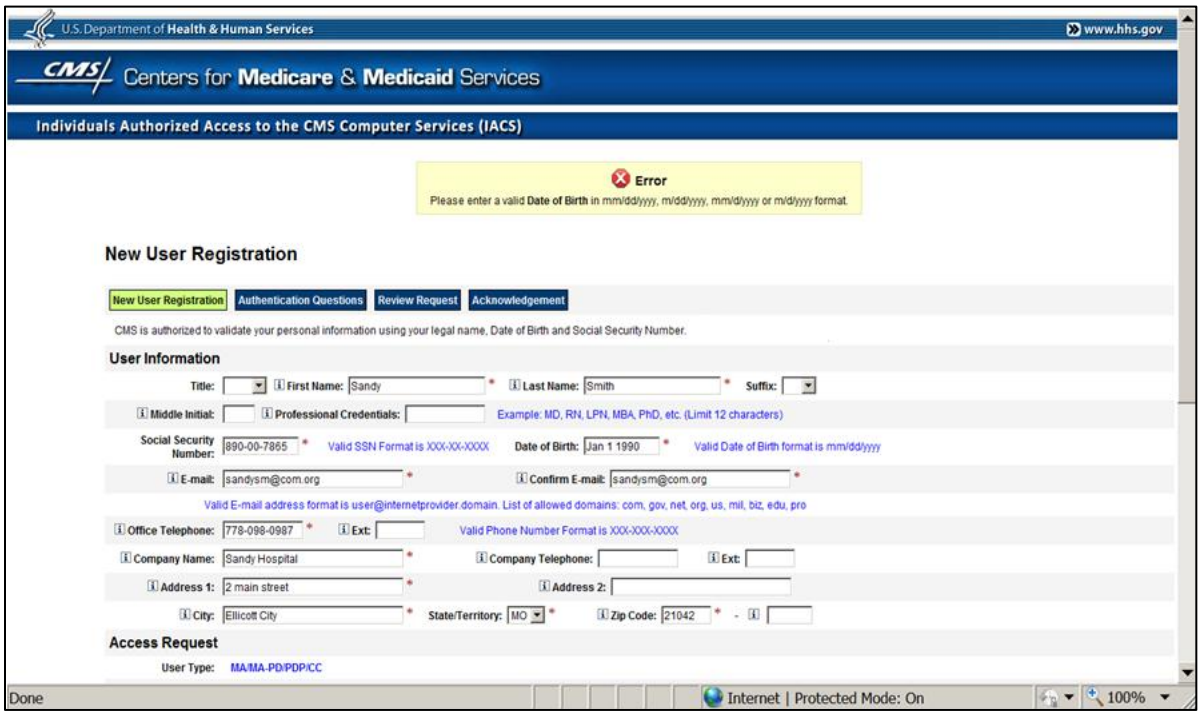

Figure 27: New User Registration Screen: Validation Failure Message

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 user entered data again. 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 successfully validated, the **E-mail Address Verification** screen will display.

9.2 Frequently Asked Questions

1. *I registered and got approved in IACS as a PQRS Submitter for the PQRS/eRx application without associating to an organization. How can I change my role to associate to an organization?*

   You will need to modify your profile to disassociate from your current PQRS Submitter role. After you disassociate from your role you may request the PQRS Submitter role with the option to associate to an organization by selecting the radio button option *"I want to associate to an Organization".*

2. *When I submit a request for the 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). Due to this, IACS will not have a way to route your certification request for approval. Thus your request for certification will be unprocessed. Please contact your IACS Helpdesk for further instructions. Refer to Section 9.3 of this document for the list of Helpdesks and their 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 does not have an Approver, the certification request will remain unprocessed for all the roles.

9.3 Support

There are multiple Helpdesks supporting IACS registrants where users can go to for help with login or other questions.

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

The Helpdesk associated with **CSP-HSTP** is the HSTP Help Desk. The phone number is 1-410-786-1354. They can be contacted at HSTP_Application_Support@cms.hhs.gov.

The Helpdesk associated with **CSP-MCSIS** is the MCSIS Help Desk. The phone number is 1-410-786-6768. They can be contacted at MCSIS_Application_Support@cms.hhs.gov.

The Helpdesk associated with the **DMEPOS Application** is the Competitive Bid Implementation Contractor (CBIC) Helpdesk. The phone number is 1-877-577-5331. They can be contacted at CBIC.admin@palmettogba.com.

The Helpdesk associated with the **PQRS/eRx Application** is the Quality Net Helpdesk. The phone number is 1-866-288-8912. They can be contacted at qnetsupport@sdps.org.

The Helpdesk associated with **HETS UI** is the MCARE Helpdesk. The phone number is 1-866-440-3805. The Fax number is 1-615-238-0822. They can be contacted at mcare@cms.hhs.gov.

The Helpdesk associated with **HPG** is the MCARE Helpdesk. The phone number is 1-866-440-3805. The Fax number is 1-615-238-0822. They can be contacted at mcare@cms.hhs.gov.

The Helpdesk associated with **Medicare Advantage/Prescription Drug Plans** is the MAPD Helpdesk. The phone number is 1-800-927-8069. They can be contacted at mapdhelpdesk@cms.hhs.gov.

The Helpdesk associated with **Medicare Drug Rebate** is the MDR Help Desk. The phone number is 1-800-927-8069. They can be contacted at mapdhelpdesk@cms.hhs.gov.

The Helpdesk associated with **Medicare Exclusion Database** is the MED Help Desk. The phone number is 1-866-484-8049. The TTY/TDD number is 1-866-523-4759. Their E-mail address is EUSSupport@cgi.com. Their hours of operation are Monday-Friday 7am to 7pm Eastern Standard Time, EST.

The Helpdesk associated with the **PS&R/STAR Application** is the External User Services (EUS) Helpdesk. The phone number is 1-866-484-8049. The TTY/TDD number is 1-866-523-4759. Their E-mail address is EUSSupport@cgi.com. Their hours of operation are Monday-Friday 7am to 7pm Eastern Standard Time, EST.

For **Gentran** login issues, IACS Administrators can be contacted at iacs_admin@cms.hhs.gov.

10.0 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 – a program that determines which plan or insurance policy will pay first if two health plans or insurance policies cover the same benefits. COB coordinates the payment process to prevent mistaken payment of Medicare benefits.
DMEPOS	Durable Medical Equipment, Prosthetics, Orthotics & Supplies

Term	Definition
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.
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.
Medicaid	A joint federal and state program that helps with medical costs for some people with low incomes and limited resources. Medicaid programs vary from state to state, but most health care costs are covered for those who qualify for both Medicare and Medicaid.
Medicare	A federal health insurance program enacted in 1965 that is financed by a combination of payroll taxes, premium payments, and general Federal revenues. This program provides health insurance to people age 65 and over, those who have permanent kidney failure requiring dialysis or transplant, and certain individuals under 65 with disabilities.
NPI	National Provider Identifier (NPI) – a unique identification number for use in standard health care transactions. The NPI is issued to health care providers and covered entities that transmit standard HIPAA electronic transactions (e.g. electronic claims and claim status inquiries). The NPI fulfills a requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and was required to be used by health plans and health care clearinghouses in HIPAA standard electronic transactions by May 23, 2007. The NPI contingency period allowed health care providers and covered entities until May 23, 2008 to become fully compliant with the NPI rule.
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.

Term	Definition
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.

11.0 Acronyms

This section defines acronyms used or referenced in this document.

Acronym	Definition
AO	Authorized Official
BAO	Backup Authorized Official
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
CSP	Center for Strategic Planning
CSR	Customer Service Representative
DBidS	Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) Bidding System
DOB	Date of Birth
DMEPOS	Durable Medical Equipment, Prosthetics, Orthotics & Supplies
EHR	Electronic Health Record
EPOC	External Point of Contact, Organizational IACS Approver
ECRS	Electronic Correspondence Referral System (ECRS)
EST	Eastern Standard Time

Acronym	Definition
FI/Carrier/MAC	Fiscal Intermediary/Carrier/Medicare Administration Contract
EUS	External User Services
HETS UI	HIPAA Eligibility Transaction System User Interface
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HPG	HIPAA Eligibility Transaction System Provider Graphical User Interface
HSTP	Health System Tracking Project
IACS	Individuals Authorized Access to the CMS Computer Services
ID	Identification
IT	Information Technology
IUI	Integrated User Interface
IVR	Interactive Voice Response
LSA	Local Service Administrator
MA	Medicare Advantage
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	Medicare 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

Acronym	Definition
POSFE	Point-of-Sale Facilitated Enrollment
PQRI	Physician Quality Reporting Initiative
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