Release Notes for Individuals Authorized Access to the CMS Computer Services (IACS) Release 2011.03

Document Version 1.0

November 2011

Document Number: IACS.REL.2011.03

Contract No.: HHSM-500-2007-00024I

Prepared for:

Centers for Medicare & Medicaid Services (CMS)
OIS/EDG/DMBDD

7500 Security Boulevard, N3-00-01

Baltimore, Maryland 21244-1850

Prepared by:

Quality Software Services, Inc. (QSSI)

10025 Governor Warfield Parkway Set 401

Columbia, Maryland 21044

REVISION HISTORY

Date	Version	Reason for Change	Author
11/01/2011	0.1	Initial Version	QSSI
11/14/2011	1.0	Final Version	QSSI

REVIEW

Dennis Horton, CMS Government Technical Lead	Date
Krishnamoorthi Ganesan, QSSI IACS Program Director	Date
Raghavan Srinivasan , QSSI IACS Project Manager	Date
Bavani Murari, QSSI BA Lead, Author	Date

CONTENTS

TABLES

1. Introduction

The Release Notes for Individuals Authorized Access to the CMS Computer Services (IACS) describes the contents of this Release (including IACS Core and Applications). This document includes the items addressed in the 2011.03 release, such as Change Requests (CRs), Remedy Tickets (RTs).

1.1 Document Layout

The remainder of the document consists of the following sections:

- **Chapter 2.0: Change Requests and Remedy Tickets –** a high level summary of the change requests (CRs) and Remedy Tickets (RTs) addressed in this release of IACS.
- **Chapter 3.0: Enhancements –** a detailed summary of the enhancements (CR) included in this release of IACS.
- **Chapter 4.0: Known Issues –** a summary of the outstanding issues with plan resolution dates
- **Chapter 5.0: Tips, Tricks and Other Advise**
- **Chapter 6.0: Documentation Updates**

2.0 Change Requests and Remedy Tickets

The following sections list the Change Requests (CRs) and Remedy Tickets (RTs) addressed by this Release of IACS.

2.1 Change Requests

Table 1: List of Change Requests

CR Number	Description
IACS-108	**Allowing MARx Monthly Report to Go to Alternate Third Party Users** This CR implements the ability for the Electronic File Transfer (EFT) Group to distinguish users that are permitted to access the financial and non-financial mailboxes. The New User Registration and Modify Profile screens will include the option to select the Report Access Type for financial and non-financial mailboxes or both. Access to the financial and non-financial reports will be available to the following user roles: MA/PDP/NET Submitters, Report View The selection of the Report Access Type check box will be required. The user must select at least one option. The new role, Report View, will be available for users registering for the MA/MA-PD/PDP/CC Application. Following implementation, existing MA/PDP/NET Submitters will have access to both the financial and non-financial reports. Users will be able to modify their report type access using the Modify Report Access Type option as part of profile modification.
IACS-418	**PQRS/eRx Application User Report** This CR allows the PQRI Helpdesk users to request a PQRS User Report that will be sent by E-mail to the requestor. The report will be an MS Excel spreadsheet. The “E-mail User Report” link will be available to the PQRI Helpdesk on the “My Profile” page. The “E-mail User Report” page allows the Helpdesk to generate a report for all users or a subset of users by Role, User Name, TIN/SSN, or Legal Business Name for the PQRS/eRx Application.

CR Number	Description
IACS-429	**HPG Submitter ID field Optional** This CR benefits the HPG New Registration process by allowing the user to register without providing a Submitter ID. IACS will no longer perform the validation against the list of valid Submitter IDs'. As part of the approval process, the MEIC Helpdesk (now known as MCARE Helpdesk) will be responsible for validating the Submitter ID for the user that is requesting the HPG User role. Once registered, the HPG user will not be allowed to modify the Submitter ID. The Submitter ID can be modified only by the IACS Administrator using the IACS Admin Console.
IACS-432	**PS&R/STAR Enhanced Search Capability** This CR enhances the search capabilities for the PS&R/STAR Helpdesk users when searching for New Registration/Account Modification pending approval requests under their scope of responsibility using the Search Request(s) function. The TIN/SSN and Legal Business Name fields will be added to the search criteria and be included in the search results under the Requested Items column.
IACS-434	**Change selected fields of Modify Profile to Non-editable** This CR restricts modification of critical user account information in order to minimize the risk of malicious activity to a user's account. The following fields will be non-editable when using the "Modify User/Contact Information" link: First Name, Last Name, and Date of Birth. Users can submit legitimate service requests through their Helpdesk if they need to change any of the above information. This CR applies only to applications that currently allow the user to modify First Name, Last Name, and Date of Birth: PS&R/STAR, PQRS/eRx, DMEPOS, and applications integrated using Simple Integration framework.
IACS-435	**Extend E-mail Verification** This CR extends the E-mail verification requirement to all applications during New User Registration. The E-mail verification process will also be extended to those applications that allow users to modify their E-mail address using the "Modify User/Contact Information" link.

CR Number	Description
IACS-436	**Helpdesk User Interface Functions** This CR will provide a means for certain Helpdesk users to perform standard help desk functions using the “Manage users under my authority” feature, as an alternate method to using the IACS Adminstration Page. This CR is applicable to the PS&R/STAR application and applications integrated using Simple Integration framework. The “Manage users under my authority” page will include two new search criteria fields, E-mail and User Status, for the Helpdesks of the applications listed above. The User Status criteria includes All, Active, Fully Disabled, Locked and Partially Disabled. Once the search has been executed, the Helpdesk will be able to select a user to perform the following standard Helpdesk functions: View user information, Unlock Account, Reset Password and Disable Account.
IACS-437	**Modify MAMA EPOCs** This CR provides the capability for the MA/MA-PD/PDP/CC Application users to request two roles during New User Registration and to add an additional role during Account Modification. The contracts in the user profile will be common to both roles. The combinations of roles allowed are defined in Section 3.1. This CR also implements archiving procedures for MAMA users that do not have contracts in their profile for 120 days and users that do not have any other IACS roles.
IACS-438	**2nd Phone Field for SI Applications** This CR allows the applications that need to comply with 2-Factor authentication requirements to collect secondary telephone information for users selecting the SMS/Mobile as their preferred 2-Factor authentication notification method. The ‘Secondary Telephone’ field can be defined as either required or optional and should be defined as a database update during Simple Integration Application setup.
IACS-439	**IPCDS get Org SO** The ‘UserAccessInfo’ and the ‘UserOrganizationInfo’ service responses of IPC Data Service will include the IACS Account ID(s) of the Security Official and the Backup Security Official of the user’s associated organization.

CR Number	Description
IACS-443	**Text for Individual Practitioner Role** This CR is applicable to the PQRS/eRx Application and requires that an Individual Practitioner confirm that they understand the definition of the Individual Practitioner role. When a user selects the Individual Practitioner role and selects “Next”, IACS presents the following prompt and by selecting ‘OK” the user will be allowed to continue with the registration process. *“I understand that registration as an eligible Individual Practitioner is only for those who receive their Medicare payment under their Social Security Number”.*
IACS-444	**Modify Pending Approval Screen Flow** This CR assists the Approvers in their approval process by redirecting the Approver back to the ‘Inbox” page after an action has been taken on a request and other approval requests are pending action. Once the “Inbox” is empty, the Approver is redirected to the “My Profile” page.
IACS-445	**Simple Integration Input Field** This CR will provide a multi-text attribute field for the applications integrated using the Simple Integration framework. IACS will accept comma separated and line separated formats in the multi-text field. The multi-text field will be defined as part of the Simple Integration Application setup process.

2.2 Remedy Tickets

Table 2: List of Remedy Tickets

Remedy Ticket #	Description
RT-1604579	**E-mail notification to Gentran does not include the mailbox names when the MED Application is added using the 'Add Application' feature by an existing IACS User** Changes will be made to ensure that the E-mail notification to Gentran contains the mailbox names when an existing IACS user modifies his profile and adds the MED Application using the "Add Application" function.
RT-1636058	**User Status should be included in the output of the stored procedure for SI Applications** Changes will be made to the stored procedure invoked by the applications integrated using the Simple Integration framework (SP_SI_GetUserInfo) to include the "User Status" field in the output.
RT-1636067	**PQRS Submitter or Representative should be able to add an additional role within the associated organization or with other organizations or outside of the organization and vice versa.** Changes will be made to permit the PQRS Submitter or PQRS Representative to add an additional role as defined below: Users with the PQRS Representative and/or PQRS Submitter roles not associated with an organization will be able to request the same role by associating with an organization and vice versa. For users with the PQRS Representative and PQRS Submitter roles requesting an EHR Submitter role, the Organization drop-down will be displayed allowing the user to associate to an organization as part of the EHR Submitter role request.
RT-1636088	**Certification request for the MAPD Help Desk Admin and MAPD Help Desk roles should be routed to the appropriate Authorizer** Changes will be made to the system to ensure that certification requests for the MAPD Help Desk role and the MAPD Help Desk Admin role are properly routed to the IUI Authorizer.
RT - 1636099	**The administrative capability associated with the role should be removed from the user account after a user disassociates from the role especially for the Helpdesk role.** The administrative capability associated with the MAPD Helpdesk and MAPD Helpdesk Admin roles will be removed after the user disassociates from the role. When the user logs back into IACS, the link to the "IACS Administration" page will not be displayed on the "My Profile" page, therefore restricting users from accessing the IACS Administration Console.

Remedy Ticket #	Description
RT-1636115	**Approvers/Helpdesks of Applications within the Simple Integration framework not being able to search pending request by Role.** Following the implementation of this remedy, Helpdesk users of the applications integrated using the Simple Integration framework will be able to search pending requests by Role. If there are multiple roles to approve, the user will have a drop-down to search the requests for a specific role.
RT-1636126	**Option "All" should be displayed along with the list of available roles in the Role drop-down menu when the approver of the SI application attempts to search pending registration/modification/certification requests.** Following the implementation of this remedy, Helpdesk users of the applications integrated using the Simple Integration framework will be able to search pending requests by Role. The "All' role option will display along with the list of available roles in the Role drop-down menu.
RT-1636139	**The E-mail notification for the user's pending request from the Top-Of-the-Chain role of the SI application should be sent to the Business Owners of the same Simple Integrated application.** Changes will be made to the system to ensure that any profile modification request of the Top-of-the-Chain role of the applications integrated using the Simple Integration framework is sent to the IACS Administrator along with an E-mail notification to the Business Owner of the application.
RT-1636146	**IACS incorrectly allows a user to submit a second request if a pending registration or modification request exists for the same application**. The system will not allow a user to submit a second registration or modification request when a pending request exists for the same application and the same organization. This applies for both PQRS/eRx and PS&R/STAR Applications. IACS will notify the user with the following message. *"A request for the selected organization is pending approval. You may not request an additional role within the same organization until the pending request has been approved."*
RT-1636164	**PQRS Submitter with or without an organization should be able to modify their Preferred 2-Factor notification method only using the "Modify Account Profile" link. This issue is also applicable to applications integrated with the Simple Integration framework.** PQRS Submitter 2-Factor roles with or without an organization and Simple Integration framework 2-Factor roles are now able to modify the Preferred 2-Factor notification method using the "Modify Account Profile" link.

Remedy Ticket #	Description
RT-1636175	**The CUA table should be cleaned up so that the users from Archived Organization are removed.** Users associated with Archived Organizations will be deleted from the CUA table.
RT-1638136	**An application Helpdesk user in the Admin Console should be able to view all their application users even if the user has multiple roles and registered for a role in another application.** This remedy ticket will allow the Helpdesks to view the users who belong to their application from the IACS Admin Console regardless of their associated IDM Organization.
RT-1664327	**Update the Inactivity task to look for the Last Login Date** The Inactivity task will use the 'Last Login Date' to determine the start date when calculating the inactivity of a user. Previously the Inactivity task was using the 'Password Expiry' date.

3.0 Enhancements

The following section provides details on the Change Requests and Remedy Tickets with the associated User Interface enhancements that are included in this release of IACS. Note that ***this section may not provide details on all changes***. For more details, refer to the Preliminary Design Review (PDR) document. The purpose of this section is to provide details on ***specific user interface changes that require further explanation***. Please see the table in Section 2.0 for a complete list of changes in this release.

3.1 IACS-108 Allowing MARx Monthly Report to Go to Alternate Third Party Users

The purpose of Change Request IACS-108 is to provide a means to limit access to certain types of monthly MARx reports as needed within the MA/MA-PD/PDP/CC Application. This change request provides the Electronic File Transfer (EFT) group a means to distinguish users that will be permitted access to financial and non-financial mailboxes. The Report View will be a new role added to the MA/MA-PD/PDP/CC Application as part of this CR and will be available in the Role drop-down for new users and existing users. The following roles will have access to the financial, non-financial mailboxes or both once the corresponding approvers approve the registration request:

- MA Submitter
- PDP Submitter
- Net Submitter
- Report View

Changes for existing users with the Submitter roles, New User Registration, and Modify Account Profile pages are as follows:

<u>Report View – New Role</u>

Users requesting the new Report View role will be allowed to enter both Medicare Advantage (Contracts starting with ‘H’) and Drug contracts (Contracts starting with ‘E’, ‘S’, and ‘9’).

Once approved, Report View users will not be provisioned to the IUI resource.

<u>Default Report Type for Existing Users</u>

As part of implementation, IACS will default the existing users with Submitter roles to have access to both financial and non-financial mailboxes. It is the MA/MA-PD/PDP/CC Application’s responsibility to ensure that users who do not need access to a particular report modify their profile accordingly.

<u>New Registration Change</u>

The “New User Registration” page, ‘Access Request’ section has been modified to provide the option to select the report access type. Based on the role selection as mentioned above, the Access Request section will display two ‘Report Access Type’ check boxes, one for financial and the other for non-financial reports:

- Access to Financial Report
- Access to Non-Financial Report

The ‘Report Access Type’ check box is a required field. The user must select at least one Report Access Type. If the user requires access to both financial and non-financial reports, then the user should select both check boxes.

<u>Modification Changes:</u>

The “Modify Account Profile” page has been modified to provide the capability to change the user’s current selection of report access type. To modify the report access type, the existing MAMA user will select the ‘Modify Report Access Type’ option from the ‘Select Modify Action’ drop-down list. The user must select at least one Report Access Type. If the user requires access to both financial and non-financial reports, then the user should select both check boxes.

The user will not be allowed to remove access to the Gentran mailboxes as part of modification. The user can only change the access from one type to another or add another report to access. Approval is not required when a user unchecks the access to a report. Approval is required whenever a user requires a new mailbox to access for a specific report. The modification request will be routed to all corresponding approvers associated with the contracts in the user's profile. The report access type applies to all the roles and contracts in the user's profile, once approved.

Approval

The "Approve / Reject Approval -Requesting Access" page has been modified to display the Report Access Type. The Approver needs to review the information as it relates to the Report Access Type, roles and contracts (refer to IACS 437).

If the 'Report Access Type' request is for a user who has two roles then the Approver's action to approve the contract(s) applies to both MAMA roles in the user's profile. Refer to IACS-437 for more details.

E-Mail Notification

The E-Mail Notification to Gentran following the user registration or profile modification will now include the Report Access Type information indicating the user's access to Financial, Non-Financial mailboxes or both.

All corresponding approvers will be notified if one of the approvers rejects the 'Modify Report Access Type' profile modification request. The E-mail notifies the Approvers that the modification request to the account profile will not be made and that the pending approval request for this modification has been removed from their pending approval queue.

3.2 IACS-418 PQRS/eRx Application User Report

This CR enables the PQRI Helpdesk to request a report of PQRS/eRx Application users that will be sent to the requestor's E-mail as a Microsoft Excel spreadsheet attachment. The report name will be PQRS_User_Report_<report run date>.

The PQRI Helpdesk user will be able to request the report by selecting the new hyperlink "E-mail User Report" on the "My Profile" page. The "E-mail User Report" page permits the PQRI Helpdesk user to generate a report of all users or a group of users. The PQRI Helpdesk can select from the following search criteria as needed:

- First Name
- Last Name
- Role
- TIN/SSN
- Legal Business Name

The Role drop-down list will allow the Helpdesk to select a specific PQRS/eRx role or the 'All Roles' option. Selecting the 'All Roles' option will generate a report for all the PQRS/eRx Application users.

The PQRS_User_Report includes the search criteria selected to generate the report and the following user information:

- IACS ID
- First Name
- Last Name
- Role
- Organization ID
- Organization Name
- Organization Tin (****Last 5 Digits)
- User Status (Active, Partially Disabled, Disabled)
- Last Password Change Date
- Create Date
- Last Certification Date

Status Definitions:

Disabled:

A user status of 'Disabled' denotes that the user has been manually disabled by the Helpdesk or by an IACS Administrator for security reasons. The disabled user is removed from all resources. A disabled user will not be able to log into any of the IACS administered applications, or use IACS self-service features to reset the password or retrieve his IACS User ID. Only an IACS Administrator can enable a 'Disabled' user.

Partially Disabled:

A user status is shown as 'Partially Disabled' when the user has not logged into the system for more than 180 days. A 'Partially Disabled' user cannot log into any application that he could previously access. A 'Partially Disabled' user can enable himself using the IACS self-service function or by contacting the Helpdesk.

Last Password Change:

The report will display the date the user last changed his password. The Last Password Change date will be blank for the following scenarios:

1. When a user has received the first time password and has not changed his password.
2. When a user has requested a password reset within the first 60 days of his registration and he has not logged in with the temporary password.

Last Certification Date:

The Last Certification Date will be blank for new users that have not gone through the Annual Certification process.

Note: The PQRS User Report will not show the user's User Status, Last Password Change Date, Create Date, and Last Certification date if the user exists only in the IPC database and not in IACS (no entry for the user in IDM or LDAP).

3.3 IACS-429 HPG Submitter ID Field Optional

This CR accommodates the HPG Application during the New User Registration process by allowing the user to register without entering the ‘Submitter ID’ field. At the time of registration, the ‘Submitter ID’ may not have been assigned; therefore, the Submitter ID field has been made optional.

Prior to this release, the user’s entry of the Submitter ID was validated against the list of valid Submitter IDs’. With this release, IACS will no longer perform the validation against the list of valid Submitter IDs’. The Submitter ID will be validated for format only. If the user enters a Submitter ID, IACS will validate that the Submitter ID is entered as alphanumeric and the length is eight (8) characters.

As part of the approval process, the MCARE Helpdesk will be responsible for validating the Submitter ID, for the user that is applying for the HPG User role.

HPG users will not be able to modify their account profile to change the Submitter ID. A Service Request must be submitted to the IACS Administrator. The MCARE Helpdesk will open an IACS Service Request requesting the IACS Administrators to modify the HPG user’s Submitter ID.

The Submitter ID can be removed by the MCARE Helpdesk by using the “Manage users under my authority” function. This existing function has not changed due to this CR.

The E-mail notification for Gentran access will not be generated if the Submitter ID was not entered as part of registration. Only non P-Type Submitters will have access to Gentran mailboxes. The Gentran E-mail notification will be generated once the Submitter ID is updated by the IACS Administrator or removed by the MCARE Helpdesk using the “Manage users under my authority” function.

3.4 IACS-432 PS&R/STAR Enhanced Search Capability

This CR enhances the Search Request(s) function for the PS&R/STAR Helpdesk users. The search for New User Registration/Account Modification pending approval requests under their scope of responsibility will include the TIN/SSN and Legal Business Name fields. The EUS Helpdesk currently supports PS&R, STAR, and MED Applications. This CR will only affect the PS&R/STAR Application since the MED Application does not have Legal Business Name or TIN in their structure. The searchable fields will include:

- First Name
- Last Name
- Request Number
- Request Expiration Date
- Role
- TIN/SSN
- Legal Business Name

The Legal Business Name and TIN/SSN will display in the 'Requested Items' column of the search results. The TIN/SSN will be masked when requesting the search and in the results section. Only the last five (5) digits of the TIN/SSN will display in the search results.

Pending approval requests that are in the PS&R/STAR Helpdesk queue prior to the 2011.3 implementation will not have the TIN/SSN and Legal Business Name information included in the pending request. In order to return results for pending approval requests dated before this release, the TIN/SSN, or Legal Business Name search attribute should not be used as the search criteria.

Pending certification requests and E-mail modification requests are not searchable using the TIN/SSN and Legal Business Name since a Security Official could be associated with multiple organizations.

3.5 IACS-434 Change Selected Fields of Modify Profile to Non-Editable

With the implementation of this CR, specific fields that may pose a security risk can no longer be modified by using the **"**Modify User/Contact Information" link on the "My Profile page. The following fields will be made non-editable:

- First Name
- Last Name
- Date of Birth

This CR only applies to the following applications that currently allow the users to modify their First, Last Name and Date of Birth fields:

- CSP-HSTP
- CSP-MCSIS
- DMEPOS
- ECRS
- GENTRAN
- MDR
- MED
- PQRS/eRx
- PS&R/STAR

For legitimate changes to the fields mentioned above, users will have to contact their Application Helpdesk who in turn should submit a Service Request to the IACS Administrator to make the change.

For those applications, that allow users to modify their E-mail address and other fields (excluding First Name, Last Name, and Date of Birth), the "Modify User/Contact Information" page will be used. The following applications will not be impacted, since the users have never had the ability to modify the First Name, Last Name, or Date of Birth:

- COB
- CSR
- Demonstration Community (EHRDS)
- HETS UI
- HPG
- MA/MA-PD/PDP/CC

3.6 IACS-435 Extend E-Mail Verification

This CR extends the E-mail verification process to all applications during New Registration. E-mail verification will be extended to those applications that allow users to modify their E-mail address using the “Modify User/Contact Information” link. Post implementation, the following applications will begin to undergo E-mail verification during New User Registration:

- COB
- CSR
- HPG
- HETS UI
- MAMA-PD/PDP/CC

E-mail Verification Stage

The E-mail verification will be initiated after the user’s registration information is entered and the ‘Next’ button is selected on the “New User Registration” page.

An E-mail containing a verification code will be sent to the user with the Subject: IACS: E-mail Address Verification. The verification code should be entered on the “E-mail Address Verification” Page within 30 minutes. The user can request to resend the Verification Code up to three times. The registration or modification process continues only when the E-mail verification was successful.

The following PQRS 2-Factor authentication roles can modify their E-mail address using Modify Account Profile, if their Preferred 2nd Factor authentication notification method is set to E-mail, in which case the E-mail verification will be initiated.

- EHR Submitter
- Individual Practitioner (EHR Submitter)
- PQRS Submitter

3.7 IACS-436 Helpdesk User Interface Functions

This CR will provide a means for certain Helpdesk users to perform standard help desk functions using the “Manage users under my authority” feature, as an alternate method to using the ‘IACS Administration Page’. In the future, the access to the IACS Administration page will be limited to IACS Administrators.

Post implementation of this CR, Helpdesks of applications listed below will have access to both the “IACS Administration Page” and the “Manage users under my authority” hyperlinks. The Helpdesk users of the applications listed below should use the “Manage users under my authority” feature to perform the standard help desk functions.

- CSP-HSTP
- CSP-MCSIS
- ECRS
- GENTRAN
- MDR State Exclusion
- Medicare Exclusion Database (MED)
- PS&R/STAR
- Any future applications that will be integrated using the Simple Integration framework

In IACS, Helpdesks can search and view the users under their scope of responsibility, using the “Manage users under my authority” function. Helpdesk users of applications as listed above can also perform the following help desk functions from the “Manage users under my authority” page**:**

- Search/View User Accounts
- Disable User Account
- Reset User Password
- Unlock User Account

The descriptions below describe the Helpdesk features using “Manage users under my authority”:

<u>Searching and Selecting a User</u>

The Helpdesk users of the applications listed above will notice a change to the “Manage users under my authority” page search criteria which will include the ‘E-mail’ and ‘User Status’ fields as additional filters. The ‘E-mail’ is a free form text field, which allows the Helpdesk user to enter a partial E-mail address to execute the search. The ‘User Status’ is a drop-down list which includes the following options that can be selected by the Helpdesk.

<u>User Status’ Selections</u>

- All (default option)
- Active
- Fully Disabled
- Locked
- Partially Disabled

<u>Status Definitions and Status Result Values:</u>

Active: A user with an Active status can log in to IACS administered applications for which he has access. The search returns all active users and includes users who are Active and Locked. The results in the Status column will display as:

- Active
- Active, Locked

Fully Disabled: A user with a Fully Disabled status has been manually disabled by the IACS Administrator and/or Helpdesks due to security risks. The disabled user will be removed from all resources. A disabled user will not be able to log into the IACS administered applications for which he could previously access, or use IACS self-service features to enable himself. Only IACS Administrators can enable a user who is fully disabled. The search returns all Fully Disabled users and includes users who are Fully Disabled and Locked. The results in the Status column will display as:

- Fully Disabled
- Fully Disabled, Locked

Partially Disabled: A user with a Partially Disabled status has been inactive for 180 days or more. The user is only disabled in LDAP. The user will be unable to access the IACS administrated applications for which he could previously access. A Partially Disabled user can enable himself by logging into IACS and answering the security and authentication questions. The search results returns all Partially Disabled users and includes users who are Partially Disabled and Locked. The results in the Status column will display as:

- Partially Disabled
- Partially Disabled, Locked

Locked: The user account has been locked due to three (3) failed login attempts. The results in the Status column will display as:

- Active, Locked
- Partially Disabled, Locked
- Fully Disabled, Locked

<u>Search Results:</u>

The Search results will be displayed in a table below the Search Criteria. The “Select” column will have a radio button to select the user. Once the radio button is selected, the Helpdesk function buttons will be enabled based on the user’s status and the possible actions allowed. After selecting a user, the View button is always enabled.

Note: Helpdesk Function buttons will not be applicable to Archived users. A Fully Disabled account will only be viewable.

<u>Helpdesk Function Buttons:</u>

- View
- Fully Disable
- Unlock
- Reset Password

Helpdesk Function: View

The View option allows the Helpdesk user to ascertain information about the user. The information will be displayed in the following tabs:

- Identity – User Account Information, 2 Factor Information and Resource Information
- Professional Contact – Professional credential and contact information
- Certification – Certification Dates and Status
- Other Info – Application specific information, if applicable.

Tab: Identity

Account Information

- User ID
- First Name
- Middle Name
- Last Name
- Title
- Role(s) - Display Name of all assigned Roles
- Email Address
- User Status
- Disabled Reason
- Password Expiration Date (Format: MM/DD/YYYY)
- RACF ID (if applicable)

2-Factor Information

- 2 Factor Authentication (if applicable)
- Preferred 2 Factor Notification Method (if applicable)

Resource Information

- Resource Name
- Disabled

Tab: Professional Contact

- User ID
- Professional Credential
- Office Telephone – Extension
- Company Name
- Company Telephone – Extension
- Company Address Line 1
- Company Address Line 2
- Company City
- Company State
- Company Zip – Zip 4

Tab: Certification

- User ID
- Certification Due Date
- Revocation Date
- Certification Status (Display certification flag followed by description)
    - V = User is Revoked
    - I = Initiated for certification but request has not been submitted
    - S = Submitted certification request, waiting for approval

- o R = Certification request rejected
- o N = Not in certification timeline

Tab: Other Info (if applicable)

- User ID
- For PS&R Helpdesk users, the following organization information will be displayed in a tabular format as applicable, depending on the user's association with the organization (Provider or FI/Carrier/MAC). If a user is associated with more than one organization, then the information about each organization will be displayed in a separate row in the table. For PS&R System Maintainers, no organization information will be displayed, as they are not associated with an organization.
  - o Organization Name
  - o Role(s)
  - o Organization TIN (Last 5 digits in the format of ****XXXXX)
  - o CMS Certification Number (if applicable)
  - o Medicare Contractor ID (if applicable)
- For Helpdesk users of applications integrated using the Simple Integration framework the attribute information will be displayed:

<u>HelpDesk Functions: Fully Disable, Reset Password, Unlock Account</u>

Fully Disable: The Fully Disable button will be enabled for either, Partially Disabled, Active or Locked users. If the user has a role(s) in other applications, the Helpdesk will receive a pop-up message informing him that the user account will be disabled for all applications and/or resources associated with the user's account. If the Helpdesk proceeds with the action then the Helpdesk will receive an acknowledgement upon a successful execution of the Fully Disable action. An E-mail will be sent to the other Application Helpdesks notifying them that the account has been disabled.

If there are no additional roles for the user account then IACS will disable the user's account but will not send out an E-mail to the other Helpdesks.

Unlock Account: A user of an application is locked after three failed login attempts. The "Unlock" button will be enabled for Locked, Active and Partially Disabled accounts. If the Helpdesk proceeds with the action then the Helpdesk will receive an acknowledgement upon a successful execution of the Unlock Password function. The user will be able to login with his current password.

Reset Password: The "Reset Password" button will be enabled for Active, Active Locked, Partially Disabled, and Partially Disabled Locked accounts. If the Helpdesk proceeds with the action then the Helpdesk will receive an acknowledgement upon a successful execution of the Reset function. The user will receive an E-mail with a random generated one-time password.

<u>Audit Helpdesk Function:</u>

IACS will audit the IACS Helpdesk functions for Reset Password, Unlock, and Disable accounts.

<u>Limitation of the Search Results</u>

"Manage users under my authority" function has a limitation in the number of records that could be displayed as search results. If the given search criteria for the search qualifies for 1000 records or more, then the search results are not displayed; rather, a warning message stating that the search qualified for more than the allowable limit will be displayed. The Helpdesk should narrow the search criteria and execute the search again.

3.8 *IACS-437 Modify MAMA EPOCs*

Change Request IACS-437 allows specific roles in the MA/MA-PD/PDP/CC application to request two (2) roles during New User Registration and to add an additional role during Account Modification. The role combinations are shown in Table 3.

A configuration object will control the feature for the MA/MA-PD/PDP/CC Application users to have two MAMA roles in their profile. A Service Request to the IACS Administrator will need to be created in order to turn off the application's ability to allow the user to have two MAMA roles.

Role Combinations

Roles	Additional Role Options
MCO Representative UI Update	MA Submitter (or) PDP Submitter
MA Submitter	MCO Representative UI Update
PDP Submitter	MCO Representative UI Update
Report View	MA Representative (or) PDP Representative
MA Representative	Report View
PDP Representative	Report View

Table 3: MA/MA-PD/PDP/CC Additional Role Combinations

New Registration

The "New User Registration" page Access Request section has been modified to allow a registrant for the MA/MA-PD/PDP/CC to select an additional role. The list in the Additional Role drop-down will be based on the first role selected. With this change, a user will be able to select two MAMA roles at the same time during New User Registration. This feature is also available for an existing IACS user who requests for an MAMA Application role.

Example: During New Registration, the user selects the MCO Representative UI Update role. The page refreshes and the 'Additional Role' drop-down displays. The drop-down list allows the user to select either the MA Submitter or the PDP Submitter role.

When a user selects the MA State/Territory Role, which is not listed in Table 3, the option to add another role is not presented.

Requests for any Submitter role type and the Report View role will also require the user to choose the Report Access Type to indicate the user's choice to Financial, Non-Financial mailboxes or both. (Refer to IACS -108).

Modification Changes

The “Modify Account Profile” page has been modified to provide the capability to add a new role using the ‘Add Role’ option from the “Select Modify Action” drop down on the “Modify Account Profile” page.

The ‘Add Role’ option allows the MAMA user to select another MAMA Role as defined in Table 3. The user will be presented with the available role(s) and depending on the role selected will be required to choose the Report Access Type.

Disassociate from the User’s Role

With the ability of a user having two MAMA roles in his profile, the user will be able to disassociate from each of these roles using the ‘Disassociate from <role name> role’ option from the “Select Modify Action” on the “Modify Account Profile” page. For those users that have two roles in their profile, the contracts will be removed from the user’s profile, only when he disassociates from both roles.

Approval

The Approver will take an action (Approve, Reject, or Defer) on the contract(s) requested. The contracts will apply to both roles.

New Registration with two roles:
The Approval request will be routed to the corresponding Approver(s) or EPOC(s). All Approver(s) or EPOC(s) must approve the user’s contract request in order for the user to acquire two roles. Since the contract applies to both roles, if one of the contracts is unapproved, then the user will only acquire the role that is associated with the approved contract(s).

Modify Profile- Add Role
The pending modify request for the additional role will be routed to the corresponding Approver(s) or EPOC(s). All Approver(s) or EPOC(s) must approve the contracts in the user’s profile and any additional contracts the user had requested as part of the role request in order for the user to acquire the additional role. Since the contracts apply to both roles, when an Approver or EPOC rejects any one of the contracts associated with the request, the new role will not be added to the user’s profile. The user will retain the existing contracts and role.

E-mail notifications will be sent to all corresponding Approvers when one of the Approvers rejects the individual contracts request from a user under his authority. The notification informs the Approvers that another Approver has rejected the contract and any pending modify approval request associated with this request will be removed from their pending approval queue. No further action is required. The requestor will be notified that the request was rejected with the justification remarks from the Approver. If an Approver defers one of the contracts, while rejecting the other, the request will be rejected and will be removed from the Approvers’ queue.

MCO Representative UI Update role and IUI Provisioning
Users with the MCO Representative UI Update role are no longer needed to be provisioned to the IUI Resource. Post implementation, when a user with the MCO Representative UI Update role modifies his profile using the “Modify Account Profile” hyperlink and the request is approved by the corresponding Approver(s), along with the profile modification that was requested by the user, IACS will remove the user from the IUI resource.

Archive Accounts

This CR implements archival of users for the following MA/MA-PD/PDP/CC Application roles that do not have contracts in their profile for 120 days or more and the user does not have any other IACS roles. If the user has other application roles in IACS, then the user will not be archived but his MAMA Application role(s) will be removed.

- MA Submitter
- PDP Submitter
- MA Representative
- PDP Representative
- Approver
- POSFE Contractor
- NET Submitter
- NET Representative
- Report View
- MCO Representative UI Update

The MAPD Helpdesk will be able to use the “Manage users under my authority” feature to search for the ‘Archived’ user. The Archival Justification reason will display, as ‘User had no contracts for 120 days’.

Once archived, the user will not be able to access IACS or IACS administered applications and he will be required to go through the New User Registration process to establish a new account.

3.9 IACS-438 2nd Phone Field for SI Applications

This CR allows applications integrated with the Simple Integration framework to collect secondary mobile phone information for the applications that need to comply with 2-Factor authentication requirements. The option of collecting the Secondary Mobile Phone information will be requested by the Appplication and should be included on the Application setup form. The implementation of the Secondary Mobile Phone field will require a database update as part of application setup. The 'Secondary Mobile Telephone' field can be setup to be required or optional depending on the application's business needs. This field will be displayed on the registration pages only when SMS/Mobile (Text message) is selected as the Preferred 2nd factor Notification method.

When the 'Secondary MobileTelephone' field is defined for the application, the user will be presented with the 'Secondary Mobile Telephone' textbox after the Preferred 2nd Factor Notifcation method is selected as SMS/Mobile (Text message). This will display on the "New User Registration" and "Modify Account Profile" pages. If the 'Secondary Mobile Telephone' is defined as required, then the user must provide a secondary mobile telephone number to complete the registration or modification.The Mobile Telephone field has been renamed to 'Primary Mobile Telephone' and the new field is named 'Secondary Mobile Telephone'.

3.10 IACS-439 IPCDS get Org SO

This CR will allow the PQRS/eRx Application to receive the IACS Account IDs of the Security Official and Backup Security Official(s) (if any) of the Organization that the user belongs to via the IPC Data Service.

The ‘User Access Info’ and the ‘UserOrganizationinfo’ responses of the IPC data service will be modified to include the SO and the BSO IACS Account IDs to which the user is associated. If the organization has more than one Backup Security Official, then the BSO IACS IDs will be included in a comma-separated format.

The Outbound XML of the ‘UserAccessInfo’ and ‘UserOrganizationalInfo’ will include the following information:

- IACS ID
- Last Name
- First Name
- MI
- Email
- User Phone
- Corp Phone
- Address Line 1
- Address Line 2
- City
- State Cd
- Zip
- User Country
- Status Flag
- SSN
- Group ID
- TIN
- SO IACS ID
- BSO IACS ID
- Group Name
- Group Type
- Oscar Number
- Contractor Number
- Group Address Line 1
- Group Address Line 2
- City
- State Cd
- Zip
- Group Country
- Group Size
- Parent Group ID
- Group ID
- Community Name
- Application Name

- Role Name
- Role Description

3.11 IACS-443 Text for Individual Practitioner Role

This CR is applicable to the PQRS/eRx Application and requires that an Individual Practitioner confirm that they understand the definition of the Individual Practitioner role.

When a user selects the Individual Practitioner Role, IACS presents the following prompt before continuing to the next stage of the registration or modification process:

"I understand that registration as an eligible Individual Practitioner is only for those who receive their Medicare payment under their Social Security Number".

The registrant will read and will be required to confirm that he is an eligibile Individual Practictioner, as defined in the message, in order to continue with the registration or modification process.

3.12 IACS-444 Modify Pending Approval Screen Flow

This CR assists the Approvers during the approval process by navigating the user back to the “Inbox“ page, “My Profile” page or the search page based on the number of requests in the Approver’s queue after an action has been taken.

After the Approver has taken an action on a request, IACS will determine if there are additional pending requests that are awaiting action in his queue.

Approver’s Inbox is empty:

- The Approver will be returned to the “My Profile” page when all pending requests in his queue have been completed.

Approver has pending requests:

When there are additional pending requests awaiting his action, IACS will return the Approver to the page in which the user selected the request.

- When the pending request was selected from a “Search Criteria for Pending Request(s)” page, then he will return to the same search page.

- When the pending request was selected from the “Inbox” page, then he will return to the Inbox page.

This applies to New Registration, Modification, and Certification approvals for all applications*.*

3.13 IACS-445 Simple Integration Input Field

This CR provides a means for applications integrated with the Simple Integration framework, to setup a new attribute field that will accept multi-text input. A Service Request will need to be created to update the database to define the field as either comma delimited or line delimited.

A comma delimited input field allows the user to input multiple attributes as one line separated by commas.

A line delimited input field allows the user to input multiple attributes separately, the user must use the enter key after each attribute.

4.0 Known Issues

The following known issues exist with the implementation of IACS Release 2011.03 and will be corrected in a future release.

Table 4: List of Known Issues

Item Number	Business / Application Area	Description	Release Issue Discovered	Fix CR/ Remedy#	Release in which Fix will be Applied
1	CR-436: Helpdesk User Interface Functions	The Helpdesks of the applications which have been integrated using the Simple Integration framework, will not be able to perform a partial search on the application specific search fields (For example, Organization Name) using the “Manage users under my authority” function. The complete information should be provided to execute the search. This issue will be fixed in a future release. Impact: None. Currently there are no applications integrated through SI that have the Organization structure. Workaround: Helpdesk should do a full-string search for the application specific search attributes.	2011.03	TBD	2012.01
2	CR-436: Helpdesk User Interface Functions	For applications integrated using the Simple Integration framework that consists of PII data as part of application specific attributes, this information will not be masked in the search criteria or search results when using the “Manage users under my authority” function. For example, if an application integrated with the Simple Integration framework has Organization as	2011.03	TBD	2012.01

Item Number	Business / Application Area	Description	Release Issue Discovered	Fix CR/ Remedy#	Release in which Fix will be Applied
		part of the application specific information, the TIN that identifies the organization will not be masked. This will be fixed in a future release. Impact: None. Currently, there are no applications integrated using the Simple Integration framework that consists of secure data as part of their application specific details. Workaround: None.			
3	CR-437: Modify MAMA EPOC	User with multiple roles disassociates from one role, which may cause the user to have access to contracts that are not applicable to the remaining role. A PDP Submitter user can associate to only Drug contracts (contracts that start with ‘S’, ‘E’ & ‘9’), but a user with both MCO Representative UI Update role and PDP Submitter role can acquire Medicare Advantage (MA) contracts(contracts that start with ‘H’) and Drug contracts. If the same user disassociates from the MCO Representative UI Update role, it will leave the PDP Submitter with access to MA contracts and Drug contracts. A standalone PDP Submitter user is not supposed to have access to Drug contracts. This issue will be fixed in a future release. This situation will apply to the Report View and PDP Representative role combination also. Impact: User may have access to contracts that are not applicable to the role.	2011.03	TBD	2012.01

Item Number	Business / Application Area	Description	Release Issue Discovered	Fix CR/ Remedy#	Release in which Fix will be Applied
		Workaround: EPOC should remove the user's contracts using the "Manage users under my authority" – Edit function. A user could remove the contracts that he does not need in his profile by using the 'Add/Remove Contracts' option as part of profile modification			
4	CR-438: Secondary Phone field for SI Applications	When an application integrated using the Simple Integration framework had opted not to use the Secondary Mobile Telephone field for 2-Factor authentication purposes, the field should not display on the Approve/Reject screen for the Approver. In this case, the "Secondary Mobile Telephone" field label is displayed on the Approve/Reject page of the pending request. However, when the user is approved and logs into his profile, no secondary phone label is displayed on his profile page. This issue will be fixed in a future release. Impact: None. There are currently no applications using 2-Factor Authentication within the Simple Integration framework. Workaround: None. This is a display only defect; no data is updated based on this.	2011.03	TBD	2012.01
5	CR-437: Modify MAMA EPOC	MAMA user can get an additional role, associated to contracts that were not explicitly approved for that role. This will occur when a user initiates a new role request followed by a new contract request	2011.03	TBD	2012.01

Item Number	Business / Application Area	Description	Release Issue Discovered	Fix CR/ Remedy#	Release in which Fix will be Applied
		and the contract request gets approved before the role request. Or the user initiates a new contract request followed by a new role request and the role request gets approved before the contract request. In other words, the order of request and approval follows this exact pattern: request 1, request 2, approval of request 2, followed by approval of request 1. When that happens the last approver will not see pending request 2 but it will, nevertheless, be applied to pending request 1 which he is approving. For example: A user with the MA Submitter role submits a modification request to add the MCO Representative UI Update role. While the request is pending, the user submits another request to add a contract to his profile. If the additional contract request was approved first, then, when the other approver attempts to take an action on the additional Update role request, he will, without knowing it, be approving the contract for the new role. The ‘Approve/Reject Request’ page reflects the user’s profile at the time of the request submission and so it does not reflect the additional contract added after the fact. This will be fixed in a future release. Impact: The user could have access to role or contracts, which may not be intended. Workaround: EPOC should remove the user’s contracts using the “Manage users under my			

Item Number	Business / Application Area	Description	Release Issue Discovered	Fix CR/ Remedy#	Release in which Fix will be Applied
		authority" – Edit function			
6	CR 436: Helpdesk User Interface functions	Roles do not refresh on the "Reset Account Password" or "Disable Account" pages after the Helpdesk user role performs multiple searches. The Helpdesk selects a user from the Manage users search results and attempts to Reset Password or Disable the user. From the Reset Account Password" or "Disable Account" pages, the Helpdesk selects the Back button to return to the search results, where they select a different user to perform the Reset Password or Disable function. The Reset Account Password" and/or "Disable Account" pages display the role of the previously selected user rather than the role of the current selected user. IACS properly executes the selected action for the selected user. This will be fixed in a future release. Impact: Will cause confusion unless the Helpdesk user is aware of and recognizes the issue. However, the discrepancy only affects the display of the role information on the Reset and/or Disable Account page. The underlying role information for the user is correct. Workaround: Helpdesk should execute individual searches instead of multiple user searches.	2011.03	TBD	2012.01
7	CR-437 Modify MAMA EPOC	A user's Role could be re-established even though the user disassociates from a role associated with contracts.	2011.03	TBD	2012.01

Item Number	Business / Application Area	Description	Release Issue Discovered	Fix CR/ Remedy#	Release in which Fix will be Applied
		This can occur if the user submits a profile modification request related to the MA Submitter role (like ‘Add Contracts’ or ‘Modify Report Access Type’) and while it is pending approval, the user disassociates from the MA Submitter role. Should the approver approve the pending modification request, the MA Submitter role will be added back to the user’s profile. It is important to note that the role is added back to IDM and not to the Enterprise Directory Server; consequently, the user will not gain additional privileges. This situation could apply to users with the following MA/MA-PD/PDP/CC Application roles as applicable. MA Submitter, PDP Submitter, MA Representative, PDP Representative, Approver, POSFE Contractor, NET Submitter, NET Representative, Report View, MCO Representative UI Update. This will be fixed in a future release. Impact: Will cause confusion if the user or Helpdesk does not recognize the issue. The user will not be able to access the MA/MA-PD/PDP/CC application with his former role since the role is not reinstated in the Enterprise Directory Server. Workaround: The user will need to disassociate from the role again.			
8	Users who belong to an application integrated	For Application integrated using the Simple Application framework, a user with a 2-Factor	2011.03	TBD	2012.01

Item Number	Business / Application Area	Description	Release Issue Discovered	Fix CR/ Remedy#	Release in which Fix will be Applied
	using the Simple Integration framework are able to request and acquire both 2-Factor user and 2-Factor approver roles	approver role can request an end user role. This allows the approver to approve his own request. This will be fixed in a future release. Impact: None. Currently there are no Simple Integrated applications using the 2-Factor role. Workaround: None.			
9	Role drop down for Applications integrated using the Simple Integration framework not being refreshed and reflecting the incorrect roles list	During and "Add Application" profile modification, the Application Role drop-down list does not refresh when the user switches from one application to. This applies to all applications integrated using the Simple Integration framework. For example, 1. From the Modify Account profile page, the user selects the Add Application option and the Select Application drop-down is displayed with a list of applications. 2. The user selects an application from the drop-down and the associated roles are displayed in the Role drop-down. 3. The user changes his mind and selects another application from the Select Application drop-down. 4. At this point, the Role drop-down fails to refresh and continues to display the roles associated to the previously selected application. 5. Assume that the user does not realize that the role drop-down has not refreshed properly and continues to select a role and completes the modification request to add a role. 6. The Approver approves the pending request, not realizing the requested role is incorrect for the	2011.03	TBD	2012.01

Item Number	Business / Application Area	Description	Release Issue Discovered	Fix CR/ Remedy#	Release in which Fix will be Applied
		application. 7. The system attempts to update the user's profile and is unable to update the role since the role selected does not belong to that application. 8. The User's profile displays the Application but not the role. This issue will be fixed in a future release. Impact: User will not be able to log in to the application. Workaround: The user will need to contact the Helpdesk to get his profile corrected. Helpdesk will need to create a Service Request for the IACS Administrator to update the user's profile to its original state. Once this is completed, the user could submit the additional role request.			
10	CR 445:	The Manage users under my authority – Search Results for an application integrated using the Simple Integration framework, do not display the search results properly when the end user roles are associated with a multi-text attribute and the approver role is not. When a Helpdesk views the user information using the Manage users function, the user and the approver information are not displayed correctly due to fact of one role having the attribute and	2011.03	TBD	2012.01

Item Number	Business / Application Area	Description	Release Issue Discovered	Fix CR/ Remedy#	Release in which Fix will be Applied
		other not having it. Impact: None: Currently there are no applications integrated using the Simple Integration framework defined with multi-text attributes. The issue is with the display of the Search results. Workaround: Helpdesk could search users by specific roles instead of “All roles” option.			
11	CR-429:HPG Submitter ID field Optional	The HPG User Modify Account Profile page displays the ‘Modify Submitter ID’ as one of the Possible Actions the user could perform. The HPG user is not allowed to modify the Submitter ID. The Modify Account Profile page for the HPG User does not have an option to modify his Submitter ID. The Possible Actions field incorrectly shows the ‘Modify Submitter ID’ as one of the actions that the user could perform. This is a display issue that will be fixed in a future release. Impact: Will cause confusion if the user does not realize that the display is misleading and the Submitter ID cannot be modified. This is a display issue only.	2011.03	TBD	2012.01

5.0 Tips, Tricks and Other Advice

The following are key points and miscellaneous items, which are not issues but are to be noted as part of the implementation of Release 2011.03.

1. **Report Access Type for existing users and Report Access Type modification options**
   a) Post implementation, the existing MA/PDP/NET Submitters will have access to both the financial and non-financial report mailboxes. Submitter roles that do not wish to have access to both mailboxes should modify their profile, using the 'Modify Report Access Type' option from the 'Select Modify Action' drop-down.
   b) Once the user has access to a mailbox, they will be allowed to change the access type. Users will not be allowed to remove their access to both Gentran mailboxes as part of modification. The user's access to the mailboxes will be removed when the user disassociates from the role or fails certification.
2. **Validation and Modification of HPG Submitter ID Field**
   a) The MCARE Helpdesk will be responsible for validating the Submitter ID during the Approval process.
   b) MCARE Helpdesk will need to create a Service Request to be directed to the IACS Administrators to add or modify the Submitter ID in the HPG User's profile.
   c) The MCARE Helpdesk will be able to remove the Submitter ID from a HPG User's profile using the "Manage users under my authority" function.
3. **Modification to users First Name, Last Name, and/or Date of Birth**
   a) Helpdesks may get a request from a user to change his First Name, Last Name, and/or Date of Birth. Helpdesk will be responsible for verifying the user's information and will need to create a Service Request to be directed to the IACS Administrator to update the user information.
4. **Helpdesk User Interface Functions using Manage users under my authority**
   a) The View function: Application specific information will not be displayed in the Other Info tab for applications integrated using the Simple Integration framework that does not have defined application specific attributes. A message indicating that no application specific information exists will display in the tab.
   b) The View function: The Other Info tab can assist the PS&R/STAR Helpdesk in determining the CCNs entered by the Security Official (SO). The Helpdesk can search by the SO role, select the SO user, and use the View function to obtain the information on the 'Other Info' tab.
5. **Impact of the multiple profile modification requests to the MA/MA-PD/PDP/CC Application users**
   a) The 'Approve/Reject Request' page only reflects the user's profile at the time of the request. Approvers need to be aware that Users can submit multiple modification requests. When a user requests two MA/MA-PD/PDP/CC roles and is approved, all contracts in his profile will apply to both roles. Refer to the Known Issue item 5 in Section 4.0 for more details.

b) Approvers should review all role disassociation E-mail notices to ensure the contracts associated with the Role are appropriate. When a user has two roles and disassociates from one role, the contracts are not removed from the user's profile. Approvers should review the user's account and remove the user's contract(s) as needed. Refer to the Known Issue item 7 in Section 4.0 for more details.

6.0 Documentation Updates

IACS User Guides have been updated to include the changes that are made to the system as part of Release 2011.03.

1. **IACS User Guide For CMS Applications**

   IACS Registration, Modification of User Profile, and Annual Certification for existing users will be explained in this document for the following CMS Applications:

   - COB
   - CSP-HSTP
   - CSP-MCSIS
   - CSR
   - DMEPOS Bidding System
   - ECRS
   - GENTRAN
   - HPG
   - HETS UI
   - Internet Server
   - MA/MA-PD/PDP/CC
   - MDR
   - MED
   - PQRS/eRx
   - PS&R/STAR
   - EHRD

2. **IACS User Guide for Approvers**

   This User Guide will explain the process for approving New Users registration, Modify Profile, and Certification requests for new users and existing users.

3. **IACS User Guide for Helpdesk**

   This User Guide will explain the process for performing help desk functions for IACS Helpdesk users.