Individuals Authorized Access to CMS Computer Services

(IACS)

Provider User Guide

(Supplemental)

Software Release 4.2.2

Document Version 1.0

April 2007

CONTENTS

FIGURES

1.0   Introduction

1.1   Purpose

This document establishes the procedures for Logging in for the first time, password resets and accessing the CMS 270/271 application using the Individuals Authorized Access to CMS Computer Services (IACS) application within the Centers for Medicare & Medicaid Services (CMS). Registration procedures for Security Officials, User/Approvers, and User/Providers are described in additional role-specific documents.

1.2   How to Use this document

When an action is required on the part of the reader, it is indicated by a line beginning with the word "Action:" For example:

Action: Click on *OK.*

The field or button to be acted upon is indicated in ***bold italics*** in the **Action** statement.

2.0 Logging in for the First Time

After registration is complete and the user logs in for the first time:

- The user must change his/her password

- The user must answer at least two (2) of the authentication questions (until that is done, s/he will not see any additional links - such as waiting approvals)

- The *change password* and *change authentication* links that appear after the first login and authentication question setup provide the user with the option of changing those values – they are not mandatory

2.1 Change your Password

Action: Using the User Identifier (UID) and onetime password provided, login to the IACS system at https://applications.cms.hhs.gov to change your password.

Action: Read the contents of the government computer system "WARNING/REMINDER" screen, and then agree by clicking **Enter CMS Applications Portal.** *(See* Figure 1*)*
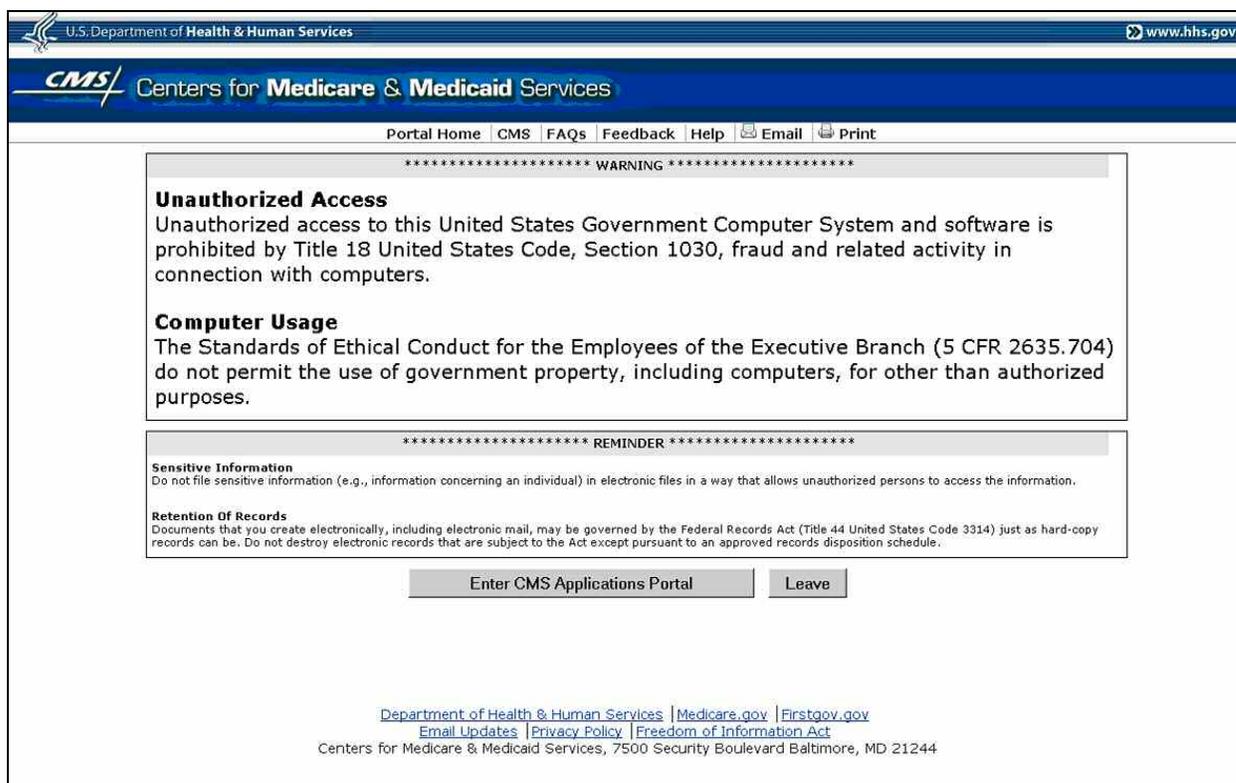
Figure 1: Government Computer System Warning/Reminder Screen

Action: If you do not want to proceed any further, you can click on **Leave** to exit**.**

The "CMS Application Portal Introduction" screen will open as shown in Figure 2

Action: Click on *Account Management* in the blue menu bar toward the top of the screen.
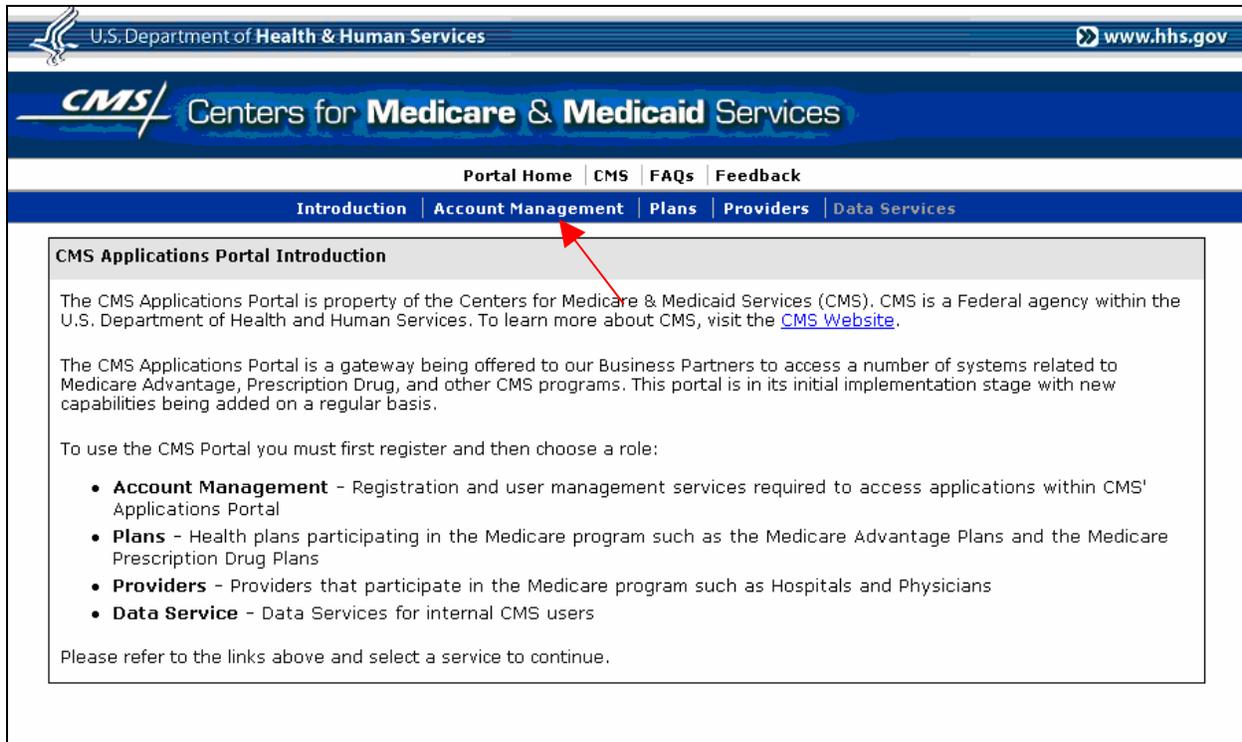
Figure 2: CMS Application Portal Introduction Screen

The screen will update to the display shown in Figure 3.

Action: Click on *My Profile* in the "Account Management" screen.

Figure 3: Account Management Screen

The "Login to IACS" screen will open as shown in Figure 4.

Action: Enter your new *User ID*

Action: Enter your onetime *Password* and click *Login*.
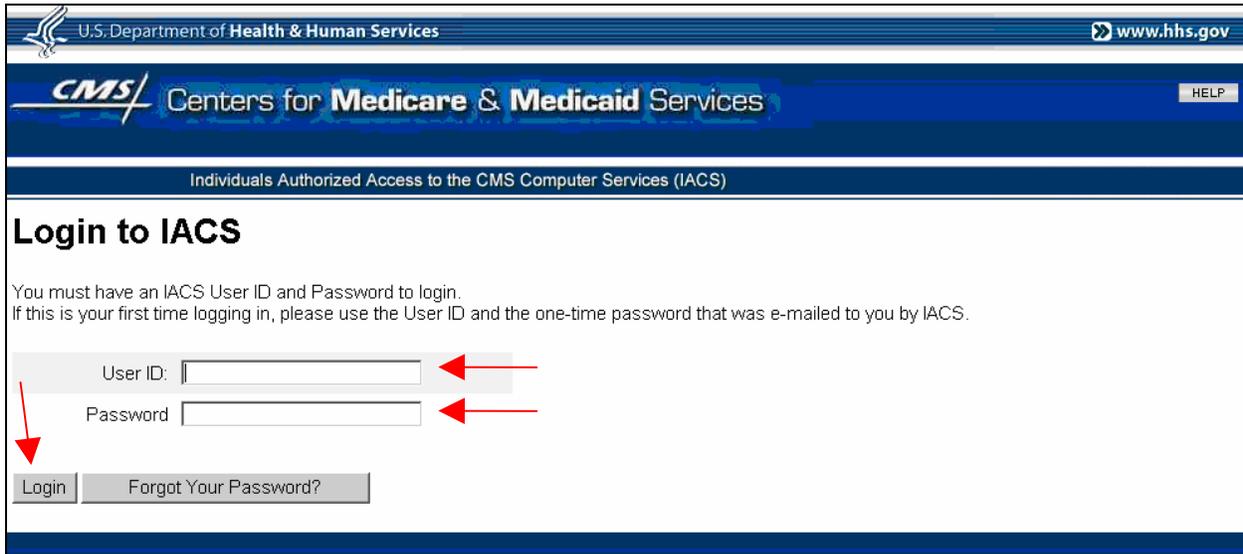
Figure 4: Log In to IACS Screen

A **Change Password** window will open as shown in Figure 5.

Action: Enter a new *Password* in the **Password** field and then re-enter it in the **Confirm Password** field as verification.

Note: This screen also appears as a result of a user requested password reset.
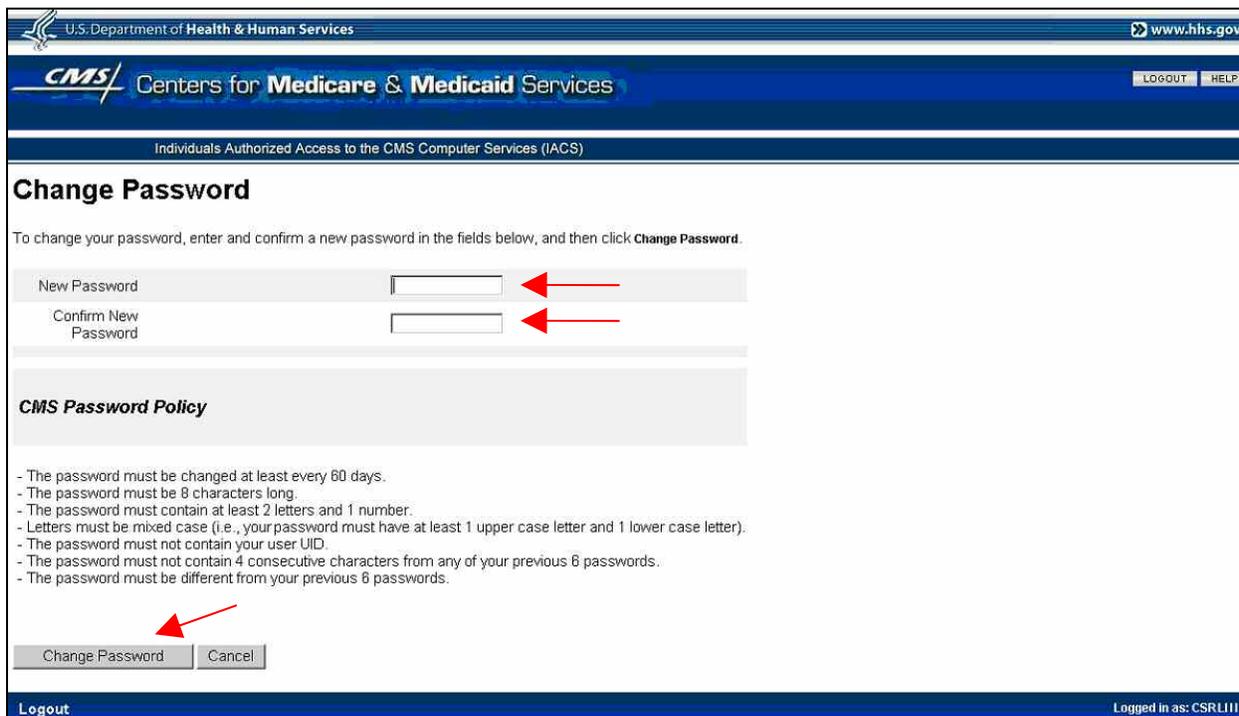
Figure 5: Change Password Field Entry Screen

The IACS password must meet the following policy rules:

- Must be 8 characters in length
- Must contain at least two alpha characters and one number (no special characters)
- Alpha characters must be mixed case (i.e., must have at least one upper case letter and one lower case letter
- Cannot begin with a number
- Must not have more than 4 consecutive characters of any of the past 6 passwords
- Must not contain the UID
- Must be different from the previous 6 passwords

Action: Click on *Change password.*

Note: If the "Change Password" screen reappears, a password policy violation has occurred. Check the message that appears below the **Change Password** label and process accordingly. (See Figure 6)

Possible password policy violation messages:

- New password cannot match any of the 6 previous passwords for this account
- Fields **Confirm Password:** and **Password:** do not match
- Must have at least 2 alpha characters
- Must have at least 1 upper case and 1 lower case alpha character
- Must have at least 1 numeric character
- Cannot begin with a number
- Must be 8 characters in length

Figure 6: Change Password Policy Violation Message Screen

In addition:

- The password must be changed at least every 60 days

- The password must not contain a user's UID

- The password must not contain a reserved word: PASSWORD, WELCOME, CMS, HCFA, SYSTEM, MEDICARE, MEDICAID, TEMP, LETMEIN, GOD, SEX, MONEY, QUEST, 1234, 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

2.2   Change Answers to Authentication Questions

Once your password has been successfully changed, you'll be asked to answer at least two (2) authentication questions. Your answers will be used in the future in the event you forget your password. (See Figure 7) You must answer at least two of the authentication questions. If you do not, you may not be allowed access to the system if you forget your password.

Action: Click on *Change Answers to Authentication Questions*.
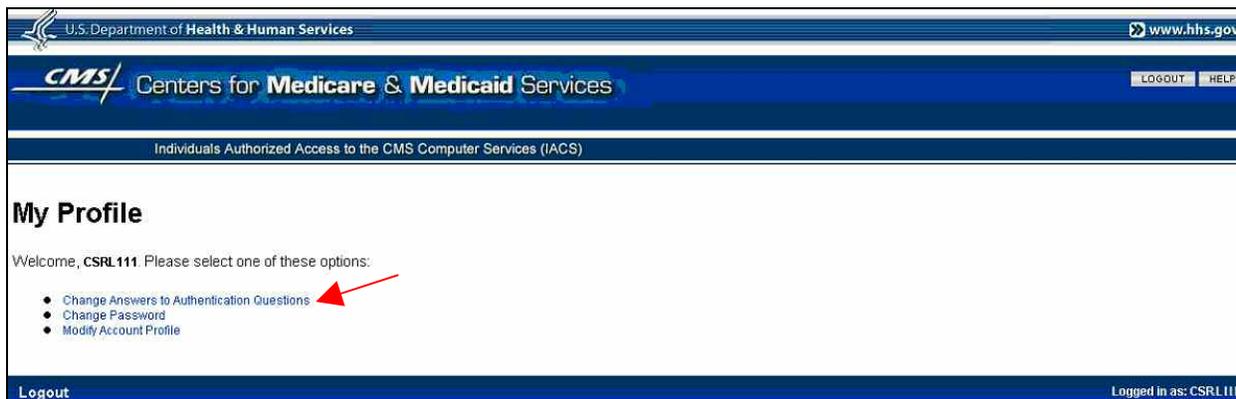
Figure 7: My Profile Screen Showing Change Answers to Authentication Questions Option

Action: Answer at least two (2) of the ten (10) *Authentication Questions.* (See Figure 8)

Figure 8: Change Answers to Authentication Questions Screen

Action: Click *Save* when you have finished answering the questions you want to answer. The question answer results will be displayed as shown in Figure 9.

Action: Click *OK* when you have finished viewing your questions.
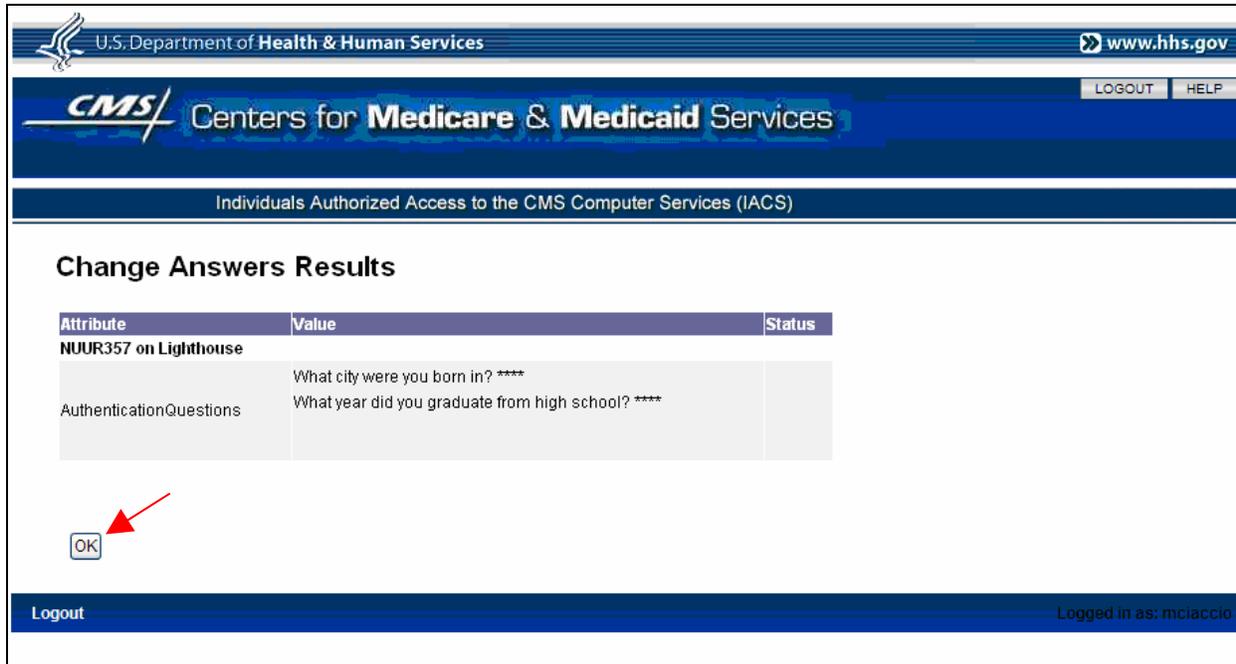
Figure 9: Change Answers Results Screen

Note: After the initial login, the *Change Password* and *Change Answers to Authentication Questions* options only need to be selected if you want to change those values. (See Figure 10)
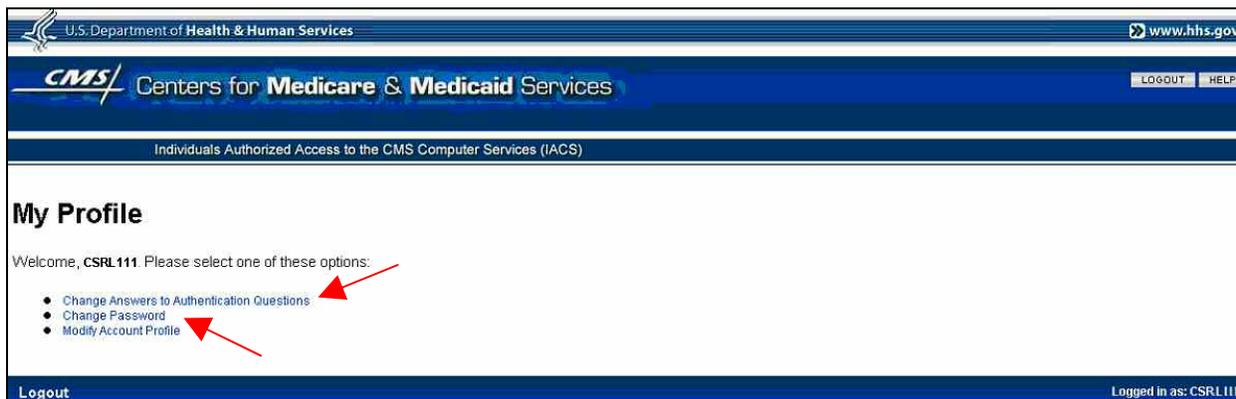
Figure 10: My Profile Screen

3.0   Password Reset

When you want to log in to IACS, you are required to enter your User ID and Password in a screen such as that shown in Figure 11.

If you enter your password incorrectly three (3) times, the system will lock your account and it can only be reset by an IACS Administrator (Admin) at CMS. While your account is locked, you cannot access any other features.

If you know you have forgotten your Password, enter your User ID and click on *Forgot Your Password?*.

Note: After a third failed login attempt, your account will be locked as stated above and you will not be able to access the "Forgot Your Password" functionality. You must then contact the appropriate Help Desk for your user community (See **Section 6.2 Help Desk Information**) to get an Admin to reset your password. When an Admin resets your password, you will be sent an email with the temporary one-time password which you may then use to go in and change the password to one of your choice.

Figure 11: Log In to IACS Screen

An "Identify User" screen will be displayed, similar to the example shown in Figure 12. Fields for the questions you answered during your initial login will be displayed. You must correctly answer at least two of the questions. If you incorrectly answer the questions three times in a row, your account will be locked. You must call the applicable Help Desk for your user community to have a system administrator unlock your account. (See **Section 6.2 Help Desk Information.**)

Action: Answer each question with the exact answer previously provided.

Action: Click on *Login*.

Figure 12: Password Identify User Screen

The "Login to IACS" screen will reappear with a new message above the User ID field indicating that a one-time password has been emailed to you. (See Figure 13)

Figure 13: Password Email Notification Screen

Action: Go to your email and get your new password. This is a one-time password and you must change your password when you log in. Figure 14 shows an example of the password notification email you will receive.

Your temporary one-time password is Q377suA4.
Please go to the link below to change your password.

Go to https://applications.cms.hhs.gov
Read the Privacy Statement and click "Enter".

Select the **"Account Management"** link on the blue menu bar, and then the **"My Profile"** link

Log into IACS using your User ID and password to change your password.

Thank you,
IACS

Please do not reply to this system-generated email.

Figure 14: Example of a Password Notification Email

Action: Refer to the **Section 2.0** and follow the steps for logging in and changing your password. You do not have to answer the authentication questions again unless you want to change your answers.

4.0 CMS Application Access

4.1 Login to Provider (270/271)

Once you have been approved and provisioned in IACS, you will want to access the 270/271 UI Application. Only users with the role of User/Provider are allowed to access the application. You will login through IACS and the service will verify and authorize you to access the desired plan. You will then be presented the opening screen for the application you are accessing.

The following steps and screens show you how to access your desired plans through IACS.

Action: Browse to https://applications.cms.hhs.gov (See Figure 15).

Action: Read the contents of the government computer system WARNING/Reminder screen, and then agree by clicking *Enter CMS Application Portal.*
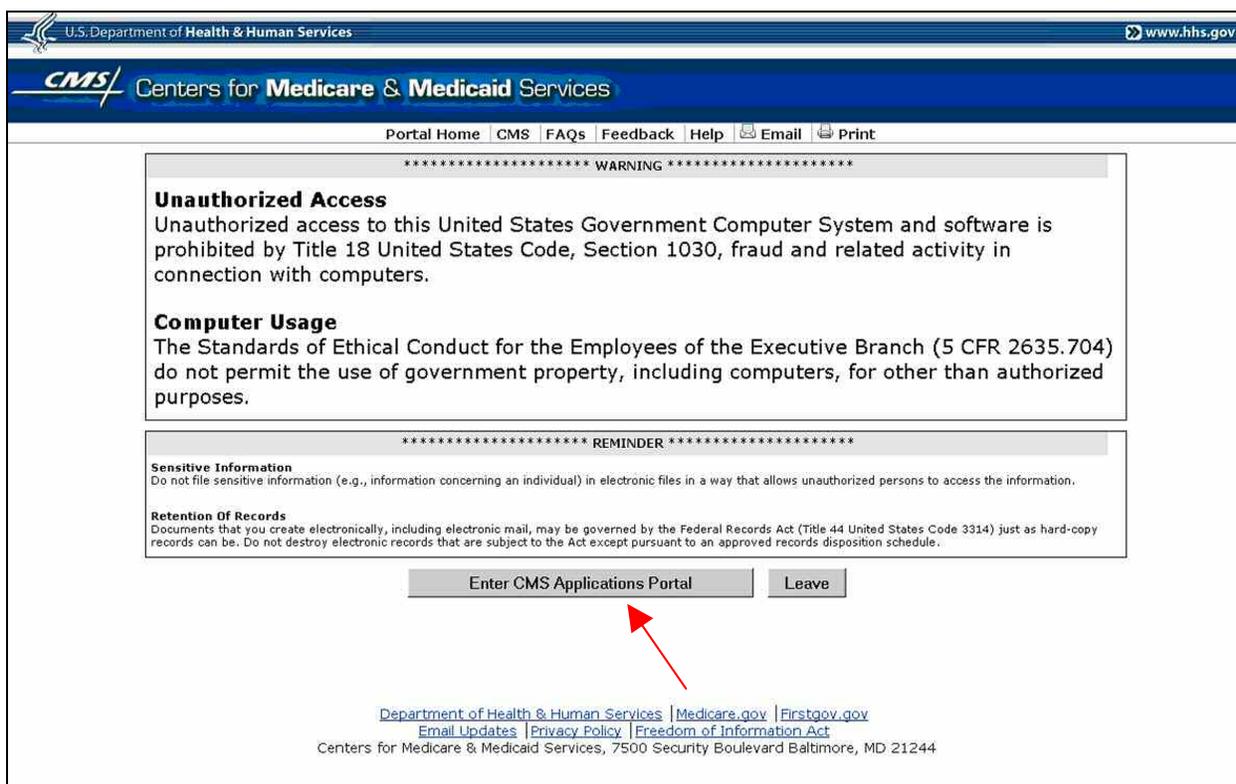
Figure 15: Government Computer System Warning Screen

If you do not want to proceed any further, you can click on *Leave* to exit.

The CMS Application Portal screen will open as shown in Figure 16.

Action: Click on *Providers* in the blue menu bar.
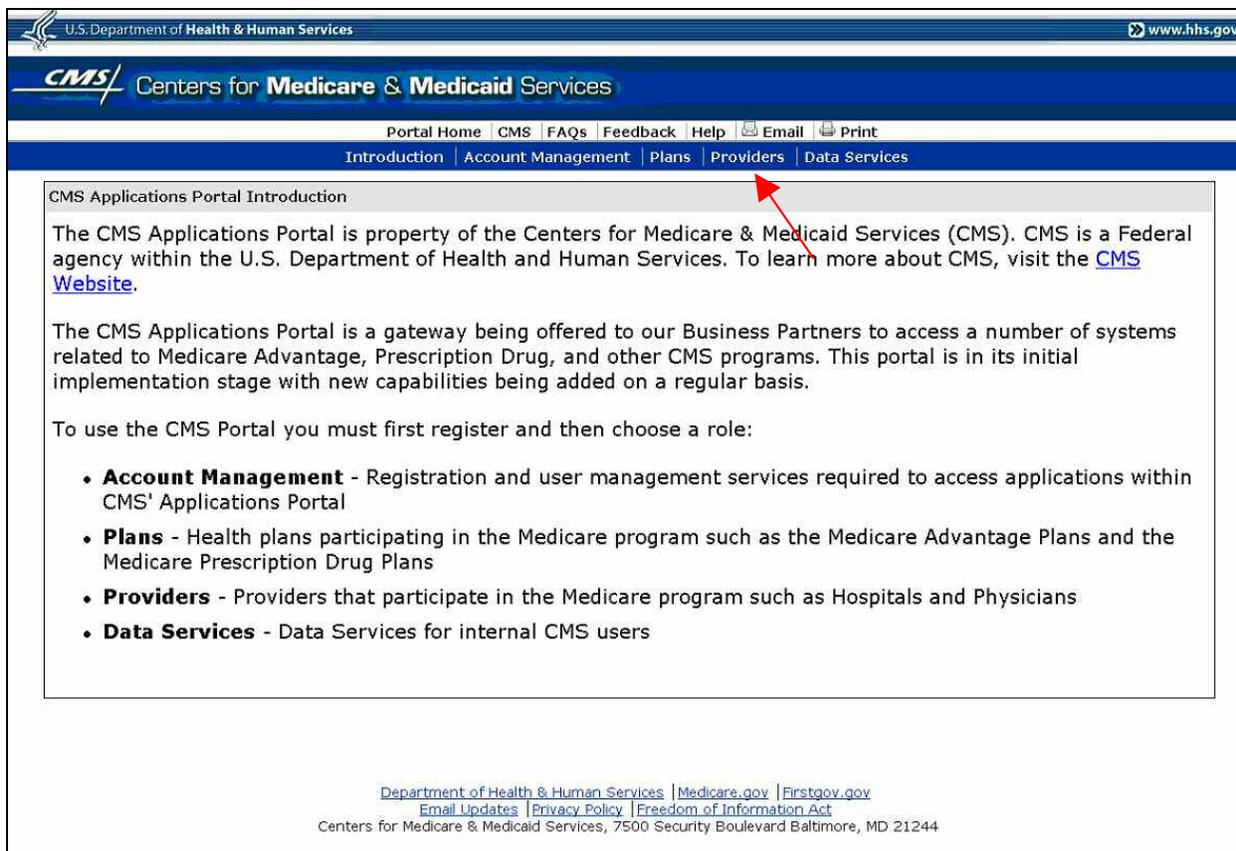
Figure 16: CMS Applications Portal Introduction Screen

The screen will change to the 'Providers' screen shown in Figure 17.

Figure 17: Providers Screen

Action: Click on **Eligibility Inquiry and Response (270/271)**.

The IACS Login screen will be displayed as shown in Figure 18.

Figure 18: Login to IACS Screen

When you login with your IACS User ID and Password, the system will verify your identity. The IACS service will notify the 270/271 application software that you are authorized to access the application. The application will then open the first screen for you to begin your work.

5.0   Questions and Troubleshooting

5.1   Help

For questions regarding the IACS system, please go to the CMS FAQ page as follows:

- Go to: https://www.cms.hhs.gov/home/tools.asp

- Under **Sitewide Tools and Resources**

- Click on **Frequently Asked Questions**

- Do a Search on "**IACS**"

Answers to many commonly asked IACS questions can be found through this process. If you have further questions, please call the applicable Help Desk for your user community. (See **Section 6.2 Help Desk Information.**)

5.2   Being Proactive

A large majority of the problems users of the IACS system face occur due to human error. Most of these can be avoided if greater care is exercised during the registration and approval process. Please double-check information on the registration form prior to submission. If you are an approver, double-check the information that your users have entered, before approving or rejecting the request. These two quick and simple steps will help get users into the IACS system as quickly as possible.

5.3   Proper Software

To optimize your access to the IACS screens, ensure the following criteria are met.

1. CMS screens are designed to be viewed at a minimum screen resolution of 800 x 600.

2. Use Internet Explorer, version 6.0 or higher.

3. Verify that the latest version of JAVA and/or ActiveX is installed on your PC.

4. Disable pop-up blockers prior to attempting access the CMS Applications Portal.

Contact your appropriate Help Desk if you have questions about any of the above criteria. (Refer to **Section 6.2 Help Desk Information.**)

6.0   Helpful Hints

6.1   Registering in IACS

1. When entering your email address, please be very careful to type the correct email address. If your email address is entered incorrectly, you will not receive your new User ID and Password.

2. When entering multiple similar items such as Contract Numbers, Call Centers, or Organization Numbers, you need to hit the **Add** button after each and every item that is entered. Do not enter all items on one line.

3. If you have a RACF-ID already assigned (this is the same as your HPMS User ID, if you have one), you need to enter that into your registration when prompted. This User ID must be entered in all UPPERCASE letters.

4. Once a user completes their registration in IACS, the EPOC will receive an email prompting them to approve the user. Follow up with your EPOC(s) to ensure this step is completed.

5. User IDs will not be issued until approvals/rejections are completed for all items entered – and there may be separate approvers for different item numbers.

6. If you have not received an email with a confirmation of your request within 24 hours of registration, please call the applicable Help Desk for your user community. (See **Section 6.2 Help Desk Information.**)

7. Do not respond to the email for any notifications you receive regarding IACS. Call the appropriate Help Desk. Responding to the email will delay any required assistance.

6.2   Help Desk Information

The Help Desk associated with the 270/271 Provider community is the MEIC Help Desk. The phone number is 1-866-440-3805. They can be contacted at *MCARE@cms.hhs.gov.*

7.0 Legal

7.1 Privacy Act Statement

The information on the web form is collected and maintained under the authority of Title 5 U.S.C., §552(e) (10). This information is used for assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. The Privacy Act prohibits disclosure of information from records protected by the statute, except in limited circumstances.

The information you furnished on this web form will be maintained in the Individuals Authorized Access to the Centers for Medicare & Medicaid Services Computer Services (IACS) Systems of Records and may be disclosed as a routine use disclosure under the routine uses established for this system as published at 09-70-0064 (08-11-94) and as CMS may establish in the future by publication in the Federal Register.

The Social Security Number (SSN) is used as an identifier in the Federal Service because of the large number of present and former Federal employees and applicants whose identity can only be distinguished by use of the SSN is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary. However, if you do not provide this information, you will not be granted access to CMS computer systems.

7.2 Rules of Behavior

CMS computer systems that you are requesting to use contain sensitive information. Sensitive information is any information which the loss, misuse, unauthorized access to, or modification of could adversely affect the national interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. To ensure the security and privacy of sensitive information in Federal computer systems, the Computer Security Act of 1987 requires agencies to identify sensitive computer systems, conduct computer security training, and develop computer security plans. CMS maintains a system of records for use in assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. CMS records all access to its computer systems and conducts routine review for unauthorized access to and/or illegal activity.

Anyone with access to CMS Computer Systems containing sensitive information must abide by the following:

- Do not disclose or lend your IDENTIFICATION NUMBER AND/OR PASSWORD to someone else. They are for your use only and serve as your electronic signature. This means that you may be held responsible for the consequences of authorized or illegal transactions.

- Do not browse or use CMS data files for unauthorized or illegal purposes.

- Do not use CMS data files for private gain or to misrepresent yourself or CMS.

- Do not make any disclosure of CMS data that is not specifically authorized.

- Do not duplicate CMS data files, create sub-files of such records, remove or transmit data unless you have been specifically authorized to do so.

- Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so.

- Do not make copies of data files, with identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so.

- Do not intentionally cause corruption or disruption of CMS data files.

A violation of these security requirements could result in termination of systems access privileges and/or disciplinary/adverse action up to and including legal prosecution. Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system. If you become aware of any violation of these security requirements or suspect that your identification number or password may have been used by someone else, immediately report that information to your component's Information Systems Security Officer or your organization approving official for CMS access.