Average Sales Price (ASP)

Registration User Guide

Version 0.1

Date: January 22, 2024

Table of Contents

1.   Purpose

The purpose of this user guide is to provide instructions for registering as a new user in the Centers for Medicare & Medicaid Services (CMS) Identity Management (IDM) system to request access to the Fee-for-Service Data Collection System (FFSDCS) Average Sales Price (ASP) Module.

CMS requires an automated data collection system that can collect and synthesize large amounts of data related to products falling under the Fee-for-Service (FFS) payment mechanisms.

CMS supplies the Medicare FFS claims processing contractors with the drug pricing files for Medicare Part B. CMS uses the FFSDCS to house various Fee-for-Schedule platforms, including the ASP Module.

Before you can log in to any FFSDCS Module, you must create a new user account. All FFSDCS Module users, regardless of their role, must complete the new user registration steps in the following section.

2. New User Registration

You must have an IDM username and password to access the ASP Module. Follow these steps to register with IDM and receive your credentials:

1. Navigate to the CMS Enterprise Portal main page.

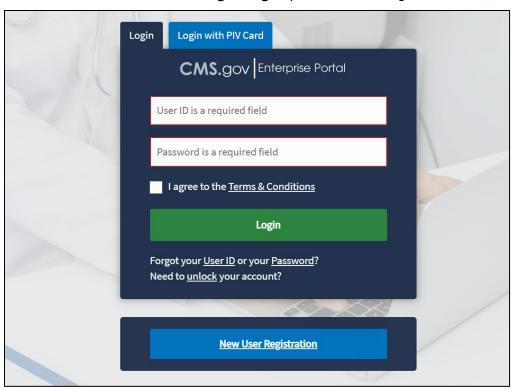   The FFSDCS **Module Login Page** opens. Refer to *Figure 1*.

Figure 1: CMS Enterprise Portal - Login Page

2. Click the **New User Registration** button.

   The **Select Your Application** page opens. Refer to *Figure 2*.

Figure 2: New User Registration - Select Your Application Drop-down

3. Click the **Select Your Application** drop-down; select **FFSDCS** from the list of applications.

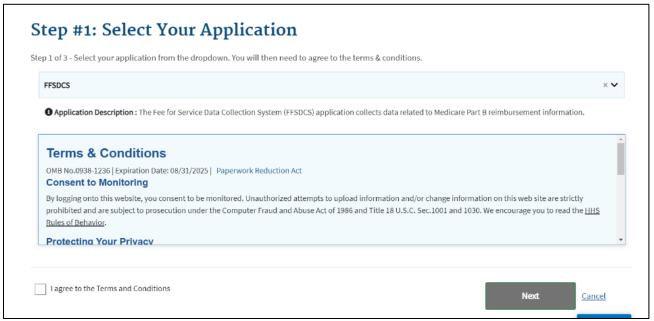The **Step #1: Terms and Conditions** page opens. Refer to *Figure 3*.

Figure 3: New User Registration - Terms & Conditions

4. Read the **Terms & Conditions**. If you agree, select the **I agree to the Terms & Conditions** checkbox; click **Next**.

    Note: By selecting this checkbox, you certify that you read and consent to monitoring while accessing and using the portal. The terms and conditions describe why the application collects personally identifiable information (PII), which is to identify the unique, new user who is registering to use the application.

    The terms and conditions link provides additional hyperlinks to the HHS Rules of Behavior and the CMS Privacy Act Statement.

5. The **Step #2: Register Your Information** page opens. Refer to *Figure 4*.
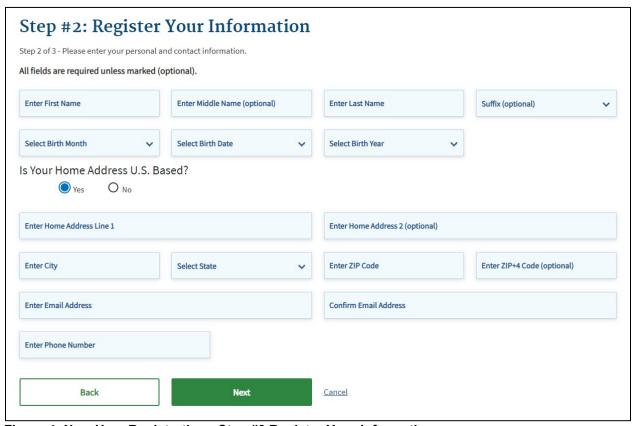
Figure 4: New User Registration - Step #2 Register Your Information

6.   Enter your personal information in each of the required fields; click **Next**.

   Note: The application requires you to complete all fields unless marked as optional.

   The **Step #3: Create User ID, Password & Security Question/Answer** page opens. Refer to *Figure 5*.

Step #3: Create User ID, Password & Security Question/Answer

Step 3 of 3 - Please create User ID and Password. Select a Security Question and provide Answer.

All fields are required unless marked (optional).

Enter User ID

Required field.

Enter Password

Confirm Password

Must contain a minimum of 15 characters.

Required field.

Security answer to be used in case you forget your password or you need to unlock your account.

Select Security Question

Enter Security Answer

Back   Next   Cancel

Figure 5: New User Registration - Step #3 Create User ID & Password

7. Type your desired user identification in the **User ID** field.

   Note: Per the User ID Requirements, your user ID must:

   a. Consist of a minimum of six (6) alphanumeric characters and cannot exceed seventy-four (74) characters.
   b. Contain at least one (1) uppercase or lowercase letter.
   c. Contain one (1) special character. You may use hyphens (-), underscores (_), apostrophes ('), and periods (.).
   d. Not have a special character as the first or last letter of your user ID.
   e. Not contain eight (8) consecutive numbers.

8. Type your desired password in the **Password** field; then re-type your password in the **Confirm Password** field. Passwords must match before you move onto the next step.

   Note: Your password must conform to the CMS Acceptable Risk Safeguards (ARS) Password Policy. You may only change your password once every 24 hours. Per the password policy, your password must:

   a. Consist of a minimum of fifteen (15) alphanumeric characters and cannot exceed sixty (60) characters.
   b. Contain at least one (1) uppercase and one (1) lowercase letter.
   c. Contain at least one (1) number.
   d. Not contain part of your user ID, first name, last name, or common passwords.
   e. Be different from your previous six (6) passwords.

Note: Special characters are optional in your password. The system accepts the following special characters: ('), ("), (!), (#), ($), (%), (&), ((), ()), (*), (+), (,), (-), (.), (/), (:), (;), (<), (>), (=), (?), (@), ([), (]), (^), (_), (`), (~).

9. Select a security question from the **Security Question** drop-down; enter your answer in the **Security Answer** field. Refer to *Figure 6*.

    Note: The system requires your security answer to reset your password or unlock your account. Per the security answer requirements, your security answers:

    a. Must contain at least four (4) alphanumeric characters.
    b. Cannot contain part of your security question.
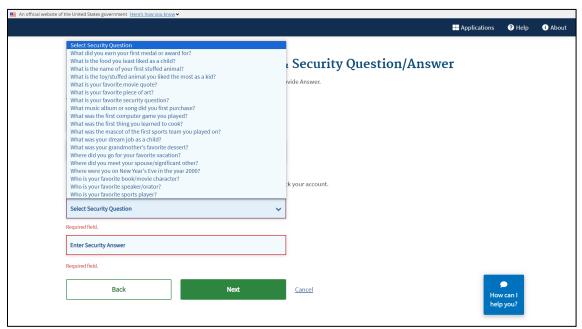   c. Can contain spaces.

Figure 6: New User Registration - Security Question/Answer Page

10. Click **Next** to complete the registration process.

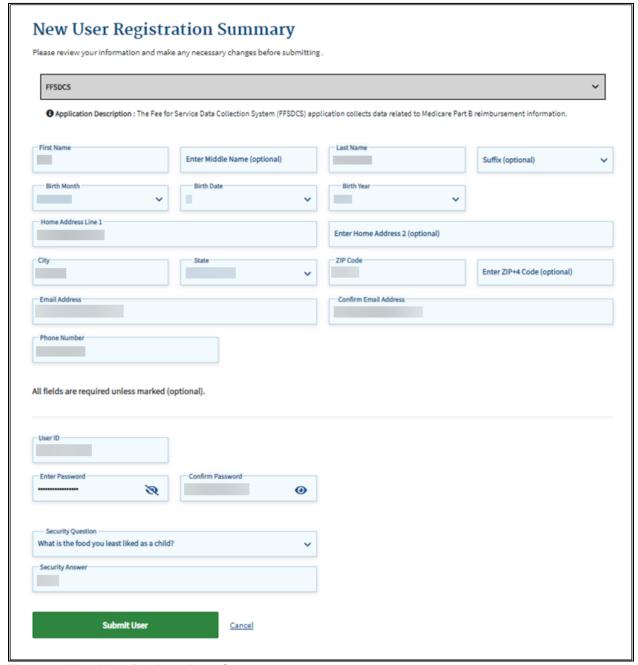   The **New User Registration Summary** page opens. Refer to *Figure 7*.

New User Registration Summary

Please review your information and make any necessary changes before submitting.

FFSDCS	⌄

ⓘ Application Description : The Fee for Service Data Collection System (FFSDCS) application collects data related to Medicare Part B reimbursement information.

First Name | Enter Middle Name (optional) | Last Name | Suffix (optional) ⌄

Birth Month ⌄ | Birth Date ⌄ | Birth Year ⌄

Home Address Line 1 | Enter Home Address 2 (optional)

City | State ⌄ | ZIP Code | Enter ZIP+4 Code (optional)

Email Address | Confirm Email Address

Phone Number

All fields are required unless marked (optional).

User ID

Enter Password | Confirm Password

Security Question
What is the food you least liked as a child? ⌄

Security Answer

Submit User | Cancel

Figure 7: New User Registration - Summary

Note: You may click the **Cancel** button to exit out of the registration process; however, the system does not save any of the changes you entered.

11. Review the **New User Registration Summary** page; make necessary changes.
12. Click the **Submit User** button to complete the registration process.

A **Confirmation** message displays. Refer to

Figure 8.

Figure 8: New User Registration Confirmation

13. Click the **login** hyperlink to return to the main login page.

Note: Wait at least five minutes before logging in to the FFSDCS Module with your new User ID and Password.

3. Logging in Using MFA

Following registration, use these steps to log in to the FFSDCS Module:

1. Navigate to the CMS Enterprise Portal main page.
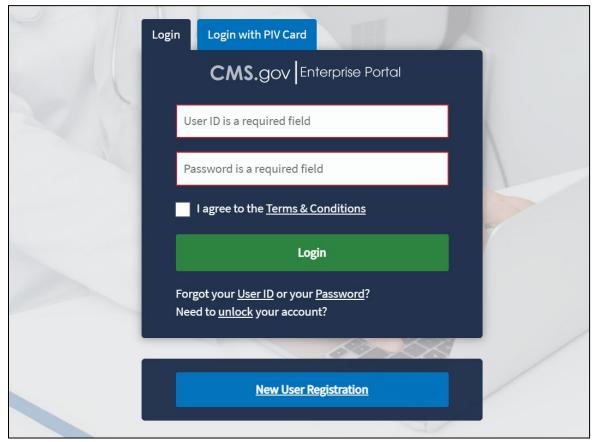
   The **FFSDCS Module Login Page** opens. Refer to *Figure 9*.

Figure 9: Logging in Using MFA - FFSDCS Module Login Page

2. Type your user ID and password in the **User ID** and **Password** fields.
3. Click the **Terms & Conditions** hyperlink and review the text in the pop-up window; close the window.
4. Read the terms and conditions. If you agree, select the **I agree to the Terms & Conditions** checkbox.

   Note: By selecting this checkbox, you certify that you read and consent to monitoring while accessing and using the portal. Additionally, the terms and conditions provide hyperlinks to the HHS Rules of Behavior and the CMS Privacy Act Statement.

5. Click **Login**.

   Note: If you forget your user ID or password, click the appropriate hyperlinked text in **Forgot your User ID or your Password?** under the **Login** button and follow the provided instructions. If you are still not able to access your account and need to unlock your account, click the hyperlinked unlock text under **Need to unlock your account?**

To confirm the security of the FFSDCS Module, as well as your data, you must authenticate your identity using a multifactor authentication (MFA) process. Users have various authentication options, including Interactive Voice Response (IVR), Email, Text Message (Short Message Service (SMS)), or Okta Verify.

6. Click the **Select MFA Device** drop-down; select your preferred MFA device type from the list. Whenever you log back into the ASP Module through this process, your preferred method of MFA reloads automatically. Refer to *Figure 10*.

Figure 10: Logging in Using MFA - Select MFA Device Type Drop-Down

7. Click the **Send MFA Code** green button to receive a one-time phone call, email, text message, or other communication to confirm registration of your identity with the FFSDCS Module. This user guide demonstrates email as the chosen MFA method. Refer to *Figure 11*.

Figure 11: Logging in Using MFA - MFA Code

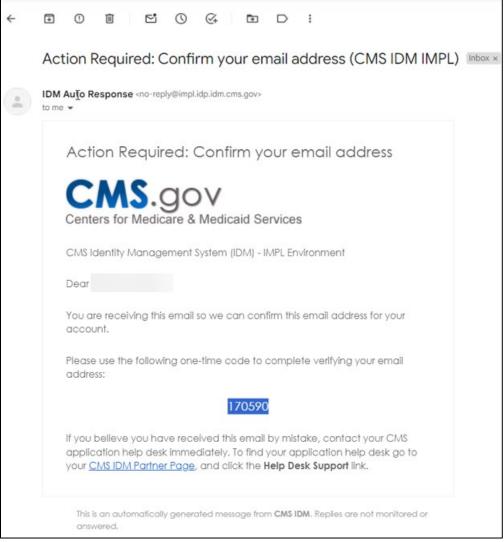The Module sends an email with a six-digit code to confirm your identity. Refer to *Figure 12*.

Figure 12: Logging in Using MFA - Confirmation Code in Email

8. Record and type the six-digit code into the **Enter MFA Code** field. Click the **Add Device** button to confirm your identity and enter the FFSDCS Module.

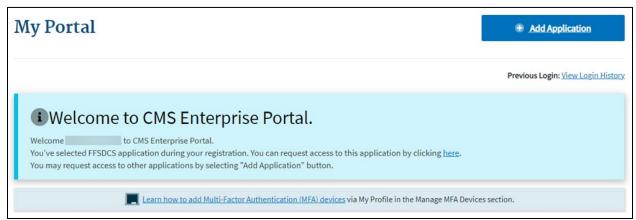   The **My Portal** landing page opens, displaying a **Welcome to CMS Enterprise Portal** message. Refer to *Figure 13*.

Figure 13: Logging in Using MFA - My Portal Landing Page

4. Select User Role/Application Request

The Medicare ASP Data Collection System is a role-based system. This means that certain system functions link to specific user role profiles. When a new user receives access, the approved role provides access to the specific functions the user needs.

As noted above, the two roles are:

Submitter: This role is designated for the person who gathers the required Medicare Part B drug data to enter and submit into the system. Once this person has completed and submitted the data, they generate a one-time password (OTP) to send to the Certifier to establish a relationship within the system. This step only happens once to initiate the relationship and only needs to happen again if the person in either role changes. A Submitter can be any individual the manufacturer chooses, including a third-party contractor.

Certifier: This role is designated for the person who reviews the information the Submitter reports to ensure it is correct and complete. The Certifier then certifies the submission of the reported data. If the Certifier requires changes to the originally submitted data reported in the system, the Certifier must notify the Submitter to update and submit the revised data. As stated in 42 CFR 414.804(a)(7), the Certifier must be the manufacturer's Chief Executive Officer (CEO) or Chief Financial Officer (CFO) or an individual who has delegated authority to sign for, and who reports directly to, the manufacturer's CEO or CFO.

It is at the discretion of each organization who to designate as Submitter and Certifier. These individuals require access to financial data and must have a strong working knowledge of how the organization operates. The Submitter and Certifier must be two different authorized representatives from the Drug Manufacturer. The manufacturer's CEO or CFO assumes responsibility for the information entered into the system.

Follow these steps to request access to an application and establish your role in the application:

1. Click the **Add Application** button.

   The **Request Application Access** page opens. Refer to *Figure 14*.

Figure 14: Select User Role/Application Request - Request Application Access

2. Click the **Select an Application** drop-down; scroll or search for your application. Refer to *Figure 15*.

Figure 15: Select User Role/Application Request - Select an Application Drop-down

3. Select **FFSDCS** from the drop-down menu. To be a Submitter or Certifier, you must register for the role on the FFSDCS Module.

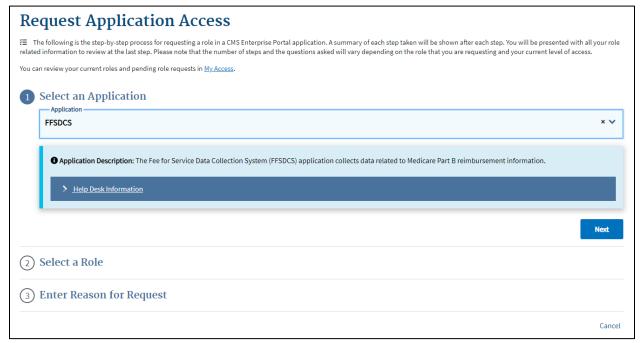The **Request Application Access** page opens. Refer to *Figure 16*.

Figure 16: Select User Role/Application Request - Select an Application

4. Click the **Next** button.

    A checkmark displays next to **FFSDCS**; the application automatically moves you to the **Select a Role** section. Refer to *Figure 17*.

Figure 17: Select User Role/Application Request - Select a Role

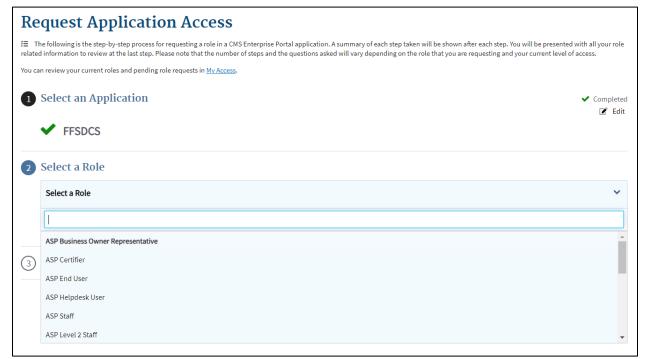5. Click the **Select a Role** drop-down; scroll or search for your application. Refer to *Figure 18*.

Figure 18: Select User Role/Application Request - Select a Role Drop-down

6. Select the correct role for the application. For example:
    a. If you are an ASP Submitter, click the **Role** drop-down and select **ASP End User** as your role. ASP Submitters can only submit data.
    b. If you are an ASP Certifier, click the **Role** drop-down and select **ASP Certifier**. ASP Certifiers can only certify data.

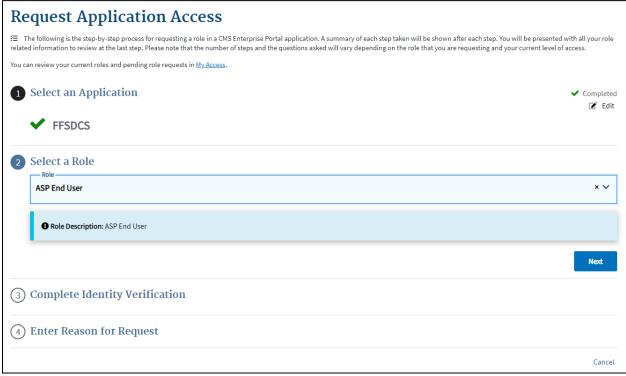   For example, the user has selected the **ASP End User** (Submitter) role in *Figure 19*.

Request Application Access

The following is the step-by-step process for requesting a role in a CMS Enterprise Portal application. A summary of each step taken will be shown after each step. You will be presented with all your role related information to review at the last step. Please note that the number of steps and the questions asked will vary depending on the role that you are requesting and your current level of access.

You can review your current roles and pending role requests in My Access.

1 Select an Application   ✔ Completed
                                                                ✎ Edit

   ✔ FFSDCS

2 Select a Role

   ── Role ──
   ASP End User   ✕ ⌄

   ❶ Role Description: ASP End User

                                                                  [Next]

3 Complete Identity Verification

4 Enter Reason for Request

                                                                    Cancel

Figure 19: Select User Role/Application Request - Selected Role as ASP End User

7. Click the **Next** button to confirm your role.

    A checkmark displays next to your selected role; the application automatically moves you to the **Complete Identity Verification** section. Refer to *Figure 20*.
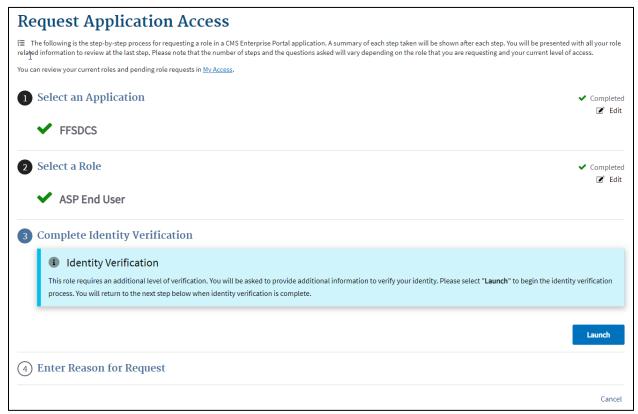
Figure 20: Select User Role/Application Request - Complete Identity Verification

8. Click the **Launch** button.

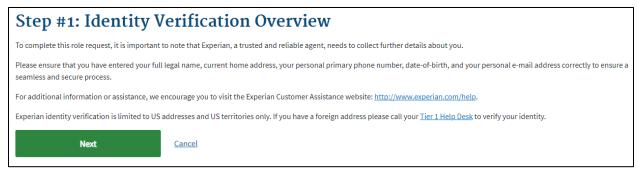   The **Step #1: Identity Verification Overview** page opens. Refer to *Figure 21*.

Figure 21: Select User Role/Application Request - Step #1: Identity Verification Overview

9. Read the **Identity Verification Overview** to gain an understanding of your privacy as well as the process Experian Credit Bureau uses to accurately confirm the identity of users; click **Next**.

   The **Step #2: Accept Terms & Conditions** page opens. Refer to *Figure 22*.

Figure 22: Select User Role/Application Request - Step #2: Accept Terms & Conditions

10. Read the terms and conditions derived from the [Paperwork Reduction Act of 1995](), consisting of three sections: Protecting Your Privacy, HHS Rules of Behavior, and Identity Verification.

11. If you agree to the terms and conditions, select the **I agree to the Terms & Conditions** checkbox; click **Next**.

    The **Step #3: Enter Your Information** page opens. Refer to *Figure 23*.

Figure 23: Select User Role/Application Request - Enter Your Information

12. Enter your information in all required fields.

    Note: Once you complete all fields, ensure the checkmark is present at the bottom of the page before moving on.

13. Click **Next**.

    The Multi-Factor Authentication Information page opens. Refer to *Figure 24*.

Figure 24: Select User Role/Application Request - MFA Information

14. Read the message about MFA information; click **Next** to continue.

    The **Register Your Phone, Computer, or Email** page opens. Refer to *Figure 25*.

Figure 25: Select User Role/Application Request - Register Your Phone, Computer, or Email

15. Select a device from the **MFA Device Type** drop-down. Enter any required information requested for the selected device; click **Next**.

    A message opens indicating the system successfully registered your device. Refer to *Figure 26*.

Figure 26: Select User Role/Application Request - Successfully Registered MFA Device

16. Click **OK**.

    A **Request Acknowledgement** page opens. Refer to *Figure 27*.

Figure 27: Select User Role/Application Request - Request Acknowledgement

17. Read the **Request Acknowledgement** statement; click **OK**.

    Note: Following submission, you may have to wait up to 72 hours (3 days) to receive an email notification.

5.   Technical Support Contact Information

Contact the FFSDCS (ASP) Application Helpdesk for issues such as:

- Account unlock
- Password reset
- Registration process questions
- System availability escalations

Table 1 provides contact information for technical support.

Table 1: Technical Support Contacts

Email Address	Phone Number	Hours
ASPHelpDesk@dcca.com	1-844-876-0765	9:00 a.m. to 6:00 p.m. Eastern Standard Time (EST), Monday through Friday

Appendix A: Revision History

Table 2 provides a revision history for this document.

Table 2: Revision History

Version Number	Date	Author/Editor	Description of Change
0.1	01/22/2024	Index Analytics	DTS-ASP-Registration-UserGuide • Initial draft following collaboration between DCCA and Index Analytics and incorporation of feedback from CMS • Various font, grammatical, punctuation, shading, formatting, date, version, pagination, glossary, and alignment corrections

Appendix B: Glossary

Table 3 provides a list of terms, acronyms, and definitions in this document.

Table 3: Glossary

Expanded Form	Acronym/Term	Definition
Average Sales Price	ASP	ASP refers to the price at which an organization typically sells a certain class of good or service. CMS uses manufacturer-reported ASPs, based on manufacturers' actual quarterly drug sales, to calculate provider payment amounts for these drugs. Federal law defines the price.
Centers for Medicare & Medicaid Services	CMS	CMS is a federal agency within the U.S. Department of Health and Human Services that administers the Medicare program and works in partnership with state governments to administer Medicaid, the State Children's Health Insurance Program, and health insurance portability standards.
Chief Executive Officer	CEO	A CEO is the highest-ranking officer or Administrator in charge of management with a corporation.
Chief Financial Officer	CFO	A CFO is the corporate executive having financial authority to make appropriations and authorize expenditures for a firm.
Eastern Standard Time	EST	EST is the standard time in the 5th time zone west of Greenwich, reckoned at the 75th meridian. This time zone is in the eastern part of the United States.
Experian	NA	Experian is a global credit information group.
Fee-for-Service Data Collection System	FFSDCS	The FFSDCS is an instrument to collect cost, revenue, utilization, and other information for FFS claims.
Identity Management	IDM	IDM is the process of managing user access to data.
Interactive Voice Response	IVR	IVR is a technology that allows a computer to detect voice and DTMF keypad inputs.
Medicare	NA	Medicare is the federal system of health insurance for people over 65 years of age and for certain younger people with disabilities.
Medicare Modernization Act	MMA	The MMA, or Medicare Prescription Drug, Improvement, and Modernization Act, is a federal law.
Medicare Part B	NA	Medicare Part B is the part of Medicare that covers doctor services, outpatient hospital care, and other medical services that Part A does not cover such as physical and occupational therapy, X-rays, medical equipment, or limited ambulance service.
Multifactor Authentication	MFA	MFA is a security system that implements more than one form of authentication to verify the legitimacy of a transaction.

Expanded Form	Acronym/Term	Definition
Okta	NA	Okta is an enterprise-grade, identity management service, built for the cloud, but compatible with many on-premises applications.
One-Time Password	OTP	An OTP is a password that is valid for only one login session or transaction.
Personally Identifiable Information	PII	PII is information that identifies or describes an individual, including but not limited to name, address, telephone number, Social Security Number, credit card number, and personal characteristics that make individual identity easily discoverable.
Short Message Service	SMS	SMS is a text messaging service component of phone, web, or mobile communication systems. It uses standardized communication protocols to allow fixed-line or mobile phone devices to exchange short text messages.

Appendix C: Figures and Tables

List of Figures

List of Tables