Table of Contents

1 Introduction............................................................................................................................. 1
  1.1 What is the Clinical Laboratory Fee Schedule Data Collection System? ....................... 1
  1.2 Purpose of the CLFS Data Collection System ................................................................. 1
  1.3 CLFS User Roles.............................................................................................................. 1
  1.4 CLFS Reference Material ................................................................................................. 3

2 CLFS Data Collection System Access.................................................................................... 4
  2.1 CLFS Data Collection System Access Process ................................................................ 4
    2.1.1 Obtaining a CMS EIDM Username and Password................................................... 4
    2.1.2 Requesting CLFS Data Collection System Access .................................................. 10
    2.1.3 Adding Multi-Factor Authentication (MFA) for an Existing Account ..................... 20

3 CLFS Data Collection System Home Page .......................................................................... 30

4 Laboratory Information......................................................................................................... 32
  4.1 Add Laboratory Information .......................................................................................... 32
  4.2 Remove Laboratory Information .................................................................................... 35

5 Data Reporting...................................................................................................................... 37
  5.1 Upload Applicable Information - CLFS Submitter........................................................ 37
  5.2 Upload Applicable Information – CLFS Submitter Large Volume (LV) Role ............... 41
    5.2.1 Edit/View Data – CLFS Submitter Large Volume Role ............................................. 45
  5.3 Manual Entry – CLFS Submitter ................................................................................... 47
    5.3.1 Edit/View Data ........................................................................................................ 48

6 CLFS Certifier Registration.................................................................................................. 50
  6.1 Laboratory Information/Verify One Time Password (OTP) – CLFS Certifier.............. 50

7 Certification.......................................................................................................................... 54
  7.1 Certification – Large Volume ........................................................................................ 57

8 Help Desk.............................................................................................................................. 61

9 Frequently Asked Questions................................................................................................. 62
  9.1 General ........................................................................................................................... 62
  9.2 Supported Browsers ....................................................................................................... 62
  9.3 Personal Information ..................................................................................................... 63
  9.4 Identity Verification ....................................................................................................... 65
  9.5 Multifactor Authentication (MFA).................................................................................. 67
9.6 Annual Certification

Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1</td>
<td>CMS Portal Home Page</td>
</tr>
<tr>
<td>2-2</td>
<td>CMS Secure Portal - New User Registration Section</td>
</tr>
<tr>
<td>2-3</td>
<td>CMS Portal Terms and Conditions Page</td>
</tr>
<tr>
<td>2-4</td>
<td>CMS Your Information Page</td>
</tr>
<tr>
<td>2-5</td>
<td>CMS EIDM User ID and Password Selection</td>
</tr>
<tr>
<td>2-6</td>
<td>CMS EIDM User ID and Confirm Password</td>
</tr>
<tr>
<td>2-7</td>
<td>CMS EIDM Challenge Questions and Answers</td>
</tr>
<tr>
<td>2-8</td>
<td>CMS Portal Registration Complete</td>
</tr>
<tr>
<td>2-9</td>
<td>CMS Portal Home Page</td>
</tr>
<tr>
<td>2-10</td>
<td>CMS Secure Portal – Login to CMS Secure Portal Section</td>
</tr>
<tr>
<td>2-11</td>
<td>CMS Portal Terms and Conditions Page</td>
</tr>
<tr>
<td>2-12</td>
<td>CMS Portal Log In Page</td>
</tr>
<tr>
<td>2-13</td>
<td>CMS Portal Password Page</td>
</tr>
<tr>
<td>2-14</td>
<td>CMS Portal Home Page</td>
</tr>
<tr>
<td>2-15</td>
<td>Request Application Access Now Button</td>
</tr>
<tr>
<td>2-16</td>
<td>Access Catalog Page</td>
</tr>
<tr>
<td>2-17</td>
<td>Request New System Access – System Description and Role Page</td>
</tr>
<tr>
<td>2-18</td>
<td>Request New System Access – TIN and Notes to Approver Page</td>
</tr>
<tr>
<td>2-19</td>
<td>Identity Verification Page</td>
</tr>
<tr>
<td>2-20</td>
<td>Terms and Conditions</td>
</tr>
<tr>
<td>2-21</td>
<td>Your Information Page</td>
</tr>
<tr>
<td>2-22</td>
<td>Register Your Phone, Computer, or E-mail Page</td>
</tr>
<tr>
<td>2-23</td>
<td>Register Your Phone, Computer, or E-mail – Confirmation Page</td>
</tr>
<tr>
<td>2-24</td>
<td>Request Acknowledgement Page</td>
</tr>
<tr>
<td>2-25</td>
<td>Pending Requests Page</td>
</tr>
<tr>
<td>2-26</td>
<td>CMS Portal Home Page</td>
</tr>
<tr>
<td>2-27</td>
<td>Terms and Conditions</td>
</tr>
<tr>
<td>2-28</td>
<td>CMS Portal Log In – User ID Page</td>
</tr>
<tr>
<td>2-29</td>
<td>CMS Portal – Register MFA Device</td>
</tr>
<tr>
<td>2-30</td>
<td>Register MFA Device Pop-up Window</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2-31</td>
<td>Terms and Conditions</td>
</tr>
<tr>
<td>2-32</td>
<td>CMS Portal Log In – User ID and Password Page</td>
</tr>
<tr>
<td>2-33</td>
<td>Security Questions</td>
</tr>
<tr>
<td>2-34</td>
<td>MFA Registration</td>
</tr>
<tr>
<td>2-35</td>
<td>MFA Registration - Confirmation</td>
</tr>
<tr>
<td>2-36</td>
<td>Request Acknowledgement Page</td>
</tr>
<tr>
<td>2-37</td>
<td>Pending Requests Page</td>
</tr>
<tr>
<td>3-1</td>
<td>CLFS Data Collection System Home Page - CLFS Submitter</td>
</tr>
<tr>
<td>3-2</td>
<td>CLFS Data Collection System Home Page - CLFS Certifier</td>
</tr>
<tr>
<td>4-1</td>
<td>Laboratory Information Page</td>
</tr>
<tr>
<td>4-2</td>
<td>Laboratory Information – Laboratory Information Saved Page</td>
</tr>
<tr>
<td>4-3</td>
<td>Laboratory Information – Registering an Additional TIN</td>
</tr>
<tr>
<td>4-4</td>
<td>Laboratory Information – Additional TIN Registered</td>
</tr>
<tr>
<td>4-5</td>
<td>Laboratory Information – Generated OTP Page</td>
</tr>
<tr>
<td>4-6</td>
<td>Laboratory Information Page</td>
</tr>
<tr>
<td>4-7</td>
<td>Removed NPI and/or CCN</td>
</tr>
<tr>
<td>4-8</td>
<td>Laboratory Information Saved with Selected NPI and/or CCN Removed</td>
</tr>
<tr>
<td>5-1</td>
<td>Upload Applicable Information Page</td>
</tr>
<tr>
<td>5-2</td>
<td>File Directory Window</td>
</tr>
<tr>
<td>5-3</td>
<td>Filename Window</td>
</tr>
<tr>
<td>5-4</td>
<td>Browse Window</td>
</tr>
<tr>
<td>5-5</td>
<td>Uploaded Data Page - Normal</td>
</tr>
<tr>
<td>5-6</td>
<td>Uploaded Applicable Information – Data Removal</td>
</tr>
<tr>
<td>5-7</td>
<td>Uploaded Applicable Information – Data Removed</td>
</tr>
<tr>
<td>5-8</td>
<td>Upload Applicable Information Page - LV</td>
</tr>
<tr>
<td>5-9</td>
<td>File Directory Window - LV</td>
</tr>
<tr>
<td>5-10</td>
<td>Filename Window - LV</td>
</tr>
<tr>
<td>5-11</td>
<td>Browse Window - LV</td>
</tr>
<tr>
<td>5-12</td>
<td>Large Volume Message Display</td>
</tr>
<tr>
<td>5-13</td>
<td>Large Volume Data Saved</td>
</tr>
<tr>
<td>5-14</td>
<td>Edit/View Large Volume Page</td>
</tr>
<tr>
<td>5-15</td>
<td>TIN Removal Pop-Up</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 What is the Clinical Laboratory Fee Schedule Data Collection System?

The Protecting Access to Medicare Act of 2014 (PAMA), requires significant changes to how Medicare calculates payment rates for clinical diagnostic laboratory tests (CDLTs) under the Medicare Part B Clinical Laboratory Fee Schedule (CLFS). Beginning January 1, 2018, private payor rates from applicable laboratories will be the basis for the revised CLFS.

The CLFS Data Collection System collects information from applicable laboratories that is used to calculate payment rates for laboratory tests paid on the CLFS. Applicable laboratories, through their reporting entity, must use the CLFS data collection system to submit and certify applicable information, that is, private payor rate data, to the Centers for Medicare & Medicaid Services (CMS).

This document provides guidance that will assist users during the completion of the following processes:

- Register as a CLFS Submitter and CLFS Certifier
- Report Applicable Information
- Certify Reported Applicable Information

1.2 Purpose of the CLFS Data Collection System

The CLFS data collection system is a component of the Fee-for-Service Data Collection System. The CLFS data collection system accepts applicable information from applicable laboratories. The data are validated, stored, and used to calculate payment rates for laboratory tests paid on the CLFS.

The CLFS data collection system supports the following business processes:

- CLFS User Registration
- CLFS Applicable Laboratory Data Reporting
- CLFS Applicable Laboratory Data Certification

The following high-level business requirements for CLFS are implemented:

- Applicable Laboratories through their reporting entity shall report applicable information to CMS
- The CLFS data collection system shall identify consistency errors found in submitted data

1.3 CLFS User Roles

The CLFS data collection system is a role-based system. This means that certain system functions have been linked to specific “user role profiles.” When a new user is given access to
the CLFS data collection system, a CLFS role is approved that provides access to the specific functions they need.

- **CLFS Submitter:** An individual of the Applicable Laboratory who is appointed as data submitter who submits applicable laboratory data through approved file uploads or manual data entry into the CLFS data collection system. The submitter may submit for multiple TINs and will generate a One-Time Password (OTP) for all of the TINs to be registered to be shared with the Data Certifier.

This role’s objective is for the user to report applicable CDLT and ADLT information to CMS once every 3 years for CDLTs and annually for ADLTs. Below are areas of the CLFS data collection system for which the CLFS Submitter role has access:

- **Applicable Laboratory Registration**
  - Requires submission of: Laboratory Name, TIN(s), National Provider Identifier (NPI), and CMS Certification Number (CCN) or Provider Transaction Access Number (PTAN)
  - The CLFS Submitter’s name must match either the Authorized Official name in CMS PECOS or another designed role available in PECOS
  - One Time Password (OTP): User must generate an OTP for all of the TINs to be registered, and share this with the CLFS Certifier so that they can successfully complete their registration

- **Data upload**
  - **CLFS Data Reporting Template:** This Comma-Separated Values (.csv) template provides specific data transmission fields for upload into the CLFS data collection system. The .csv file is a pre-defined template (i.e. upload via excel or text file)
  - Upload Data: Best option for laboratories submitting a large amount of data
  - Manual Entry: Best option for laboratories with only a few Healthcare Common Procedure Coding System (HCPCS) codes to submit

- **Status:** Status of the applicable information submitted can be found via the “Edit/View Data” page

- **Validation:** Validation is performed for all data submitted. Specific validation rules can be found in Section 5.

- **Corrections**

- **CLFS Certifier:** A President or Chief Financial Officer (CFO) of the applicable laboratory, or an individual appointed as data certifier who certifies the accuracy and completeness of applicable information submitted to CMS.

  - Registration: Must receive an OTP from CLFS Submitter to complete registration for all TINs to be registered
Certifies data
- Reviews Data; cannot make edits to data
- If changes are necessary, CLFS Certifier must inform data CLFS Submitter; data CLFS Submitter to make any edits
- Once data are certified, they cannot be viewed or updated by the laboratory

1.4 CLFS Reference Material

The following additional reference materials are utilized in order to successfully submit and certify applicable data into the CLFS data collection system:

- **EIDM User Guide**
- **CLFS Data Reporting Template**
- **Contextual Help**

Click on **EIDM Links** for any assistance with using the system and to view applicable videos.
2 CLFS Data Collection System Access

Users are required to access the CMS Portal at https://portal.cms.gov to begin the registration and role assignment process.

CMS has established the Enterprise Identity Management (EIDM) system to provide our Business Partners with a means to apply for, obtain approval, and receive a single User ID they can use to access one or more CMS applications. The EIDM Authentication System will prompt the user to create a username and password that conforms to the system’s policies; this user ID and password is not affiliated with the user’s CMS User ID (Enterprise User Administration [EUA]) and password. After the user successfully creates a username and password, the user must create security questions and answers. The user must then re-log in with the new credentials and request the specific FFSDCS CLFS Submitter or CLFS Certifier role as applicable. As part of the role request process the EIDM Authentication System will begin the identity proofing process. After the user’s identity is verified, the CMS Portal will push the user’s data to CM to review the role request and approve it. For additional details on EIDM, review the EIDM User Guide.

2.1 CLFS Data Collection System Access Process

CLFS users with an existing CMS EIDM username and password can skip Section 2.1.1 and continue on to Section 2.1.2, Requesting CLFS data collection system Access.

2.1.1 Obtaining a CMS EIDM Username and Password

A CMS EIDM username and password are required in order to access the CLFS data collection system. Perform the following steps in order to receive the required credentials:

1. Access the CMS Portal by entering the following Uniform Resource Locator (URL) into your browser: https://portal.cms.gov.
   
   The CMS Portal Home Page is shown in Figure 2-1.
The CMS Secure Portal section is located in the top-right section of the CMS Portal Home Page as shown in Figure 2-2.

2. Click on the “New User Registration” link.
   
   The “Terms and Conditions” page opens, as shown in Figure 2-3.
Note: Read through the Terms and Conditions on the page. The page states that you consent to monitoring while accessing and using this website. The page also details the reasons for collecting Personal Identifiable Information (PII), which are that it will only be used to uniquely identify the new user who is registering with the system. The page provides links to the HHS Rules of Behavior and the CMS Privacy Act Statement.

3. If you agree to the terms and conditions, click the corresponding check box and click on the Next button.

Note: Users must agree to the terms and conditions to continue the registration process.

The “Your Information” page opens, as shown in Figure 2-4.
4. Enter your personal information in the required fields which are indicated by an asterisk. (the additional fields are optional, but may be required for further identity verification) and click on the **Next** button.

The “CMS EIDM User ID and Password Selection” page displays as shown in Figure 2-5.
5. Enter your desired User ID in the “User ID” field. The User ID must be a minimum of 6 and a maximum of 74 alphanumeric characters. Allowed special characters are dashes (-), underscores (_), apostrophes (‘), @ and periods (.).

6. Enter your desired password in the “Password” field. The CMS Portal password must conform to the following CMS Acceptable Risk Safeguards (ARS) Password Policy:
   a. Be changed at least every sixty (60) days;
   b. Be a minimum of eight (8) and a maximum of twenty (20) characters;
   c. Be changed only once a day;
   d. Contain at least one (1) letter and one (1) number;
   e. Contain at least one (1) uppercase and one (1) lowercase letter;
   f. Not contain your User ID; and
   g. Be different from your previous six (6) passwords.

7. Re-enter your desired password in the “Confirm Password” field.
   Note: The passwords must match before you can continue.

The password fields populate as shown in Figure 2-6.
8. Select a Challenge Question from each of the three (3) drop-down lists for which the answer is known.

9. Enter the answers to the Challenge Questions in the corresponding “Answer” fields. The special characters that are allowed are apostrophes (‘), hyphens (-), and spaces followed by alphanumeric characters.

The files populate as shown in Figure 2-7.

Figure 2-7: CMS EIDM Challenge Questions and Answers

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

    Note: You may click on the **Cancel** button to exit out of the registration process. New information or changes entered will not be saved.

    The “Registration Complete” screen displays as shown in Figure 2-8.
11. Click on the **OK** button to return to the CMS Portal Home Page. Please wait at least 5 minutes before logging on to the CMS Portal with your new EIDM user ID and password.

### 2.1.2 Requesting CLFS Data Collection System Access

Perform the following steps to request access to the CLFS data collection system:

1. Enter the address for the CMS portal ([https://portal.cms.gov](https://portal.cms.gov)) into your web browser and click on the **Enter** button.

The CMS Portal Home Page opens as shown in Figure 2-9.

**Figure 2-9: CMS Portal Home Page**

The CMS Secure Portal section is located in the top-right section of the CMS Portal Home Page as shown in Figure 2-10.

**Figure 2-10: CMS Secure Portal Section**
2. Click on the “Login to CMS Secure Portal” link.
   The “Terms and Conditions” page opens, as shown in Figure 2-11.

3. Read through the terms and conditions on the page. The page states that you consent to monitoring while accessing and using this website. If you agree to the terms and conditions, click on the I Accept button. Users must agree to the terms and conditions to continue the log-in process.
   The “CMS Portal Log In” page opens as shown in Figure 2-12.
4. Enter your EIDM user ID and click on the Next button. The system requests a password as shown in Figure 2-13.

**Figure 2-13: CMS Portal Password Page**

5. Enter your password and click on the Log In button. The CMS Portal Home Page opens as shown in Figure 2-14.
6. Click on the Request Access Now button on the CMS Portal Home Page, as shown in Figure 2-15.

The “Access Catalog” page opens as shown in Figure 2-16.
7. Click on the **Request Access** button in the “FFSDCS” section (The CLFS data collection system is part of the Fee-for-Service Data Collection System [FFSDCS]).

The “Request New System Access” page opens as shown in Figure 2-17.
8. Click on the down-arrow next to the “System Description” drop-down box and select *FFSDCS – Fee for Service Data Collection System*. Then click on the down-arrow next to the “Role” drop-down box, select the applicable role (CLFS Submitter or CLFS Certifier).

The page expands for you to enter the TIN that you will be registering, and any notes to the Approver for that same TIN, as shown in Figure 2-18. If you plan to report for multiple TINs, enter one of the TINs for which you will be reporting and make note of that TIN; you will need it later on when registering your laboratory in the CLFS data collection system. You will be able to register all of your TINs once you are within the CLFS application.
9. Enter your TIN, make any notes to the Approver, and click on the Submit button.

The “Identity Verification” page opens, as shown in Figure 2-19.

10. The “Identity Verification” page describes how your personal information will be used to verify your identity before being assigned to the selected role. CMS uses Experian as an external identity provider. Experian uses information from your credit report to assist with confirming your identity. The Experian system will pose questions to you based on the data in your report. Read the “Identity Verification” page carefully, and click on the Next button to proceed.

The “Terms and Conditions” page opens, as shown in Figure 2-20.
11. Read through the Terms and Conditions on the page. The page states that you consent to monitoring while accessing and using this website. The page also details the reasons for collecting PII, which are that it will only be used to uniquely identify the new user who is registering with the system. The page provides links to the HHS Rules of Behavior and the CMS Privacy Act Statement. If you agree to the terms and conditions, click the corresponding check box and click on the Next button.

The “Your Information” page opens with the previously entered information pre-populated, as shown in Figure 2-21.
12. Enter any missing required information in the fields and click on the **Next** button. A page will open that will ask you a series of questions to verify your identity. These questions are generated from the information in your credit report.

Answer the questions and click on the **Next** button. Your identity will be verified based on your answers. Once your identity has been verified, you will be asked to register your second factor authentication token such as phone, computer, or e-mail, as shown in Figure 2-22.
13. Select a Multi-Factor Authentication (MFA) to register by clicking on the down-arrow in the “MFA Device Type” field, complete any information requested depending on the device chosen, and click on the **Next** button.

A message displays confirming registration of your MFA device, as shown in Figure 2-23.

**Figure 2-23: Register Your Phone, Computer, or E-mail – Confirmation Page**

14. Click on the **OK** button.

A message displays confirming the receipt of your request as shown in Figure 2-24.

**Figure 2-24: Request Acknowledgement Page**

15. Click on the **OK** button.

A Pending Requests window displays showing any pending requests, as shown in Figure 2-25.
Note: After submitting a request, please wait until up to 72 hours for an e-mail notification before using the system.

16. You will now be able to access the FFSDCS CLFS data collection system using the CMS Portal. The FFSDCS CLFS data collection system is accessed using a link that is displayed on the main navigation menu.

2.1.3 Adding Multi-Factor Authentication (MFA) for an Existing Account

MFA is a security mechanism that is implemented to verify the legitimacy of a person or transaction.

MFA is an approach to security authentication which requires users to provide more than one form of verification in order to prove their identity. MFA registration is required only once when you are requesting a user role, but will be verified every time you log into the CMS Enterprise Portal.

Registered CMS.gov Enterprise Portal users with an existing account, who wish to access a CMS MFA protected application, will be directed through the MFA registration process. During the MFA registration process, the CMS.gov Enterprise Portal requires registration of a phone, computer, or e-mail to add an additional level of security to a user’s account. The user is given five options to select from to complete the registration process. The same steps can be followed to register multiple MFA devices.

Depending on the MFA option you choose to register, you may need access to download and install software on your computer/phone; your phone should be able to receive text messaging (Short Message Service [SMS]); or you should have a valid e-mail address.
Users who already have an active CMS.gov Enterprise Portal account and a role in FFSDCS can register for EIDM Multi-Factor Authentication (MFA), remove a registered MFA device, and log in with Multi-Factor Authentication when accessing an application resource/URL that is MFA protected.


   Note: The CMS Enterprise Portal supports the following internet browsers:
   - Internet Explorer 8
   - Internet Explorer 9
   - Mozilla – Firefox
   - Chrome
   - Safari

   *Enable JavaScript and adjust any zoom features to ensure you are not seeing the screen in too wide of a view.*

   The CMS Portal Home Page opens as shown in Figure 2-26.

   **Figure 2-26: CMS Portal Home Page**

2. Click *Login to CMS Secure Portal* on the CMS Enterprise Portal.

   The “Terms and Conditions” page opens, as shown in Figure 2-27.
3. Read through the Terms and Conditions on the page. The page states that you consent to monitoring while accessing and using this website. If you agree to the terms and conditions, click on the **I Accept** button. Users must agree to the terms and conditions to continue the log-in process.

The “CMS Portal Log In – User ID” page opens as shown in Figure 2-28.
4. Enter your EIDM user ID and click on the **Next** button.

The “CMS Portal – Register MFA Device” page opens as shown in Figure 2-29.
5. Click on the “Register MFA Device” link.

A “Register MFA Device” pop-up window displays requesting confirmation that you want to navigate away from the login page, as shown in Figure 2-30.
6. Click on the OK button.

The “Terms and Conditions” page opens, as shown in Figure 2-31.

Figure 2-31: Terms and Conditions

7. Read through the Terms and Conditions on the page. The page states that you consent to monitoring while accessing and using this website. If you agree to the terms and conditions, click on the I Accept button. Users must agree to the terms and conditions to continue the log-in process.

The “CMS Portal Log In – User ID and Password” page opens as shown in Figure 2-32.
8. Enter your User ID and Password, and click on the **Log In** button. The “Security Questions” page opens as shown in Figure 2-33.

![Security Questions](image)

Figure 2-33: Security Questions
9. Enter the answers to your security questions, and click on the **Next** button.

The “MFA Registration” page opens as shown in Figure 2-34.

**Figure 2-34: MFA Registration**

![MFA Registration](image)

10. Select an MFA to register by clicking on the down-arrow in the “MFA Device Type” field, complete any information requested depending on the device chosen, and click on the **Next** button.

A message displays confirming registration of your MFA device, as shown in Figure 2-35.
11. Click on the OK button.

A message displays confirming the receipt of your request as shown in Figure 2-36.

Figure 2-36: Request Acknowledgement Page

12. Click on the OK button.

A Pending Requests window displays showing any pending requests, as shown in Figure 2-37.

Figure 2-37: Pending Requests Page
Note: After submitting a request, wait until up until 72 hours for an e-mail notification before using the system.
3 CLFS Data Collection System Home Page

The CLFS data collection system is comprised of numerous pages and pop-up windows to allow applicable laboratories to report and certify applicable information. The fields displayed on each page differ based on the type of user logged in and the privileges assigned to the user role for the logged in user. The user can enter data into the fields in the CLFS data collection system unless the field is displayed with a gray background.

If the user is new to the system, the user will be placed immediately into the Laboratory Information page to register his or her laboratory information with the CLFS data collection system. If the user has already registered, the user will be placed directly onto Data Collection page (for a CLFS Submitter role) or Certification page (for a CLFS Certifier role).

The CLFS data collection system Home Page displays content based on user role and the privileges assigned to the user role. The CLFS data collection system Home Page Welcome Screen is shown in Figure 3-1 for CLFS Submitters, and Figure 3-2 CLFS Certifiers.

Figure 3-1: CLFS Data Collection System Home Page - CLFS Submitter
Figure 3-2: CLFS Data Collection System Home Page - CLFS Certifier

What is the Clinical Laboratory Fee Schedule Data Collection System?

The Medicare Access to Medicare Act (MAA) requires significant changes to how Medicare pays for clinical laboratory tests (CLTs) under the Medicare Part E Clinical Laboratory Fee Schedule (CLFS). Beginning January 1, 2012, Medicare payment rates for applicable laboratories will be the basis for the Medicaid CLFS.

The CLFS data collection system requires information from applicable laboratories that is used to calculate payments for laboratory tests under the CLFS. Applicable laboratories file their data electronically through an intermediary, such as a MAC, to enter in their report forms. The intermediary then sends the information to CMS to calculate payment rates for applicable tests paid on the CLFS.

Purpose of the CLFS Data Collection System

The CLFS data collection system accepts appropriate information from applicable laboratories. The data are validated, coded, and used to calculate payment rates for laboratory tests paid on the CLFS.

CLFS User Notes

CLFS User Notes include all applicable laboratories who are assigned as data submitter. The applicable laboratories submit data through approved data submitters or manual data entry into the CLFS data collection system. GSTs are also responsible for submitting applicable laboratories, or an individual appointed as a data submitter in the CLFS data collection system. The beneficiary's accuracy and completeness of applicable information submitted to the CLFS.

CLFS Reference Material

The following reference materials are available to prepare successfully submit and enter applicable data into the CLFS data collection system:

- CLFS User Guide
- CLFS User Manual
- EHR Manual
- CLFS Data Entry Manual
- Physician Data Entry Manual
- Data User Guide

CLFS Data Collection System Home Page
4 Laboratory Information

4.1 Add Laboratory Information

The following steps are to be used to enter data into the CLFS data collection system as a CLFS Submitter:

1. Log in to CLFS as CLFS Submitter to open the “Laboratory Information” page.

   The “Laboratory Information” page displays as shown in Figure 4-1.

   **Figure 4-1: Laboratory Information Page**

   ![Figure 4-1: Laboratory Information Page]

2. Enter the following:

   - TIN (use the same TIN entered when completing EIDM registration (see Section 2.1.2, Step 8)
   - Laboratory Name
     - One CLFS Submitter and One CLFS Certifier per TIN is allowed
     - A Submitter may be registered for multiple TINs
   - TIN type (either Employer Identification Number [EIN] or Other).
   - NPI and click on the **add** button
   - CCN, select type of CCN from drop-down list, and click on the **add** button

3. Click on the **Save** button.

   A message appears stating that the laboratory has been saved successfully, as shown in Figure 4-2.
4. To register a new TIN, select “Register new TIN” from the TIN drop-down list, and enter a new TIN, Lab name, NPI, and CCN type.

The data for the new TIN populates as shown in Figure 4-3.

Figure 4-3: Laboratory Information – Registering an Additional TIN

5. Click on the Save button,

A message displays that the laboratory information has been saved, and the drop-down list displays a list with the new TIN added, as shown in Figure 4-4.
6. When it is known who the CLFS Certifier for the same reporting TIN(s) will be, generate an OTP to provide to the CLFS Certifier in your organization to complete registration. This is done by clicking on the **Generate One Time Password (OTP)** button.

   The system displays the OTP, which will be valid for 7 days as shown in Figure 4-5.

   **Figure 4-5: Laboratory Information – Generated OTP Page**

7. Copy the OTP and share it to the person assigned to be the CLFS Certifier.

   Note: If an additional TIN is registered after an OTP has been generated, use the same OTP to the newly registered TIN(s). The same OTP applies to all registered TINs. The CLFS Submitter does not need to create a separate OTP for each TIN.
4.2 Remove Laboratory Information

The following steps are to be used to remove data from the CLFS data collection system as a CLFS Submitter:

1. Log in to CLFS as CLFS Submitter to open the “Laboratory Information” page.
   The “Laboratory Information” page displays as shown in Figure 4-6.

   **Figure 4-6: Laboratory Information Page**

2. To remove an NPI and/or CCN, select an NPI and/or CCN from the list box and click on the **remove** button.
   Note: At least one NPI or CCN must remain in the list.

   The list box refreshes and the selected NPI and/or CCN are removed from the list, as shown in Figure 4-7.
3. Click on the **Save** button.

A message displays stating that the laboratory information has been saved, as shown in Figure 4-8.

**Figure 4-8: Laboratory Information Saved with Selected NPI and/or CCN Removed**
5 Data Reporting

Applicable laboratories are required to report applicable information to the CLFS data collection system using a file transfer process or through manual online data entry. The following sections detail the steps required to submit applicable laboratory data using file uploads and manual online data entry.

5.1 Upload Applicable Information - CLFS Submitter

The CLFS data collection system provides applicable laboratories the ability to report applicable information to CMS using a file transfer process. Perform the following steps to enter data using the upload process:

1. Log in as CLFS Submitter and click on Data Reporting and then click on Upload Applicable Information.

The “Upload Applicable Information” page displays as shown in Figure 5-1.

![Figure 5-1: Upload Applicable Information Page](image)

At the top center of the page is a link to the data reporting template that could be used to enter data in .csv format. Previous upload submissions will be displayed at the upper portion of the page. Only one file per TIN can be uploaded.

Note: Template Requirements

- You may change the filename
- Do not add additional columns to the template
- Do not add, remove, or otherwise change columns or column headings within the template
- Do not submit blank rows between data entries
You must submit all data in contiguous rows

Enter the HCPCS Code, Payment Rate, Volume, and NPI. The basic edits for the data items are:

a. HCPCS Code: alphanumeric or all numeric
   5 characters
b. Payment Rate: numeric
   not a negative value
   99999.99 format
c. Volume: numeric
   not a negative value
   can be zero
   no decimal places
d. NPI: numeric
   10 digits fixed
   no decimal places
   cannot have 5 consecutive same digits
   must pass Luhn check digit formula

2. To upload the data, click on the **Browse...** button.
   The file directory window displays as shown in Figure 5-2.

   **Figure 5-2: File Directory Window**

   ![File directory window](image)

3. Select the directory path and filename to upload.
   The filename appears in the “File name” window as shown in Figure 5-3.

   **Figure 5-3: Filename Window**

   ![Filename window](image)

4. Click on the **Open** button.
   The filename appears in the “Browse” window as shown in Figure 5-4.
5. Click on the **Upload Data** button.

The “Refresh” button can be clicked when an upload is taking awhile to process to see if the upload is still processing or completed. Multiple uploads are allowed. Duplicate data is also allowed if applicable, please use caution to ensure that all data that appears to be duplicated is legitimate. After the upload process has completed, the results will be displayed at the bottom of the screen.

Note: If the status returns a result of “ERROR,” click on the link in the “Filename” column to receive the description of the error in your database.

Note:

- If the file being uploaded is greater than 3,400,183 bytes, but less than 29,360,128 bytes, it is considered a Large Volume (LV) file. Once an LV file is uploaded your role will be modified to an LV Submitter. For further instructions on how to Upload, Edit, or Delete data for LV files, please refer to sections 5.2 and 5.2.1.

A message will display stating “A Large Volume file is detected and will be submitted tonight after business hours. The results of this upload will be available tomorrow, please review the results then.”

The data from the uploaded data template displays on the screen as shown in Figure 5-5.
Data can be sorted in HCPCS code order in ascending or descending order as well as the “NPI” and “Result” fields (can be used when locating errors). The data can be viewed using the scroll features. If there is at least one validation error on the entire file, none of the data is saved. The data is only saved when the entire file has no validation errors. The “Result” field will give the details of the data validation errors(s). All of the records that pass validation will have the message # of # lab submission data saved. In the “Result” field, when all of the data has passed validation, each entry will have the message Saved.

6. To remove an uploaded and saved file, click on the box in the Removed column, as shown in Figure 5-6.

Figure 5-6: Uploaded Applicable Information – Data Removal
7. The selected file to be removed automatically disappears from the list and a message displays stating that the data have been removed, as shown in Figure 5-7.

Figure 5-7: Uploaded Applicable Information – Data Removed

5.2 Upload Applicable Information – CLFS Submitter Large Volume (LV) Role

The CLFS data collection system provides applicable laboratories the ability to report applicable information to CMS using a file transfer process. If the file being uploaded is greater than 3,400,183 bytes, but less than 29,360,128 bytes, it is considered an LV file. Once an LV file is uploaded your role will be modified to a LV Submitter. Perform the following steps to enter data using the upload process:

1. Log in as CLFS Submitter and click on **Data Reporting** and then click on **Upload Applicable Information**.

   The “Upload Applicable Information” page displays as shown in Figure 5-8.
At the top center of the page is a link to the data reporting template that could be used to enter data in .csv format. Previous upload submissions will be displayed at the upper portion of the page.

Note: Template Requirements

- You may change the filename
- Do not add additional columns to the template
- Do not add, remove, or otherwise change columns or column headings within the template
- Do not submit blank rows between data entries
- You must submit all data in contiguous rows
- Enter the HCPCS Code, Payment Rate, Volume, and NPI. The basic edits for the data items are:
  a. HCPCS Code: alphanumeric or all numeric
     5 characters
  b. Payment Rate: numeric
     not a negative value
     99999.99 format
  c. Volume: numeric
     not a negative value
     can be zero
     no decimal places
     up to 6 digits
d. NPI: numeric
   10 digits fixed
   no decimal places
   cannot have 5 consecutive same digits
   must pass Luhn check digit formula

The Refresh button is used when a submission is taking an extended period of time to process. By clicking on the Refresh button, the User can see if the file upload is still processing or completed.

2. To upload the data, click on the Browse… button.
   The file directory window displays as shown in Figure 5-9.

   **Figure 5-9: File Directory Window - LV**

3. Select the directory path and filename to upload.
   The filename appears in the “File name” window as shown in Figure 5-10

   **Figure 5-10: Filename Window - LV**

4. Click on the Open button.
   The filename appears in the “Browse” window as shown in Figure 5-11
5. Click on the **Upload Data** button.

The file to upload displays with the Status as “Scheduled” and a message displays stating that an LV file has been detected and will be available tomorrow, as shown in Figure 5-12.

![Figure 5-12: Large Volume Message Display](image)

6. To know when the file has been saved, click on the **Refresh** button.

The file to upload displays with the Status as “SAVED”, as shown in Figure 5-13.
5.2.1 Edit/View Data – CLFS Submitter Large Volume Role

The CLFS system provides applicable laboratories the ability to edit information to CMS. Perform the following steps to edit data.

1. Log in as CLFS Submitter and click on Edit/View Data.
   The “Edit/View Data” window displays as shown in Figure 5-14.

   ![Figure 5-14: Large Volume Edit/View Page](image)

2. To edit data, click the file link in the “Download” section, and edit change the information in the .csv file. The basic edits for the data items are:
   a. HCPCS Code: alphanumeric or all numeric
      5 characters
   b. Payment Rate: numeric
      not a negative value
      99999.99 format
c. Volume: numeric
   - not a negative value
   - can be zero
   - no decimal places
   - up to 6 digits

d. NPI: numeric
   - 10 digits fixed
   - no decimal places
   - cannot have 5 consecutive same digits
   - must pass Luhn check digit formula

3. Click on “Data Reporting” from the menu on the left side of the screen, click on “Upload Applicable Information,” and re-upload your file.

4. To remove a file, click on the **Remove** button next to the applicable file.

5. To remove all of the files, click on the **Remove All Files** button.
   A pop-up box displays asking if you are sure you want to remove all of the files for the selected TIN as shown in Figure 5-15.

   **Figure 5-15: TIN Removal Pop-Up**

   ![TIN Removal Pop-Up](image)

6. Click on the **Ok** button.

   All of the files are removed for the selected TIN as shown in Figure 5-16.

   **Figure 5-16: Edit/View Page with TIN Removed**

   ![Edit/View Page with TIN Removed](image)
5.3 Manual Entry – CLFS Submitter

The CLFS data collection system provides applicable laboratories the ability to report applicable information to CMS using manual key-in entry of data. Perform the following steps to enter data using the manual data entry process.

1. Log in as CLFS Submitter, click on **Data Reporting** from the left side of the screen, and then click on **Manual Entry Applicable Information**.

   The “Manual Entry Applicable Information” page displays as shown in Figure 5-17.

   ![Figure 5-17: Manual Entry Applicable Information Page](image)

   Note: If multiple TINs are registered, select a TIN from the “Lab TIN:” dropdown list.

2. Enter the HCPCS Code, Payment Rate, Volume, and NPI.

   The basic edits for the data items are:

   a. **HCPCS Code**: alphanumeric or all numeric
      5 characters
   b. **Payment Rate**: numeric
      not a negative value
      99999.99 format
   c. **Volume**: numeric
      not a negative value
      can be zero
      no decimal places
   d. **NPI**: numeric
      10 digits fixed
      no decimal places
      cannot have 5 consecutive same digits
      must pass Luhn check digit formula

3. Click on the **Save** button.

   The screen displays the confirmation that the data have been successfully saved with further instructions, either to have the CLFS Certifier certify the data or to go to the “Edit/View Data” screen to change data, as shown in Figure 5-18. If there are validation errors, the system will display an error message at the field in error.
5.3.1 Edit/View Data

The CLFS system provides applicable laboratories the ability to edit information to CMS. Perform the following steps to edit data.

1. Log in as CLFS Submitter and click on **Edit/View Data**.

   The “Edit/View Data” window displays as shown in Figure 5-19.

   **Figure 5-19: Manual Entry-Edit/View Data Page**

2. The data can be sorted in ascending or descending order clicking on any of the headers. Click on the header once for ascending order, click again for descending order.

   The system will show how many records there are.

3. To edit data, click in any of the fields and change the information. The basic edits for the data items are:
   
   a. HCPCS Code: alphanumeric or all numeric
      
      5 characters
   
   b. Payment Rate: numeric
      
      not a negative value
      
      99999.99 format
c. Volume: numeric
   not a negative value
   can be zero
   no decimal places

d. NPI: numeric
   10 digits fixed
   no decimal places
   cannot have 5 consecutive same digits
   must pass Luhn check digit formula

The system displays the change made in the field and a message displays stating that the data needs to be certified.

If there are any data entries that need to be removed, the user can click on the X box under the “Remove” column. If all of the data entries need to be removed, the user can click on the “Remove All” button, as shown in Figure 5-20.

Figure 5-20: Manual Entry-Edit Data Confirmation
6 CLFS Certifier Registration

6.1 Laboratory Information/Verify One Time Password (OTP) – CLFS Certifier

To verify the relationship between the CLFS Submitter and the Certifier, a CLFS Certifier must enter the applicable information and the OTP sent to them by the CLFS Submitter.

1. CLFS Certifier logs into the system.
   The “Laboratory Information” screen displays as shown in Figure 6-1.

   **Figure 6-1: Certifier - Laboratory Information Window**

2. Enter the following fields:
   a. TIN(s) provided by the CLFS Submitter
   b. Lab Name (Optional)
   c. The OTP provided by the CLFS Submitter for all TINS.
3. Click on the **Verify** button to verify the OTP.
   A verification message that the OTP has been certified displays as shown in Figure 6-2.
To add another TIN to certify, select “Register new TIN” from the TIN drop-down menu as shown in Figure 6-3.

5. Enter the following fields:
   a. TIN
   b. The OTP provided by the CLFS Submitter

6. Click on the **Verify** button to verify the OTP.

A verification message that the OTP has been verified displays, as shown in Figure 6-4.
7. To remove a TIN select a TIN from the TIN drop-down menu, as shown in Figure 6-5.

Figure 6-5: Laboratory Information – TIN to be Removed

7. Click on the Remove TIN button.

A verification message displays stating that the selected TIN has been successfully removed, and the dropdown list no longer contains the removed TIN, as shown in Figure 6-6.
Figure 6-6: Laboratory Information – Selected TIN Removed Message
7 Certification

Data certification is a process where an applicable laboratory representative (CLFS Certifier) certifies the accuracy of the data. The CLFS Certifier must certify all data items pending certification. The CLFS certifier cannot make any edits to the data. If the CLFS certifier identifies a need to edit data, this must be completed by the CLFS submitter.

1. CLFS Certifier logs and clicks on “Certification” from the left side of the screen. The “Certification” window displays as shown in Figure 7-1.

   Figure 7-1: Certification Window

2. Select a TIN from the drop-down box. The data for the selected TIN display as shown in Figure 7-2.

   Figure 7-2: Selected TIN Data to be Certified

3. Click on the Certify All button. A “Data Certification Statement” pop-up window displays as shown in Figure 7-3.
4. Review the statement, click in the box next to “I agree to the above certification statement,” and then click on the **Certify** button.

Note: The system will display a message “All data records are certified. Certification has been completed and closed for this reporting period.”

All of the “Results” for the data changes are changed from being “SAVED” to “CERTIFIED” as shown in Figure 7-4.

**Figure 7-4: Certification - Data Certified Window**

**Warning:** Once the CLFS Certifier has certified the data for the current period, data submission is closed and no more data can be entered for that TIN. Be sure that all applicable information is entered, accurate, and complete before certifying the data. If corrections need to be made post certification, please contact the CLFS helpdesk:

- **Application Help Desk**
  - E-mail: [CLFSHelpDesk@dcca.com](mailto:CLFSHelpDesk@dcca.com)
  - Phone: 844-876-0765
- 9AM-6PM Eastern, Non-Peak
- 9AM-9PM Eastern, Peak (i.e., January-March 2017)

5. To certify data for another TIN, select another TIN from the TIN dropdown menu. The data for the selected TIN display as shown in Figure 7-5.

Figure 7-5: Certification – Certify Another TIN

![Figure 7-5: Certification – Certify Another TIN](image)

Note: if you select a TIN where data has already been certified, you will receive a message stating that the data have already been certified for the selected TIN, as shown in Figure 7-6.

Figure 7-6: Certification – Selected TIN has Already Been Certified Message

![Figure 7-6: Certification – Selected TIN has Already Been Certified Message](image)

6. Click on the **Certify All** button and repeat step 4.

All of the “Results” for the data changes are changed from being “SAVED” to “CERTIFIED” as shown in Figure 7-7.
7.1 Certification – Large Volume

Data certification is a process where an applicable laboratory representative (CLFS Certifier) certifies the accuracy of the data. The CLFS Certifier must certify all data files pending certification. The CLFS certifier cannot make any edits to the data file. If the CLFS certifier identifies a need to edit the data file, this must be completed by the CLFS submitter.

1. CLFS Certifier logs into the system and clicks on “Certification” from the left side of the screen.
   
   The “Certification” window displays as shown in Figure 7-8.

   **Figure 7-8: Certification Window – Large Volume**

2. Select a TIN from the drop-down box.
   
   The file for the selected TIN displays as shown in Figure 7-9.
3. Click on the **Certify All** button.

   A “Data Certification Statement” pop-up window displays as shown in Figure 7-10.

   ![Figure 7-10: Data Certification Statement](image)

   **Figure 7-10: Data Certification Statement**

   **Data Certification Statement:**
   
   I certify that the reported applicable information is accurate and that all information and statements made in the submission are true, complete, and current to the best of my knowledge and belief and are made in good faith. I understand that information contained in this submission may be used for Medicare reimbursement purposes.

   - [ ] I agree to the above certification statement
   - [ ] Certify

4. Review the statement, click in the box next to “I agree to the above certification statement,” and then click on the **Certify** button.

   Note: The system will display a message “All data records are certified. Certification has been completed and closed for this reporting period.”

   The “Results” for the data file changes “SAVED” to “CERTIFIED” as shown in Figure 7-11.
Warning: Once the CLFS Certifier has certified the data for the current period, data submission is closed and no more data can be entered for that applicable laboratory. Be sure that all applicable information is entered, accurate, and complete before certifying the data. If corrections need to be made post certification, please contact the CLFS helpdesk:

Application Help Desk
- E-mail: CLFSHelpDesk@dcca.com
- Phone: 844-876-0765
  - 9AM-6PM Eastern, Non-Peak
  - 9AM-9PM Eastern, Peak (i.e., January-March 2017)

5. To certify data for another TIN, select another TIN from the TIN dropdown menu, as shown in Figure 7-12.

Figure 7-12: Certification – Certify Another TIN – Large Volume

Note: if you select a TIN where data has already been certified, you will receive a message stating that the data have already been certified for the selected TIN, as shown in Figure 7-13.
6. Click on the **Certify All** button and repeat step 4.

All of the “Results” for the data changes are changed from being “SAVED” to “CERTIFIED,” as shown in Figure 7-14.

**Figure 7-14: Certification - Data Certified Window – Large Volume**
8 Help Desk

After role request submission – Please wait up to 72 hours; you will receive an e-mail notification.

Points of contact:

- Policy Questions
  - CLFS_Inquiries@cms.hhs.gov
    - Examples:
      - Is my laboratory an applicable laboratory
      - “What data do I submit”?
    - Reference: CLFS Frequently Asked Questions

- Application Help Desk
  - E-mail: CLFSHelpDesk@dcca.com
  - Phone: 844-876-0765
    - 9AM-6PM Eastern, Non-Peak
    - 9AM-9PM Eastern, Peak (i.e., January-March 2017)

- Issue examples:
  - Account Unlock
  - Password Reset
  - Registration process questions
  - Policy Question escalations
  - System Availability escalations
  - Other
9 Frequently Asked Questions

9.1 General

1. **What is the CMS Enterprise Portal?**
   The CMS Enterprise Portal is a convenient single point of entry to numerous CMS applications, systems, and databases.

2. **Who is eligible to have a CMS User Account?**
   All US citizens who are over 18 years of age and have a valid US residential address are eligible to have a CMS User Account.

3. **Who do I contact for Portal Login issues?**
   CMS Portal login issues should be directed to “our helpdesk info.”

9.2 Supported Browsers

1. **What browsers are supported by the CMS Enterprise Portal?**
   The CMS Enterprise Portal supports the following browsers:
   - Internet Explorer (IE) 11
   - Firefox
   - Chrome
   - Safari

2. **What browser mode is supported?**
   There are different browser modes that can be specified by you, the user. Only the native browser mode is supported. To find out what browser mode you are using, hit the F12 key while in IE. The top of the resulting window/panel will show the browser mode being used.

3. **What document mode is supported?**
   There are different document modes that can be specified by you, the user. Only the native document mode is supported. To find out what document mode being used, hit the F12 key while in IE. The top of the resulting window/panel will show the document mode being used.

4. **Is JavaScript required for the CMS Enterprise Portal?**
   JavaScript needs to be enabled for successful use of the Enterprise Portal.
1. **What personal information is required to provide in order to register for my user account?**

   You must provide your legal name, current home address, primary phone number, and e-mail address. You must enter your first and last name as they appear in legal documents, such as your driver’s license or passport. If you have a suffix included in your name (such as Sr., Jr., Ii, etc.), make sure you select it from the suffix field exactly as it appears on legal documents.

2. **Why should I submit personal information to create a user account and how safe is it?**

   EIDM collects personal information to uniquely identify users when registering with the system. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID/Password. For security level information please visit: [Centers for Medicare & Medicaid Services (CMS) Website Privacy Policy](#).

3. **Can I register for an EIDM user account with a foreign address and an international phone number?**

   Yes, EIDM allows users to register with a foreign address and an international phone number. At a minimum, foreign addresses must include the following information:
   - House number, street name, and country; and
   - An international phone number that must start with the country code, followed by the area code, and the primary phone number.

4. **Can I change my foreign address to a U.S. address, and vice versa?**

   Yes, EIDM allows users to change their address from a foreign address to a U.S. address, and vice versa. Use the ‘Change Address’ link under the ‘My Profile’ menu to change your address.

5. **What will you do with my PII?**

   EIDM uses an external authentication service provider, Experian, to verify your identity based on the information you provide. Experian verifies your information against its records to successfully identify you. CMS provides, on public-facing websites, their Terms & Conditions of how your information will be handled when registering for a CMS EIDM user account.

6. **How many days do I have to confirm my EIDM account?**

   EIDM requires users to confirm their account between 30 and 180 days. Accounts are confirmed by selecting the link provided to the user in their account confirmation e-mail. If the user fails to confirm their account, then the link and the account will expire.
7. **How can I update my personal information?**

   You can update your personal information by selecting ‘My Profile’ from the dropdown menu at the top right hand corner of the CMS Portal home page. You will then be directed to the ‘View My Profile’ page, where you can change your personal information by selecting the links on the right side of the page. You may be requested to answer challenge questions based on the changes you make.

8. **Where can I find information regarding who has the right to request a Social Security Number (SSN)?**

   Federal law mandates that State departments of motor vehicles, tax authorities, welfare offices, and other governmental agencies request your SSN as proof that you are who you claim to be. However, the Privacy Act of 1974 requires that any government agency requesting your SSN provide details on how this information will be used, and what law or authority requires its use.

   For information on who has the right to request your SSN please select the following link: [Who Can Lawfully Request My Social Security Number?](#).

   The Privacy Act can be read at the following link: [The Privacy Act of 1974](#).

9. **I already provided my personal information during registration to setup an EIDM user account. Why do I have to provide it again to access certain applications?**

   When you have selected an application or role that requires a higher level of security, you are required to complete Identity Verification. In most cases, you may need to provide a few more details (i.e. SSN, Date of Birth) to be able to request access to the selected application or role.

10. **Will my SSN be shared with any federal or private agency?**

    Your SSN will be used for verification purposes only. EIDM does not share your SSN with any other federal or private agency.

11. **How often do I need to update my password?**

    EIDM requires that users update their password at least once between 60 days and 24 months depending on the user role community. Once your password expires, you will be prompted to enter your new password. You can use the ‘Change Password’ self-service feature located on the ‘My Profile’ page. To use this feature, you must sign into the CMS Portal and select the ‘My Profile’ link from the dropdown menu at the top right hand corner of the CMS Portal home page. You must click the ‘Change Password’ link on the ‘My Profile’ page to change your Password.
9.4 Identity Verification

1. **What is Identity Verification?**

   Identity Verification is the process of providing sufficient information (e.g., identity history, credentials, or documents) to a service provider for the purpose of proving that an individual is who he/she claims to be. Individuals requesting electronic access to CMS protected information or systems must be identity proofed prior to being given access.

2. **Why does Experian require my personal information?**

   Experian uses your personal information to verify your identity against your personal information record.

3. **Does verifying my identity by Experian affect my credit score?**

   No, this kind of inquiries is known as a “soft inquiry.” Soft inquiries do not affect your credit score, and there are no charges related to them. Soft inquiries are displayed in the consumer version of the credit profile, which is neither viewable nor reported to lenders. If you order a credit report from Experian, you will see an entry of inquiry by the CMS Medicaid Services with CMS’ address on the date the request was made.

4. **Will I be required to go through Identity Verification after changing my address from foreign address to U.S. home address and vice versa?**

   No, you will not be required to re-do Identity Verification if you already have a role that previously required your identity to be verified.

5. **What if I have problems completing Identity Verification? Is there an Experian Help Desk?**

   Yes, Experian Verification Support Services is a dedicated call center for individuals who have failed the online Remote Identity Proofing (RIDP) process while attempting to obtain a CMS EIDM user account. If you fail online RIDP, EIDM will generate a reference code and the Experian Verification Support Services contact information will be provided on the screen for further action.

6. **What happens if the Experian Help Desk cannot verify my identity?**

   If your identity cannot be verified, even with assistance from the Experian Help Desk, you will need to contact your application specific Help Desk to go through a document based proofing process. If your Application Help Desk cannot verify your identity, your access to CMS applications that require a higher level of security will be restricted.

7. **Why am I not able to change my User ID?**

   The User ID identifies you uniquely to EIDM; therefore, you cannot change your User ID.

8. **Can I use the same credentials for different applications?**

   Yes, you may use the same credentials to access different applications. Once you have logged into the CMS Portal home page, you can request access to other applications.
9. When I try to login I get an error message “Incorrect combination of User ID or Password. Please try again. If you need further assistance, you may use the “Forgot User ID” or the “Forgot Password” link to help you.” What should I do?

Please check the user ID and password that you entered. An incorrect combination of these will result in such an error message.

10. When I try to login I get an error message “Incorrect combination of User ID, Password or Security Code. Please try again. If you need further assistance, you may use the “Forgot User ID” or “Forgot Password” links to help you. For issues with the Security Code, you may use the "Unable to Access Security Code?" link or contact your Application Help Desk.” What should I do?

Please check the user ID, password, and Security Code that you entered. An incorrect combination of these will result in such an error message.

11. When I try to log in, I am prompted to enter a Security Code. What do I do if I don’t have an MFA device registered to my account or am having issues retrieving a Security Code?

For issues with logging in with a Security Code you may use the following options:

- If you do not have an MFA device registered to your account, you may use the “Register MFA Device” link on the Password and Security Code page for assistance.

- If you are unable to retrieve a Security Code from your registered MFA device or do not have your device available, you may use the “Unable to Access Security Code?” link on the Password and Security Code page for assistance.

- If you have trouble using the “Register MFA Device” or “Unable to Access Security Code?” links, you may contact your Application Help Desk for assistance.

For more information about MFA, please refer to section 9.5 Multifactor Authentication (MFA)

12. When I try to log in, I get the error message stating “Your account is disabled. Contact the Help Desk to enable your account.” Why does this happen?

A user’s account can be disabled by Application Help Desks or by EIDM Administrators for possible reasons that are linked to security violations or fraud detection. In order to enable your disabled account, you are required to contact the Application Help Desk.

13. When I try to log in, I get the error message stating “Your account has been locked. Please try again later.” Why did this happen and how can I get my account unlocked?

After three unsuccessful attempts to login, your account will be locked. Your account will be unlocked after 60 minutes have elapsed since your third consecutive failed authentication attempt. After the 60 minutes have passed, you will be required to enter valid credentials associated to your user account to unlock the account. If you are unable to unlock your account, you may call your Application Help Desk for assistance.
14. When I try to log in, I am directed to the ‘Unlock My Account’ view. Why is this and how do I unlock my account?

EIDM locks your user account if no account activity is reported for 60 days. When you login after 60 days the system will display the ‘Unlock my Account’ view; enter your User ID and correctly answer all challenge questions on the next page; enter your old password and then a new password in the input fields of ‘New Password’ and ‘Confirm New Password’ to unlock your account.

15. What are challenge questions and why do I need to select and answer them when setting up my account?

EIDM uses challenge questions for security purposes to verify your account. When you register your account, you will need to select three different questions and provide an answer for each question. You will be asked to answer the challenge questions in the future if you forget your password, change your address, change your phone number, or to unlock your account. Correct responses to the challenge questions will enable EIDM to confirm your account.

9.5 Multifactor Authentication (MFA)

1. What is MFA?

MFA is a type of login (authentication) that, in addition to a user ID and password, requires another “factor” such as a Security Code. To comply with CMS policy, most users will need to establish a second login “factor” commensurate with the level of access requested. CMS uses Symantec’s Validation and Identity Protection (VIP) service to add a second layer of protection for your online identity. Symantec provides VIP through computer, phone, and e-mail.

2. How do we use MFA?

You will be asked to enter your user ID, password, and an additional Security Code that is generated by Symantec VIP software to gain access to your application. The Security Code can be generated by:

- A free Symantec application that can be downloaded to your desktop or Smartphone;
- An SMS or Interactive Voice Response (IVR) once you have registered your phone in your application; or
- By e-mail.

The “Where can I get the MFA software?” section below provides the necessary information to install the Symantec application on your desktop or Smartphone.

3. How do I get an MFA device?

Your application will prompt you to register an MFA device when you request access to protected information and you have not already registered an MFA device with the application. You will be given a choice of MFA Security Code delivery methods. The primary MFA Security Code delivery method is to download software and install it on your computer or a mobile device. Alternatively, if you require special support, you can set up
SMS or IVR to deliver your MFA Security Code. Details on where to get the MFA software are described below.

4. **Where can I get the MFA software?**

You will need MFA software if you choose to receive your MFA Security Code on a computer, laptop, or mobile device. You will be required to download the MFA software from Symantec and install it on your device of choice.

To download the desktop software for Windows or Mac, go to the Validation and IP Protection Center and follow the instructions.

If using an iPhone, Android, Blackberry, or other mobile device, use your device to navigate to Validation and ID Protection Mobile Center and follow the instructions.

SMS, IVR, and e-mail options do not require a software download.

5. **When I click on an application, I am redirected to the MFA login screen. What is this?**

The MFA login screen is displayed when you attempt to access an MFA-protected application. If you have an MFA device, you will be able to access the application. If you do not have an MFA device, then you will have to register for MFA using either your phone or computer.

6. **What are the types of devices I can register with for my MFA?**

You can add one or more of the following devices as your MFA device:

- Smartphone, Computer, or Tablet – By downloading the Symantec VIP access application;
- IVR – By registering with a U.S. phone number;
- SMS – By registering with a U.S. phone number; and
- E-mail – By registering with a valid e-mail address (the e-mail address associated with your profile will be used).

7. **How do I register my MFA device (phone, computer, or e-mail) to my EIDM user account?**

Once you successfully complete the Identity Verification process, EIDM will display the ‘Register your Phone, Computer, or e-mail’ page depending on the application role being requested. Alternatively, you can register for MFA by selecting the ‘Register your Phone, Computer, or e-mail’ link under ‘My Profile’.

Your device can be registered for MFA in one of five ways:

a. Download VIP access software on your phone – Enter the alphanumeric Credential ID generated by the VIP access client. Then enter the Security Code generated by the VIP client.
b. Download VIP access software on your computer – Enter the alphanumeric Credential ID generated by the VIP access client. Then enter the Security Code generated by the VIP client.

c. Text Message SMS – Use this option to have the Security Code texted to your phone. You must enter a valid phone number and your phone must be capable of receiving text messages. Carrier charges may apply.

d. IVR – Use this option to receive a Voice Message containing the Security Code. You must provide a valid phone number and (optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks ‘*’; period ‘.’; comma ‘,’; pound ‘#’, followed by numeric 0 to 9. For example: 4885554444, 1112.

   • * (asterisk) Used by some phone systems to access extension;
   • . (period) Creates a delay of approximately 5 seconds;
   • , (comma) Creates a short delay of approximately 2 seconds;
   • # (pound) Used by some phone systems to access an extension; and
   • A comma may be used if you are unsure of the special character supported by your company’s phone system.

e. e-mail – You can also opt to use the e-mail in your profile to receive a Security Code when logging into a secure application.

8. How do I register for MFA if I receive an error when installing the software on my computer?

If you are having trouble downloading and installing the MFA software on your desktop or laptop, it is possibly due to your company’s Information Technology (IT) policy that disables users from installing any software on company-provided machines. Check with your company’s IT department for assistance. If your company does not allow you to install MFA software, one alternative is to use a mobile device that you control, or you can also use a voice call to obtain the Security Code. You can refer to other instructions in this FAQ section for information on cell phone installation and IVR usage.

9. I cannot use the desktop MFA software or the mobile phone MFA software. What should I do?

Your application allows you to set up a voice or SMS delivery method for your Security Code that does not require an MFA software download. You can register a phone number and select SMS or IVR. Then your application can register your phone number and delivery method with Symantec. After your MFA is activated, when you login to your application you will receive either a phone call or text message that contains your Security Code, depending on the delivery method you selected.

The SMS and IVR Security Codes expire within 10 minutes of when they are sent, so please make sure you provide a phone number that will be accessible to you during your typical work hours. For example, do not use a residential phone number if you will normally login
from your place of employment. E-mail Security Codes expire within 30 minutes of when they are sent.

10. Can I access multiple applications if I’m Multi-Factor Authenticated (MFA)?

Once you have been multi-factor authenticated (i.e. “logged in”) into your application, if you do not log out of the system, you can access other protected CMS Applications that require MFA without having to be authenticated again with an MFA Security Code. If you log out of the system, when you log back in, you will be asked to present your MFA Security Code when accessing your CMS Application.

11. How do I use my MFA device to log into my CMS EIDM user account?

When you log into your application, the system will display the MFA login screen. You will be required to enter your user ID, password, and the MFA Security Code. If you have registered an MFA device, enter your user ID, password, and the Security Code that is displayed on your MFA device, as shown in Figure 9-1.

![Figure 9-1: Security Code](image)

For your protection, an MFA device automatically generates a new Security Code each time it counts down from a 30-second timer.

If you have registered an MFA SMS or IVR device, when you log into your application, the system will send you a Security Code via text message or voice call to the number you registered in EIDM.

For your protection a Security Code sent via SMS or IVR counts down from a 10-minute timer. The Security Code sent via e-mail counts down from a 30-minute timer.

12. How do I add additional MFA devices to my CMS EIDM user account?

You can register up to five MFA devices to your user account. Additional MFA devices can be added to your account after you have been prompted by your application to set up the first MFA device. The “Register your Phone, Computer, or e-mail” link on the “My Profile” page will appear once you have successfully set up your first MFA device. You can click on the link and add additional MFA devices to your user account.
13. Will I be charged cell phone time each time I use Symantec VIP MFA on my mobile device?

It depends on what delivery method you use. The Symantec VIP MFA software is free. Once the Symantec VIP MFA application is downloaded and installed on the phone it does not utilize any cell time to generate the six-digit security code. Cell or network traffic is used to download the application to one’s mobile device. There are no recurring charges associated with the use of either software option. If you choose not to use the software option and select SMS or IVR, carrier charges may apply.

14. I lost all my MFA devices linked to my EIDM user account. How do I deactivate the linked devices and link new devices to my user account?

Your Application Help Desk should be able to assist you in removing/deactivating the registered devices and registering new devices to your user account.

15. What should I do if I lock my MFA device?

You must contact your Application Help Desk to unlock the registered MFA device.

16. If my Credential ID is copied or stolen, can someone else access my CMS EIDM User account?

No. A Credential ID cannot be used to access an EIDM user account.

9.6 Annual Certification

1. What does it mean when my account is inactive?

A CMS Portal account is inactive when a user has not logged into either their application or the CMS Portal for 60 days or more.

2. What does it mean when my account is locked?

A user’s account is locked following 60 days of inactivity. The user is prevented from logging into any application. To unlock an account the user must: login to the CMS Portal, answer their challenge questions, and reset their password; or call the Application Help Desk.

3. What does it mean when my account is deleted?

When a user’s CMS Portal account does not have a role in any application and has been inactive for more than 360 days it will be deleted. The user’s account may no longer be used for any purpose and the user may register again to create a new account.

4. What is an Account Review?

Users wishing to acquire a role in their application must first register for a CMS Portal account. Account Reviews are conducted every six months to check for the presence of at least one application role in a user’s account. If an account does not have any application roles associated to it and has been inactive for more than 180 days, it will fail. If the account has been inactive for more than 360 days, it will be deleted.
5. Is there anything I need to do for Account Reviews?
   If you have an application role associated to your account then no action is required on your part. If you do not have an application role associated to your account and have been inactive for more than 180 days, you will receive an e-mail with instructions on how to proceed.

6. I got an e-mail that my account failed an Account Review. What should I do next?
   If you no longer require an account in the CMS Portal, no further action is required on your part. If you wish to continue using your account, please follow the instructions in the e-mail describing how to proceed.

7. I got an e-mail that my account was deleted as part of an Account Review. What should I do to get my account back?
   If your account was deleted as part of Account Review, you must create a new account. Please go to the CMS Portal and follow the on screen instructions to create a new account.

8. What is a Role?
   A Role is the name (e.g. Submitter or Representative) given to a set of privileges and permissions that an individual may perform within an application or other computer resource. Users must submit a role request which should be approved and then the role will be added to the user’s profile. Use of a role is typically granted for one year by an application Business Owner, their representatives, authorizers, Help Desk personnel, or other approver. Each year, continued use of a role must be approved or the role will be removed from the user’s profile. This annual re-approval is known as Annual Certification.

9. What is Annual Certification?
   CMS security guidelines require that each year, the use of a role must be approved or the role will be removed from the user’s profile. Annual Certification is the process of approving a user’s continued use of a role and is valid for one year. Annual Certification is typically performed in the same manner as the original role approval process used by Business Owners, their representatives, authorizers, Help Desks, or other approvers. If the continued use of a role is not approved, then the role will be removed from the user’s profile and an e-mail will be sent notifying the user that their role has been removed.

10. What is an Annual Certification due date?
    The Annual Certification due date is the date that a role is due to be certified. This is normally one year after the last Annual Certification.

11. How often does my role need to be certified?
    Your role needs to be certified once a year. It is your approver’s responsibility to certify your role and usually requires no action on your part.

12. What do I need to do to have my role certified?
    It is your approver’s responsibility to certify your role and usually requires no action on your part. If your role failed Annual Certification, an e-mail will be sent to you with more information.
13. I got an e-mail that my role was removed because it failed Annual Certification. How do I get my role back?

If you still need access to the role that was removed, you must request the role again. Please follow the instructions provided in the e-mail.

14. I am an approver who is responsible for approving role requests. What do I need to do for Annual Certification?

As an approver for role requests, you will be responsible for certifying users’ roles by the certification due date. An ‘Annual Certification’ link can be found where you usually go to approve user role requests. On that page you will be able to search, review, certify, or revoke the certifications for users under your authority. If no action is taken by the certification due date, the role will be removed.

15. I am an approver and I received an e-mail informing me that I have roles pending Annual Certification. What do I need to do?

As an approver for users’ role requests, you are also responsible for certifying those roles annually. 30 days before a role’s certification due date, you will receive an e-mail providing a count of user roles that are due for certification within the next 30 days, 15 days, 7 days, and 1 day. If no action is taken by the certification due date, the role will be removed.

16. If my role is automatically approved, do I need to take any action for Annual Certification?

If your role requests are automatically approved, they will also be automatically certified. Some automatically approved roles require the information provided, when the role was first requested, to be validated against a trusted resource. As part of Annual Certification, this information will need to be revalidated. If the validation is successful, your role will be certified automatically and no action is required on your part. If the validation fails, CMS.gov will send you an e-mail notifying you that validation failed and describing how to correct the error before the certification due date for your role.

17. Why can’t I see all my users’ roles in the Pending Certification View Page?

The Pending Certification View Page shows a maximum of 250 roles that you are responsible for certifying in the next 30 days. If you have more than 250 roles to certify in the next 30 days or wish to see roles due for certification past the next 30 days, you must use the Search feature.

18. I am searching for roles that I need to certify but don’t see any results after selecting the Search button. Why is my search not displaying any results?

The most likely reason is that your search did not match any existing role certifications. The search will also not return any results if there are more than 250 certifications found for your specific search criteria. Please ensure that you narrow down your search so that no more than 250 certifications will be found from your search request.
## Appendix A  Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADLT</td>
<td>Advanced Diagnostic Laboratory Test</td>
</tr>
<tr>
<td>ARS</td>
<td>Acceptable Risk Safeguards</td>
</tr>
<tr>
<td>ASP</td>
<td>Average Sales Price</td>
</tr>
<tr>
<td>CCN</td>
<td>CMS Certification Number</td>
</tr>
<tr>
<td>CDLT</td>
<td>Clinical Diagnostic Laboratory Test</td>
</tr>
<tr>
<td>CFO</td>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>CLFS</td>
<td>Clinical Laboratory Fee Schedule</td>
</tr>
<tr>
<td>CM</td>
<td>Center for Medicare Management</td>
</tr>
<tr>
<td>CMS</td>
<td>Centers for Medicare &amp; Medicaid Services</td>
</tr>
<tr>
<td>EIDM</td>
<td>Enterprise Identity Management</td>
</tr>
<tr>
<td>EIN</td>
<td>Employer Identification Number</td>
</tr>
<tr>
<td>EUA</td>
<td>Enterprise User Administration</td>
</tr>
<tr>
<td>FAQ</td>
<td>Frequently Asked Questions</td>
</tr>
<tr>
<td>FFSDCS</td>
<td>Fee for Service Data Collection System</td>
</tr>
<tr>
<td>HCPCS</td>
<td>Healthcare Common Procedure Coding System</td>
</tr>
<tr>
<td>IE</td>
<td>Internet Explorer</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IVR</td>
<td>Interactive Voice Response</td>
</tr>
<tr>
<td>LV</td>
<td>Large Volume</td>
</tr>
<tr>
<td>NPI</td>
<td>National Provider Identifier</td>
</tr>
<tr>
<td>OTP</td>
<td>One Time Password</td>
</tr>
<tr>
<td>PAMA</td>
<td>Protecting Access to Medicare Act</td>
</tr>
<tr>
<td>PFS</td>
<td>Physician Fee Schedule</td>
</tr>
<tr>
<td>PII</td>
<td>Personal Identifiable Information</td>
</tr>
<tr>
<td>PTAN</td>
<td>Provider Transaction Access Number</td>
</tr>
<tr>
<td>RIPD</td>
<td>Remote Identity Proofing</td>
</tr>
<tr>
<td>Acronym</td>
<td>Translation</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SSN</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>TIN</td>
<td>Tax Identification Number</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>VIP</td>
<td>Validation and Identity Protection</td>
</tr>
</tbody>
</table>