Enrollment: Multi–Factor Authentication for I&A System

July 30, 2019

Presenters:

Keith Washington, CMS
Acronyms in this Presentation

• I&A – Identity & Access Management System
• MFA – Multi-Factor Authentication
• NPPES – Nation Plan & Provider Enumeration System
• PECOS – Provider Enrollment, Chain, and Ownership System
• HITECH – Health Information Technology for Economic and Clinical Health
• EHR – Electronic Health Record Incentive Program
• EUS – External User Services
Agenda

• I&A Overview

• I&A MFA Background and Overview

• I&A MFA Walkthrough and Details Overview

• NPPES Multi-Factor Authentication

• Q&A
I&A Overview

I&A Provides:
1. Authentication
2. Authorization

Supports the Following Applications (aka Business Functions):
   a. NPPES (National Plan and Provider Enumeration System)
   b. PECOS (Provider Enrollment Chain and Ownership System)
   c. EHR (Electronic Health Record Incentive Program) (aka HITECH)
I&A MFA Background and Overview
I&A MFA Background and Overview

• **What is Multi-Factor Authentication?**
  • Multi-Factor Authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user’s identity for a login or other transaction

• **Why is CMS implementing this?**
  • This is to improve identification and authentication security for the four public facing applications I&A, NPPES, PECOS and HITECH, starting with I&A in September 2019
I&A MFA Walkthrough and details Overview
I&A MFA Walkthrough and Details Overview

How do I get started?

• **Existing I&A users:** You will be prompted with an option to set up your MFA devices as you login to your application. You will have a grace period of up to 30 days to delay setting up your MFA devices.

• **New I&A users:** You will be prompted to set up your MFA devices as you set up your account. You will not be able to get an I&A account unless your MFA setup is completed.

What Devices Can I Use?

• You can use a mobile Phone (SMS or Voice), landline phone (Voice), or Email address (Email)

How many devices can I add?

• You can add up to two devices, a Primary Authentication device/method and an Alternative Authentication device/method
Users will have a 30 day grace period to set up MFA. All applications will have a cutoff date in June 2020 to set up MFA for all users.

- I&A APP Configuration: 30 ~ 300 days
- NPPES APP Configuration: 30 ~ 210 days

I&A MFA Framework
- I&A APP MFA Integration
- NPPES APP MFA Integration
- PECOS App MFA Integration
- HITECH APP MFA Integration

Initial APP MFA Deployment
Application MFA grace period is applicable within this date range
Application MFA cut off date
I&A MFA Walkthrough and Details Overview – I&A Login

**Important Announcement:**
To better protect your information, we will be implementing Multi-Factor Authentication (MFA) in September 2019.

Authorized users are able to sign in to the Identity & Access Management System. If you are a new user you must first register.

**Sign In**
* Indicates required field(s)

- **User ID:** Mfauser7
- **Password:** *********

**One account to access multiple systems**
Create one account with the Identity & Access Management System to manage access to NPPES, PECOS, and EHR incentive programs, manage staff, and authorize others to access your information.

**PECOS**
Use this system to register for Medicare or update your current enrollment information.
Register to receive EHR incentive payments for eligible professionals and hospitals that adopt, implement and upgrade or demonstrate meaningful use with certified EHR technology.

**NPPES**
Use this system to apply for and manage National Provider Identifiers (NPIS).
I&A MFA Walkthrough and Details Overview – MFA Initial Setup Cont’d

Identity & Access Management System

User Registration - Multi-Factor Authentication (MFA) Setup

We need a way to deliver a temporary code to you to verify your identity. We can do this via a phone number (either by voice or Text/SMS) or you can choose to have it sent to you in an e-mail. You must enter this code on the next page.

You must identify at least one method for receiving your verification code; however, you may provide up to two different methods.

Please note the following Text/SMS and Voice Call Details:
- International phone numbers are not supported.
- Standard message and data charges may be applied by your carrier.
- By entering a Mobile Phone Number, you are certifying that you are the account holder or have the holder’s permission to use the phone number to receive a Text/SMS message.

Please select a Multi-Factor Authentication Method:

* Authentication Method:
  - Select Primary Authentication Method
  - Select Primary Authentication Method
  - Phone Number Text/SMS
  - E-mail Address
  - Phone Number Voice Call

Continue | Cancel
We need a way to deliver a temporary code to you to verify your identity. We can do this via a phone number (either by voice or Text/SMS) or you can choose to have it sent to you in an e-mail. You must enter this code on the next page.

You must identify at least one method for receiving your verification code; however, you may provide up to two different methods.

Please note the following Text/SMS and Voice Call Details:
- International phone numbers are not supported.
- Standard message and data charges may be applied by your carrier.
- By entering a Mobile Phone Number, you are certifying that you are the account holder or have the holder's permission to use the phone number to receive a Text/SMS message.

Please select a Multi-Factor Authentication Method:

**Authentication Method:**
- Phone Number Text/SMS

**Phone Number:**
Enter your 10 digit phone number the way you normally dial it.
Identity & Access Management System

User Registration - Multi-Factor Authentication (MFA) Setup - Verify Code

Step 1: User Security
Step 2: User Info
Step 3: MFA Setup
Final Review

* Indicates required field(s)

A Text/SMS was sent to (301) [redacted]

* Enter Code: 796845

Haven't received a Text/SMS yet? Resend Text/SMS

Need to make changes where you receive your code? Back to Setup Page

Verify Code | Cancel
Congratulations, your Phone Number (301) [redacted] was successfully verified! This will be used to verify your identity upon logging in.

If you wish to set up an Alternative MFA method, please select Begin Alternative Setup.

Begin Alternative Setup

Complete Registration | Cancel
I&A MFA Walkthrough and Details Overview – MFA Login

Identity & Access Management System

Multi-Factor Authentication (MFA) - Method

* indicates required field(s)

We would like to send you a code to verify your identity.

* Select where you wish to receive your verification code:

- Primary Authentication Method: Phone Number Text/SMS: (xxx)xxx-9321

Need to make changes where you receive your code?  

Send Verification Code  |  Cancel  

Reset MFA
Multi-Factor Authentication (MFA) - Verification

* Indicates required field(s)

Your Verification Code will be sent to:
* Select where you wish to receive your verification code:
  - Primary Authentication Method: Phone Number Text/SMS: (xxx)xxx-9321

* Are you logging in to the system on a Public or Private device?
  - This is a Public Device
  - This is a Private Device

* Enter Code: 

Haven't received the code yet or need a new code? Send New Code

Verify Code | Cancel
Users will be able to declare that the device they are using is a private device. This option will allow the user to bypass the MFA portion of the login for up to 24 hours.

By selecting the Consent button, you are agreeing to let the system install a cookie on your Private Device Browser. This will give you the ability to bypass Multi-Factor Authentication for the next 24 hours when logging into the system.
Identity & Access Management System

User Information Integrity Check - Multi-Factor Authentication (MFA) Setup

We are implementing Multi-Factor Authentication to ensure your data is secure. We do this by sending you a temporary code to you to verify your identity. The code can be sent to you either via a phone number (either by voice or Text/SMS) or an e-mail.

Multi-Factor Authentication is currently optional, but will become required in 28 days. Do you want to set up your Multi-Factor Authentication now?

- Yes, I want to set up my Multi-Factor Authentication now
- No, I will set up my Multi-Factor Authentication later

Continue | Cancel
I&A MFA Walkthrough and Details Overview – Reset MFA at Login

Identity & Access Management System

Multi-Factor Authentication (MFA) - Method

* indicates required field(s)

We would like to send you a code to verify your identity.

* Select where you wish to receive your verification code:

[ ] Primary Authentication Method: Phone Number Text/SMS: (xxx)xxx-9321

Need to make changes where you receive your code? [Reset MFA]

Send Verification Code ▶  Cancel
Users who need to unlock or reset MFA will have to answer 3 security questions or provide correct user information to access I&A.
Users can delete/add MFA methods.
NPPES Multi-Factor Authentication
NPPES Multi-Factor Authentication

- NPPES MFA for R3.10.0 goes live in December 2019
  - If you have set up MFA in I&A already (after R3.9.0 is deployed), you will need to enter your User ID, password, and the second factor when you log into NPPES
  - If you have not set up MFA before, you will have a 30 day grace period to set it up. Meanwhile, whenever you log into NPPES, you will be prompted to set up MFA through I&A.
Users will have a 30 day grace period to set up MFA. All applications will have a cutoff date in June 2020 to set up MFA for all users.

<table>
<thead>
<tr>
<th>I&amp;A APP Configuration</th>
<th>30 ~ 300</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPPES APP Configuration</td>
<td>30 ~ 210</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I&amp;A APP MFA Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NPPES APP MFA Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PECOS App MFA Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HITECH APP MFA Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Initial APP MFA Deployment
Application MFA grace period is applicable within this date range
Application MFA cut off date
NPPES Multi-Factor Authentication – Login

Registered User Sign In
Log in to view/update your National Provider Identifier (NPI) record.

User ID
Dr. James

Password

SIGN IN
FORGOT USER ID OR PASSWORD?

Create a New Account
You need an Identity & Access Management System (I&I) User ID and Password to create and manage NPIs.

Individual Providers, Organization Providers, Users working on behalf of a provider

If you don’t have an I&I account, need to update your existing I&I account, or don’t remember your User ID or Password, select the CREATE or MANAGE AN ACCOUNT button below to go to I&I.

Once you have successfully created your I&I account, your existing Type 1 NPI will be associated with your I&I account.

After successfully creating your I&I account, return to NPPES and use your I&I User ID and Password to log into NPPES where you can create and maintain the NPI data associated with your provider(s).

CREATE or MANAGE AN ACCOUNT

*If your User ID is associated with a large number of providers, you could experience a small delay while the application retrieves all NPPES profile related information.
NPPES Multi-Factor Authentication – Optional Grace Period

This screen appears only if you haven’t Setup MFA in I&A

Attention: Multi-Factor Authentication will soon be required when logging into NPPES.

We are implementing Multi-Factor Authentication to ensure your data is secure. We do this by sending a temporary code to you to verify your identity. The code can be sent to you either via a phone number (either by voice or Text/SMS) or an email.

Multi-Factor Authentication is currently optional when logging into NPPES, but will become required in [X] days. Select the GO TO I&A TO SET UP MFA button to log into I&A and set up your MFA before returning to log into NPPES. Select the CONTINUE LOGGING INTO NPPES if you don’t wish to set up your MFA at this time.
NPPES Multi-Factor Authentication – Login
(After Setting Up MFA)

Need to make changes to where you receive your verification code? Go to I&A and Reset MFA

Select where you wish to receive your Verification Code:

- Primary Authentication Method: Phone Number Text/SMS (***-***-6770)
- Alternative Authentication Method: Email Address: W****@email.com

SEND VERIFICATION CODE  CANCEL
NPPES Multi-Factor Authentication – Login – Cont’d
(After Setting Up MFA)

Multi-Factor Authentication (MFA)

* Indicates Required Fields.

Need to make changes to where you receive your verification code? [Go to I&A and Reset MFA]

Select where you wish to receive your Verification Code:

- Primary Authentication Method: Phone Number Text/SMS (***-***-6770)
- Alternative Authentication Method: Email Address: W****@email.com

Are you logging in to the system on a Public or Private device?

- This is a Public Device
- This is a Private Device

Enter Code: 

Haven’t received the code yet or need a new code?

SEND NEW CODE

VERIFY CODE  CANCEL
Question & Answer Session
Resources

• For any questions relating to your I&A MFA setup (Initial setup, MFA login, account reset … etc. ) contact EUS Support
  I&A Helpdesk:
  • Website: https://eus.custhelp.com/
  • By E-mail: EUSSupport@cgi.com
  • By Phone: 1-866-484-8049 (TTY/TDD: 1-866-523-4759)

• E-mail your questions related to I&A MFA or NPPES MFA to:
  For I&A Related Questions: EUSSupport@cgi.com
  For NPPES Related Questions: customerservice@npienumerator.com
Thank You – Please Evaluate Your Experience

Share your thoughts to help us improve – Evaluate today’s event

Visit:

• **MLN Events** webpage for more information on our conference call and webcast presentations

• **Medicare Learning Network** homepage for other free educational materials for health care professionals

The Medicare Learning Network® and MLN Connects® are registered trademarks of the U.S. Department of Health and Human Services (HHS).