



mln webcast

A MEDICARE LEARNING NETWORK® (MLN) EVENT

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
- NPES – 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 Overview

I&A Provides:

1. Authentication
2. Authorization

Authentication vs. Authorization



Who you are



What you can do

Supports the Following Applications (aka Business Functions):

- a. NPES (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, NPES, 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



I&A MFA Walkthrough and Details Overview – Road Map

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.

	Short Grace Period	Cutoff Date (Days From Deployment)
I&A APP Configuration	30	~300
NPPES APP Configuration	30	~210

	Sep-2019	Oct-2019	Nov-2019	Dec-2019	Jan-2020	Feb-2020	Mar-2020	Apr-2020	May-2020	Jun-2020
I&A MFA Frame Work										
I&A APP MFA Integration										
NPPES APP MFA Integration										
PECOS App MFA Integration										
HITECH APP MFA Integration	TBD									

- 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

Identity & Access Management System [? Help](#)

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:**

* **Password:**

Sign In ▶

[? Forgot Password](#)

[? Retrieve Forgotten User ID](#)

[? Enter your PIN](#)

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. **Create Account Now** ▶

 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.

 Use this system to apply for and manage National Provider Identifiers (NPIs).

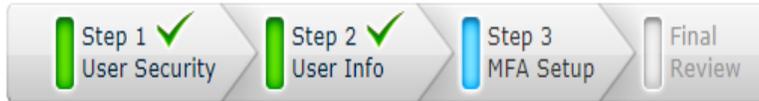


I&A MFA Walkthrough and Details Overview – MFA Initial Setup Cont'd

Identity & Access Management System

[? Help](#)

User Registration - Multi-Factor Authentication (MFA) Setup



[« Back to Previous Page](#)

* indicates required field(s)

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

Continue

[Cancel](#)

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



I&A MFA Walkthrough and Details Overview – MFA Initial Setup Cont'd

Identity & Access Management System [? Help](#)

User Registration - Multi-Factor Authentication (MFA) Setup

Step 1 ✓ User Security Step 2 ✓ User Info **Step 3 MFA Setup** Final Review

[* indicates required field\(s\)](#) [« Back to Previous Page](#)

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:**
Enter your 10 digit phone number the way you normally dial it.

| [Cancel](#)



I&A MFA Walkthrough and Details Overview – MFA Initial Setup Cont'd

Identity & Access Management System ? Help

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

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

[« Back to Previous Page](#)

* indicates required field(s)

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

* Enter Code:

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](#)



I&A MFA Walkthrough and Details Overview – MFA Initial Setup Cont'd

Identity & Access Management System

[? Help](#)

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



[« Back to Previous Page](#)

* indicates required field(s)

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

* Enter Code:

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](#)

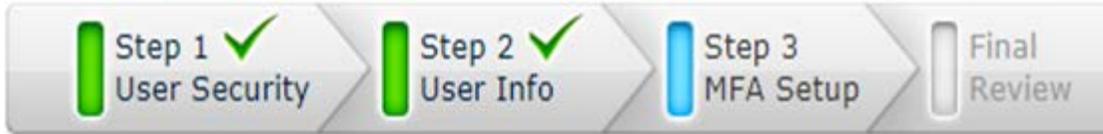
[Cancel](#)



I&A MFA Walkthrough and Details Overview – MFA Initial Setup Cont'd

Identity & Access Management System Help

User Registration - Multi-Factor Authentication (MFA) Setup - Primary MFA Setup Complete



Info 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

[?](#) Help

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](#)



I&A MFA Walkthrough and Details Overview – MFA Login Cont'd

Identity & Access Management System [? Help](#)

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:**

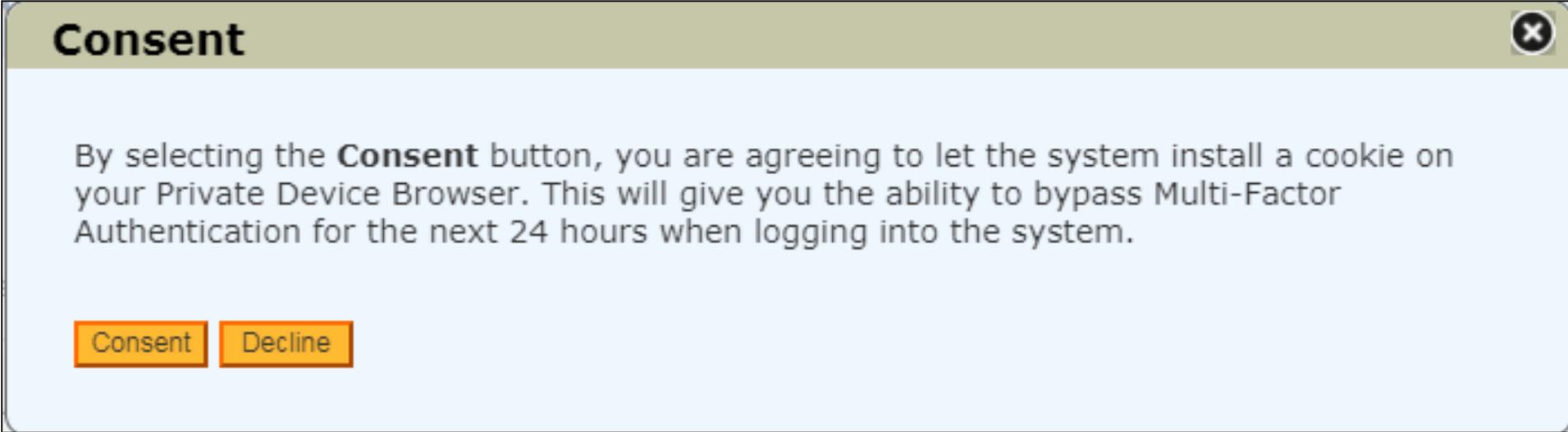
Haven't received the code yet or need a new code? [Send New Code](#)

[Verify Code](#) | [Cancel](#)



I&A MFA Walkthrough and Details Overview – MFA Login Cont'd

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.

A screenshot of a web browser consent dialog box. The dialog has a title bar with the word "Consent" and a close button (an 'X' in a circle). The main text reads: "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." At the bottom of the dialog, there are two buttons: "Consent" and "Decline", both with orange backgrounds and black text.

Consent

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.

Consent Decline



I&A MFA Walkthrough and Details Overview – Optional Grace Period

Identity & Access Management System

 Help

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

 Help

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](#)



I&A MFA Walkthrough and Details Overview – MFA Reset/Unlock

Users who need to unlock or reset MFA will have to answer 3 security questions or provide correct user information to access I&A

Reset/Unlock Multi-Factor Authentication (MFA) - Challenge Information [« Back to Previous Page](#)

Note: To reset/unlock your MFA you will need to successfully complete one of the following two options:

1. Correctly answer three Security Questions associated with your account.
2. Enter the User Information associated with your account.

If you choose Option 1, and are unable to correctly answer three of the Security Questions associated with your account, you will be required to complete Option 2 and correctly enter the User Information associated with your account before being allowed to reset/unlock your MFA.

* indicates required field(s)

Security Questions **OR** **User Information**

***Security Question 1:**
What size shoe do you wear?

***Security Question 2:**
What is your SSN issue state?

***Security Question 3:**
What is your favorite season of the year?

Continue ▶

*** Social Security Number (Enter Last 4 Digits):**

*** Date of Birth:**
Ex: (MM/DD/YYYY)

*** First Name:**

*** Last Name:**

*** Personal Phone Number:**

*** Home ZIP/ Postal Code:**

Continue ▶



I&A MFA Walkthrough and Details Overview – MFA Modify Page

Users can delete/add MFA methods

The screenshot shows a web interface for the Identity & Access Management System. The page title is "Reset/Unlock Multi-Factor Authentication (MFA) - Confirmation". Under the heading "Multi-Factor Authentication Setup", there is a section for "Primary Authentication Method" which lists "Phone Number Text/SMS" with a redacted phone number "(301) [REDACTED]" and a link to "Delete this Authentication Method". Below this is the "Alternative Authentication Method" section, which contains an "Add Authentication Method" button. At the bottom of the form is a "Proceed to Log into I&A" button.



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.



NPPES Multi-Factor Authentication – Road Map

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

NPPES APP Configuration

Short Grace Period
Cutoff Date (Days From Deployment)

30	~300
30	~210

Sep-2019	Oct-2019	Nov-2019	Dec-2019	Jan-2020	Feb-2020	Mar-2020	Apr-2020	May-2020	Jun-2020
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------

I&A MFA Frame Work

I&A APP MFA Integration

NPPES APP MFA Integration

PECOS App MFA Integration

HITECH APP MFA Integration

TBD

- Initial APP MFA Deployment
- Application MFA grace period is applicable within this date range
- Application MFA cut off date



NPPES Multi-Factor Authentication – Login



SEARCH NPI REGISTRY HELP

Registered User Sign In

Log in to view/update your National Provider Identifier (NPI) record.

User ID ⓘ

DrJames

Password

SIGN IN

FORGOT USER ID OR PASSWORD?

*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

Create a New Account

You need an Identity & Access Management System (I&A) 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&A account, need to update your existing I&A account, or don't remember your User ID or Password, select the CREATE or MANAGE AN ACCOUNT button below to go to I&A.



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

After successfully creating your I&A account, return to NPPES and use your I&A 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



NPPES Multi-Factor Authentication – Optional Grace Period

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

NPPES
National Plan & Provider Enumeration System

Multi-Factor Authentication (MFA)

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.

[GO TO I&A TO SET UP MFA](#) [CONTINUE LOGGING INTO NPPES](#)



NPPES Multi-Factor Authentication – Login (After Setting Up MFA)



NPPES
National Plan & Provider Enumeration System





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

[SEND VERIFICATION CODE](#) [CANCEL](#)



NPPES Multi-Factor Authentication – Login – Cont'd (After Setting Up MFA)



National Plan & Provider Enumeration System





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?



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).

