Enrollment: Multi-Factor Authentication for I&A System Webcast

Moderated by Leah Nquyen
July 30, 2019 2:00pm

Table of Contents

Operator: Hello and welcome to today's Medicare Learning Network® event. My name is Britney, and I'll be your web event specialist today. All lines have been placed on mute to prevent any background noise. Please note that today's event is being recorded. During the presentation, we'll have a question and answer session. You can ask text questions at any time. Click the green Q&A icon on the lower left-hand corner of your screen, type your question in the open area and click submit. We will also be taking questions via the phone lines, and instructions on how to do so will be given at the appropriate time.

If you would like to view the presentation in a full screen view, click the full screen button in the lower right-hand corner of your screen. Press the escape key on your keyboard to return to your original view. For optimal viewing and participation, please disable your popup blockers and finally should you need technical assistance, as a best practice, we suggest you first refresh your browser. If that does not resolve the issue, please click on the support option in the upper right-hand corner of your screen for online troubleshooting. It is now my pleasure to turn today's program over to Leah Nguyen. Leah, the floor's yours.

Announcements & Introduction

Leah Nguyen: I am Leah Nguyen from the Provider Communications Group here at CMS, and I'm your moderator today. I would like to welcome you to this Medicare Learning Network webcast on Enrollment Multi-Factor Authentication to The Identity and Access System. Before we get started, there are a few items that I'd like to quickly cover. Today's event uses webcast technology. We recommend streaming the audio live through your computer speakers. Those of you participating via webcast may download a copy of today's slide presentation by clicking on the blue files button at the bottom left side of your screen and please note that this event is being recorded and transcribed.

Today's event is not intended for the press, and the remarks are not considered on the record. If you are a member of the press, you may listen in, but please refrain from asking questions during the question and answer session. If you have inquiries, contact press@cms.hhs.gov. At this time, I'd like to turn the call over to Srini Kunnam from Turning Point Global Solutions.

Presentation

Srini Kunnam: Good afternoon. Thanks Leah and Britney. Good afternoon everyone or good morning if you're in a beautiful state like California and Hawaii. My team and I are very excited to be here presenting to you how Multi-Factor Authentication is going to work in I&A. This is our Identity and Access Management System followed by NPPES. Next slide, please.

Some of you may be familiar with these acronyms. These are the systems we are going to cover in today's presentation. Starting from I&A through NPPES, HITECH and also our helpdesk EUS for I&A. Next slide, please.

Agenda

In today's presentation, we're going to start with I&A. Some of you may be familiar with this and then we'll move on to MFA, and some of you may be familiar with the MFA also. For example, if you're logging into your banking website nowadays, you have to enter your user ID and password. In addition to that, you'll get a text message with a code you need to enter at the time of login. This is going to work similar to what you do on the banking

website. So, we're going to walk you through how it's going to work on I&A followed by how it's going to work on NPPES. Just like Brittney and Leah mentioned, there's going to be a Q&A session at the end. We'll answer all your questions. Next slide, please.

I&A Overview

Let's start with I&A Overview. Next slide, please.

I&A is our Identity and Access Management System. This is a system we use today to access your I&A account, or it could be your NPPES Provider Information or PECOS Provider Enrollment Information or EHR Electronic Health Records Information. For all these 3 websites, you use I&A account. I&A does 2 things; 1 is authentication. So, let's say you are starting as a group practice manager for a Nephrology practice. There are 10 providers in that group and also you have a type II NPI for the group itself and then you need to manage all of that. Since you are brand new, you may or may not have an I&A account.

The first thing you will do is you will go to I&A, and then register yourself. You will enter your email ID. You can pick your own user ID and password and you'll enter all your personal information. Once you do that, it'll get your account activated. That is authentication. With that user ID and password, you can login to NPPES, you can login to PECOS, you can login to EHR. The next thing you need is you need access to the provider in a Nephrology practice. That is controlled by authorization. You may be billing official for some of your provider or you may be a staff end user. Depending on what level of access you are given, you can access the same information and do the business functions in the NPPES, PECOS or EHR. That is the authorization part of it. Authentication is the user ID and password that you login with. Authorization is what providers and business functions you have access to. Next slide, please.

I&A MFA Background and Overview

And now that we know that how I&A works, we're going to see how MFA is going to work. MFA is Multi-Factorial Authentication. This is in addition to your user ID and password. We want to make sure that your data is secure. For example, some of us have a habit of recording your passwords and user IDs in an Excel spreadsheet or in an email or in Post It notes posted next to our monitors, which is not a good idea. If a hacker were to get a hold of your user ID and password, then a hacker may be able to access your account. We don't want that. So, what we are going to do is we're going to protect that with a second factor.

This factor will be sent to you at the time of login, so you don't have to remember, you don't have to write in an Excel spreadsheet, this is just one time. The next time you login, you get a different second factor. Why are we doing it? Because we care about you, we care about your data, you want to make sure that your data in NPPES, PECOS, EHR and I&A is secure. In I&A, we will start with I&A that is going live on September 9, 2019, and then you will see the complete roadmap shortly. Slide number 8, please.

I&A MFA Walkthrough and Details Overview

Next, we will walk you through the screens of how I&A is going to work shortly. The first thing is there are 2 categories of users going back to the example of you starting with a Nephrology practice.

If you don't have an I&A account, you'll be considered as a brand-new user. If you were to register yourself in I&A after September 9th, which is when we're going live with MFA, you have to register with MFA on day 1. Some of you may be using I&A today. In that case, you're considered as an existing user. We care about you also. So, what we want to do is we want to give you a 30-day grace period because on day 1, you may not be ready to register yourself because you want to get going with whatever you need to do on NPPES, PECOS and HITECH. In that case, we understand that. So, we give you a 30-day grace period from that time you login for the first time after September 9th.

So, existing users get a 30-day grace period, new users have to register with MFA on day 1 starting September 9th. The next question is what devices can I use? You can use your cell phone. Now, most of us have cell phones. You can use that to get a text or you can use your email, it could be the email of your choice. The third option is you can use your phone number to get a phone call. It could be a landline, or it could be a cell number, whatever you prefer, and you can have up to two devices that you can add. For example, I may have my cell number as my primary device, or I may have an alternative method like my email ID. Next slide, please.

This is the road map I was referring to before. Everybody, all the existing users get a 30-day grace period. That is what you see at the top. And then the next diagram on the middle, we are showing you our dates for implementing I&A MFA. That is going live in September on September 9th. And then below that, you see NPPES that is going live in December, to be precise on December 9th, and then followed by PECOS in the April of next year. By June 2020, all the systems that are listed here, I&A, NPPES, PECOS and HITECH, they'll all be requiring you to use MFA. Thereafter, sorry, no more grace period. Next slide, please.

Here is the screen that might be familiar to some of you. This is the login screen for I&A. Going back to the example of you starting with a Nephrology practice, you go to the right side to create an account now. If you have an I&A already, you login with that I&A account by entering the user ID and password. On this screen, you see the MFAuser7 that is the sample user ID we've picked for you today, and then you hit the sign in button or the create account button. Next slide, please.

Irrespective if you're a brand-new user or an existing user, MFA process is pretty much similar. The first thing you need to do is what is your preferred method of getting the code. It could be your email, or it could be your cell phone where you want to get a text, or it could be a landline where you prefer getting a phone call. So, you can pick your primary method. So, in this case, I'm going to pick up my phone number, text SMS, which is the first choice, and then I'm going to go to the next screen. Next screen, please.

So, I've selected my phone number, text SMS, and then I am going to enter my phone number here, and then I enter my phone number, and then I hit the button send text or SMS. Next slide, please.

Once I do that, I get this screen. Here is where I need to enter the code. I will get a six-digit code if I were to pick my SMS text as my primary option or email and the code is just five digits long if it is a phone call, that's one less digit to remember when you're attending this phone call. So, you enter this code here, six-digit code or a five-

digit code. Five-digit code is only for phone calls, six digits is for email and text. You enter that here and then you can hit the button verify code.

There is one more functionality here. You see that resend text SMS. Let's say you are about to enter. That's when your boss calls you and says, “Hey can you do this for me?” and then you get distracted and then the code will expire in 5 minutes if it is through text or a phone call. If it is through email, your code will expire in 15 minutes. So, within the time limit if you don't enter, all you have to do is hit the resend button. That way you can get a fresh code and then you can enter it here and then hit the button verify code. You enter that code and then you hit verify code button. Next slide, please.

In this example, I'm entering the code as 796845 that I got to my cell phone as a text and then I'm going to hit the verify code button. As soon as I hit the verify code button, you'll see the next screen. Next screen, please.

Here, that's it. You're done. You get a congratulatory message at the top with your phone number and then everything is done. So, what I did was I picked my preferred method of authentication and then I entered the phone number and then I entered the code I got as a text and then I completed it. So, this is it. Your registration is complete. You may see in the middle of the screen begin alternative setup.

So, here is the used case. Let's say go to a nice beach for my summer vacation and then we all know that the cell phones are attracted to water and then I dropped my cell phone on the beach, it gets completely wet and it stops working. The next day I come into work, I need to have a way to login to I&A. So, the best thing would be for me to setup an alternative way. That way, I can use the phone number if it is available or if I happen to get it wet at the beach, I can setup an alternative way like my work email address to get the same code. That way the next day when I come into work, I'll still be good. So, that is optional. You can do that by setting up begin alternative setup. Next slide, please.

So, with this, you're pretty much set. Next time onwards when you login to I&A, you're going to be prompted with the screen as soon as you enter your user ID and password. When you enter this, you're going to see your primary authentication method and also the alternative method. In this case, I didn't setup one. If I had setup one, in the upcoming slides you'll see that example. So, my primary device is stored here and then also displayed here, and then I know I recognized the last four digits of my cell number. I know that this is the right number and then I hit the button, send verification code. This screen you will get after entering your user ID and password after September 9th and after setting up MFA. Every time you login, you'll see the screen. Next slide, please.

Here's another important functionality, some of your power users. You login to I&A multiple times a day. In that case, we have a feature where we will remember your computer in this case or any device that you use to login to I&A for the next 24 hours. For that, all you have to do is select the radio button that says this is a private device. Once you do that and enter the code, then you hit the button verify code, you're good for the next 24 hours. All you have to do is enter your user ID and password every time you login for the next 24 hours.

You don't have to worry about getting a text and entering it because we understand that you have a lot of things to do, and then we want to make it a little bit easier for you to login every time. One thing we would do is we're going to show you on the screen once you select the, this is a private device. Next slide, please.
We're going to show you this consent popup box. This is to make sure that you allow us to store a little file cookie on your machine that maybe can remember your choice and also your computer for the next 24 hours. That way,

our system won't prompt you with a second factor request. Obviously, you don't want to use this option when you're at a library, and using the library computer make sure that you use this option when you're using a trusted computer like your work computer. Next slide, please.

Remember the existing users get an optional grace period. Let's say I'm within the grace period, this is after September 9th and then I have a I&A account already. I login for the very first time. This is the screen I will get. At this time, I have a choice. I can setup my MFA authentication now or I can come back and set it up if I am busy with something else. So, this is the optional grace period. You will get the screen for the next 30 days after September 9th from the first time you login to I&A. After the grace period ends, you have to setup your MFA. Slide 21, please.

Remember that example where I went to the beach and then got my cell phone wet? In that example, obviously I didn't setup an alternative method. So, the next time I come into work, unfortunately, the phone ending with 9321 doesn't work anymore, and I still have to login. In that case, I can hit the button that says reset MFA. Once I do that, we're going to show you on the next screen what you need to do. Next slide, please.

So, in this example, I lost my phone and I have to login to I&A, and unfortunately, I didn't setup an alternative way. So, when I hit the button reset MFA, you are prompted with this. In this case, some of you may remember your security answers still. If you don't remember, you have to enter your personal detail. If you get three chances to get them right, if you enter them correctly, then you can reset your MFA. You can pick a new device, new email address, new cell phone.

For example, you move on to your new job and then you get up shining your iPhone from your new employer, with a new phone number, and then obviously you want to change that. In that case, you can set the reset button, come to the screen, answer the security questions correctly or enter your personal information correctly and then you will be given an option to setup your MFA device or delete the old ones. Next slide, please.

So, in this example, I lost my phone, I hit the reset button and then I entered my security questions answers correctly or I entered the personal information correctly. I am prompted with this screen. Here, I can delete my authentication method. For example, my phone number is not valid anymore. I got a brand-new phone, I can delete it and setup an alternate one under primary one or my phone number works, but unfortunately, I don't have my phone with me, I left it at home. In that case, I can use the alternative method, setup my work email address and then I get the code and then I can go on with whatever I need to do on I&A. Next slide, please.

NPPES Multi-Factor Authentication

Okay. That's how I&A is going to work. After September 9th, you just login, use your grace period or you setup MFA on day 1. You can use your cell phone, voice call or email to get your code. This is similar to how the banking websites work nowadays. So, once you setup your MFA and I&A, then you're set. When we go live with NPPES on December 9th, all you have to do is start using MFA on NPPES also, but if you haven't set it up, don't worry. You'll get a 30-day grace period if you just use NPPES. Next slide, please.

Remember this roadmap. We talked about your grace period after 30 days for existing users, we talked about I&A going live in September. Now, we're going to focus on NPPES. NPPES is going live on December 9th with

Multi-Factor Authentication. We're doing this in steps, first I&A, then NPPES, then PECOS and then HITECH. PECOS is scheduled go live in April. Next slide, please.

Here is the MFA login, before that, this is the NPPES login page. Here, I am logging in as Dr. James and next slide, please.

Remember the optional grace period you get in NPPES. As soon as I login after December 9th and within the optional grace period, this is the screen I'm going to get and unfortunately, I haven't setup my MFA and I&A yet. So, I have two options. I can use a grace period and continue logging into NPPES during that time or I can take this opportunity if I have a couple of minutes to setup my MFA and I&A. Remember, you always setup your MFA and I&A even though you may use NPPES, PECOS or HITECH, you always go back to I&A to setup your MFA and also reset MFA if you have to. Next slide, please.

Now, I have setup my MFA in I&A and then logging in NPPES. Luckily, I setup my primary method and then I also setup my alternative method. I'm going to choose the first one, primary authentication method with the phone number ending with 6770. I know that is my phone number. I'm going to hit the button send verification code. Next slide, please.

This time, I have prompted. This is similar to what you saw in I&A. You have the option to remember your device for the next 24 hours. So, in this case, I am going to say that I am choosing public device, but you can also choose it's a private device if you are using your work computer and then you enter your code and then hit verify code. If you didn't get the code and then you waited a couple of minutes, if you haven't received it, it was lost in cyberspace. All you have to do is send a new code button. Click the new code button and then you'll get a new code that you can enter. Next slide, please.

So, that concludes how MFA is going to work on I&A followed by NPPES. All you have to do is pick a device, get the code, enter it and then thereafter start using it whenever you use I&A or NPPES. If you are an existing user, you get a 30-day grace period. If you are a new user after September 9th, you have to set it up on day 1. Now, I'd like to turn over the control to Leah to conduct the Q&A session.

Question & Answer Session

Leah Nguyen: Thank you Srini. Our subject matter experts will now take your questions. Throughout the Q&A session, we'll ask webcast participants to provide feedback about their experiences with the technology used today. Remember to disable your popup blockers for best results. We will begin our session by answering a few questions that we received from webcast participants and then take each question from the phone. Operator, please prompt the telephone users and begin to compile the Q&A roster. Operator, can you please give the instructions to compile the Q&A roster for the telephone participants?

Operator: Certainly. As a reminder, to ask an audio question, do so by pressing star and the number one on your telephone keypad. Again, that is star one. You may withdraw your question at any time by pressing the pound key.

Leah Nguyen: Okay, and while you compile the roster, we'll start taking some questions from the webcast and our first question is. How long will my MFA code last?

David Hong: The MFA code will last for 5 minutes if you are using SMS or using the voice call. If you are using email, that will last for 15 minutes.

Leah Nguyen: Great thank you. Our second question is. Can the system handle international phone numbers?

David Hong: It is not supposed to handle the international phone number. It will handle all the US territories phone numbers.

Leah Nguyen: Looks like we have one more from the webcast. Am I required to setup two methods of MFA or just one?

David Hong: You only required to setup one. You can add your second one later on if you wanted to, but when you set your account, you can setup only your primary account and you can see your MFA setup correctly.

Leah Nguyen: Thank you, and operator, do we have any questions from the phone line?

Operator: You do have a question from the line of Barbara Sorenson.

Barbara Sorenson: -- need to revalidate their Medicare enrollments every 5 years. Is there a problem with them waiting 4 to 5 years to go in and update the I&A?

David Hong: My name is David Hong. So, I'll answer the question. Yes. If you don't login to I&A every 4 and 5 years, let's say after September 9th, you go in there 4 years from now and login for the first time. What's going to happen is that it would force you to setup your MFA before you can actually login to either PECOS or NPPES or HITECH.

Barbara Sorenson: Okay. Okay. Thank you.

Leah Nguyen: Thank you. Now, let's take another one from the webcast. Can the MFA email be the same as the email listed on the primary email address field within I&A? If not, does the MFA email need to be a unique email or could it be shared? For example, the same email for a group of physicians in the same clinic.

David Hong: There's no limitation of whether or not you use the same email. You can use that same email or different email. For the second part of the question of whether or not the email can be shared. Technically, you can, but it is not recommended.

Leah Nguyen: Here's another one from the webcast. Can the alternate method see a generic email, or does it have to be specific to provider?

David Hong: Similar to the previous question, yes, you can use a generic email if you want to, but it is not recommended.

Leah Nguyen: Thank you, and can we take another question from the phone?

Operator: As a reminder in order to ask an audio question, please press star and the number one on your telephone keypad. Again, that is star one.

Leah Nguyen: All right. Perfect. We have another one from the webcast. If using a cellphone or landline, does the number need to be unique per practitioner or can it be the same, say for multiple docs in a group?

David Hong: Technically, you can use the same number for multiple doctors, but again this is not recommended.

Leah Nguyen: And our next question is, you have to enter in an alternate method at creation of account or can you add a method later?

David Hong: Yes, you can add the alternative method later. You actually can adjust or change your MFA method later or at any time.

Leah Nguyen: Our next question is, do you need to get a new code from MFA upon every login outside of the private device that allows for 24 hours?

David Hong: Correct. You would have to get a new verification code or every time you login.

Leah Nguyen: And I'm sorry, next question is, will I&A still lock you out completely if you go over more than 180 days without changing your password?

Carl Schell: Can you repeat the question?

Leah Nguyen: Will I&A still lock you out completely if you go over more than 180 days without changing your password?

Srini Kunnam: If it prompts to reset your password – or it could lock you.

David Hong: Yes, it will work the same. The MFA implementation does not change the password or change the policy.

Leah Nguyen: Okay. Let's take another question from the phone.

Operator: You have a question from the line of Gloria Baltavar. Gloria your line is open.

Gloria Baltavar: Yes. We're a health care provider and we use the NPPES to search and make sure that the NPI is correct and it's valid. Do we still have to create an account?

Leah Nguyen: Can you repeat your question?

Gloria Baltavar: Okay. We are a health care provider and we use the NPPES to verify, all we do is search. Would we still need to create an account?

David Hong: Assuming you're using the NPI to search, no you don't have to create an account.

Gloria Baltavar: Okay.

Leah Nguyen: Thank you. And our next question from the webcast, does the private computer option remember your login and what if more than one doctor uses the same computer for enrollment purposes?

David Hong: The private computer consent is based on per user per computer. So, if you have two users logging into same computer, each of them will have their own reference of their cookies.

Leah Nguyen: Thank you, and our next question is can any preferred email address be used for MFA or does it have to be the email address associated with the particular I&A account?

David Hong: It doesn't need to be the particular address. You can use any email address you preferred.

Leah Nguyen: Thank you, and can we take another question from the phone?

Operator: As a reminder in order to ask an audio question, please press star and the number one on your telephone keypad. Again, that is star one.

Leah Nguyen: I'm sorry. We'll take another question from the webcast. Why deploy different dates for NPPES and PECOS since I&A logins have to be changed every 60 days and those are shared on the other account? Other deployment dates seem unnecessary?

David Hong: Fair questions, but basically when we are looking to the schedule, they are some occasions or chances where you will actually have your I&A account for setup or not setup and you're going to NPPES setup or not setup. Then, we actually play with different configurations and we still believe that giving the grace period for each and every application will allow the best flexibility for us to make sure that all the applications will migrate to MFA gracefully.

Leah Nguyen: Thank you, and our next question is how many alternate addresses can you have?

David Hong: Can you clarify the question?

Leah Nguyen: That's all that's there.

David Hong: I think what you meant is probably the alternative MFA method. If that is the question, only one. So, you have one primary and one alternative.

Leah Nguyen: And our next question from the webcast is can you setup the MFA prior to September 9, 2019?

David Hong: No, you don't have the capability to set that up until we started deploying or we have completed deployment on September 9th.

Leah Nguyen: The next question is will we still be required to update our password every 60 days?

David Hong: Yes.

Leah Nguyen: I thought I'd remember that one. And our final question right now is so do you have to get an MFA code for each system every day?

David Hong: Yes, except if you have your private consent to allow yourself to bypass it for 24 hours, but on the next day, you still have to get it. Yes.

Leah Nguyen: And hold on for just one moment. All right. We have one more from the webcast. What happens if the MFA is never setup?

David Hong: If you never setup and you never try to login, nothing will happen, but the next time you try to login, let's assume either your application grace period is passed or your application cutoff date is passed and you try to login any subsequent day, the system will force you to setup MFA. If you do not want to setup MFA, it will just continue to be an account without an MFA setup, but you cannot login.

Leah Nguyen: And the next question is, do the staff end users have to create their own I&A account in order to work on behalf of their organization in PECOS and NPPES?

David Hong: Yes.

Carl Schell: I highly recommend it.

Leah Nguyen: Okay. All right. Hold on for just a moment.

All right. We're getting more questions. Can you use two email addresses as MFA: one primary and the other secondary?

David Hong: No, that is not allowed. When you setup primary and secondary method, it has to be something different. So, you cannot use two SMS or two emails. It has to be one type. The primary and the secondary has to be different type of MFA.

Leah Nguyen: All right. Let me get our next question.

Our next question is if an existing user is trying to access PECOS, is required to make a password change in I&A, will they be required to setup MFA right away before they can change their --.

David Hong: -- password?

David Hong: So, it depends on whether or not you have passed the I&A grace period. So, basically you -- when you want to change your passwords to PECOS, you will need to go into the I&A application and depending on whether that is the first time you're log into the I&A after the I&A deployment date or it was past your I&A grace period, you may or may not need to setup the MFA. It's purely based on assuming that you're logging to the I&A on the day that you try to change your PECOS password.

Leah Nguyen: Our next question for the webcast is who is required to use Multi-Factor Authentication?

David Hong: Every user.

Leah Nguyen: Ok great. And can we take a question from the phone?

Operator: You have a question from the line of Cheri Hooper.

Cheri Hooper: Hi. I'm questioning the difference between public device and a private device?

David Hong: Yeah. So, public and private device are basically any public device – any private device is something that is your own. You know that is safe, it's no accessible by other people that is like a loose fascination, but for the purpose of the selection, it's basically wanting to if you are not using your own safe device, don't try to consent the cookies, otherwise you might compromise your account. If you're in doubt, you can just use public all time then get the status. You just have to type in your MFA code.

Leah Nguyen: Thank you.

Cheri Hooper: So…

Leah Nguyen: Go ahead

Cheri Hooper: I was going to say, so if you're using your work computer, then you would use public device?

David Hong: Most of the time when you use your work computer, we consider that private because it's your own. It's safe, it's not publicly used.

Cheri Hooper: So, you're not talking about what we're using for the MFA like if I use my private cell phone, that's not the question you're asking.

David Hong: We're not talking -- of the MFA. We're talking about the computer that you use to log into I&A.

Carl Schell: So, I think a good example would be for a public device if you were in a library where multiple people are able to use that computer and it's not just something that you use by yourself, but a private device is something where you know that you are the primary person using that device at most times.

Cheri Hooper: Okay. So, again if you're at work and you're using that device, would it be private?

Carl Schell: Correct.
Cheri Hooper: Okay. Thank you.

Leah Nguyen: Thank you, and another question from the webcast. What is the cutoff date for all I&A users are required to use Multi-Factor Authentication to access I&A?

David Hong: June 2020.

Leah Nguyen: Okay. Good. All right let's see what other questions we have from the webcast. What happens if you are a company that completes applications on behalf of field clinicians?

Carl Schell: Sure. Hi, this is Carl Schell from CMS. Typically, we suggest that if you're in I&A, you should have your own account and you should establish surrogacy connection with -- or employer connection with each one of these people who have their I&A accounts for accessing. We definitely do not encourage sharing of accounts.

Leah Nguyen: And our next question is can you have one email for all of your providers in your group for verification? We have 40 providers.

David Hong: Yes, similar to the previous answer. Yes, technically you could, but it's not recommended. We really prefer to have the I&A user to have their own MFA factor. That's the purpose of adding this another layer of security.

Srini Kunnam: You know just add to what David Hong said, this is Srini. That's where the employer-employee relationship is helpful. So, in this case, you are the employee with all the 40 providers as your employers. That way you can manage that account. All you have to do is just sign up for one I&A account for yourself and then you can manage others information.

Leah Nguyen: Our next question is as long as I'm a staff user for the provider, does it matter if they do not login?

David Hong: Yeah. Believe if you were able to do all the functions that a provider needed to do as the desktop end user is okay for provider, not setting up the MFA because they wouldn't login themselves, so it's falling in the same category if someone doesn't login for many years what's going to happen or they will have an account that is not enabled, but since you have the staff end user, that can manage for the provider if it's actually going to be okay.

Leah Nguyen: Can we take another question from the phone?

Operator: You have a question from the line of Marie Grainey.

Marie Grainey: Yes, hello. I work on behalf of 13 providers. So, when I login, can I use my personal cell phone for the MFA? Can I setup my personal cell phone for that?

David Hong: Yes, you can. May I clarify, are you logging as yourself and manage the other providers or are you logging on their behalf directly into their account?
Marie Grainey: I would be logging on their behalf.

David Hong: Yeah, that is not a recommended practice even though technically you can do it, but Carl is here as mentioned, this is not recommended.

Carl Schell: Yeah, I mean according to CMS -- practices, the idea is that it's supposed to be one account per one person and you're not supposed to be able to access other people's accounts using their private login information. The ideal way to handle that is to setup surrogacy or employment connection to each one of their

accounts so that you can manage everything with your one single log on. So, in that case, you would be able to use your personal cell phone for MFA, but you would only have to have that in your own account and you would be able to access all the other accounts through your one login.

Marie Grainey: I see. Okay. All right. Thank you.

Carl Schell: Yes.

Leah Nguyen: Thank you. And we have another question from the webcast. When all is implemented on -- in June 2020, can you go to any system to start the day so to speak and get your MFA start the 24-hour clock?

David Hong: I assume you're talking about the private computer consensus. Right now, it is configured that each application would actually track it separately. If you are logging in into I&A, NPPES and PECOS at a different time, the 24 hours is based on per computer per user per application so you might have to login three times.

Leah Nguyen: And our next question is I have I&A newly to my office. I've just started using it in the past month. So, this MFA is pulling out all three of the functions together to have – hold on – to have one password for NPPES, PECOS etc.?

Carl Schell: So, hi, this is Carl from CMS. So, I&A allows you to setup one account and it allows you to access NPPES, I&A, PECOS and HITECH using one password. It does not currently allow you to login once and share that login session with all of the applications. Every time you go to each one of the applications, you will have to login and also do MFA for each one of them. Unfortunately, that's the way it is right now. We're looking into the future to potentially have a unified login system where it will work across the applications, but there's no timeline for that.

Leah Nguyen: And our next question is if the MFA is a setup I&A, does that cover the NPPES and PECOS setup at the same time?

Carl Schell: So, this is Carl again. So, once you set it up in I&A, you won't have to set it up separately for NPPES and PECOS. That same MFA method will work in all systems.

Leah Nguyen: And our next question from the webcast. Aren't the alternate -- aren't the alternate information the type of information that's stolen slide 22, meaning MFA isn't secure since you can bypass it?

Carl Schell: So, right now that is our only method both with the alternative questions that you have there or the private information. I think that one of the things that we're trying to do is make sure that anyone who logs in does have a secure way of making sure that they have a secondary factor of authentication. You are correct that a lot of times that information is stolen, and we will most definitely take that back and pass it through our CMS security team to make sure that we're not making any mistakes there.

Leah Nguyen: Thank you. And can we take a question from the phone?

Operator: You have a question from Barbara Sorenson.

Barbara Sorenson: Hi. My question is currently PECOS, when a provider needs to electronically sign an application, they can use a pin that Medicare sends them to bypass the login in PECOS to electronically sign an application. Will that still be an option, and will that pin allow them to bypass the MFA regulation as well?

Carl Schell: Hi. So, this is Carl again. The pin for provider signatures won't be affected at all from MFA.

Barbara Sorenson: Okay. So, if they have not setup MFA yet and then they go in with a pin, that's not going to require them to setup MFA to electronically sign the form?

Carl Schell: Correct.

Barbara Sorenson: Okay. Thank you.

Leah Nguyen: Thank you, and our next question from the webcast. What if a provider staff updates the passwords? How will this MFA work?

David Hong: When they update a password, it does not necessarily have to trigger the MFA change because they're tracked independently. If the person already has the password and account they also have the primary MFA factor setup, 2 days later they go change that password that MFA factor would not need to be adjusted. So, whatever it is there, will continue to be there.

Leah Nguyen: Our next question is can a billing company create their own login and link multiple providers via surrogacy to that login and update information on their behalf?

David Hong: Yeah, that's correct. That's how the surrogacy is supposed to work.

Leah Nguyen: Thank you, and can we take a question on the phone?

Operator: You have a question from the line of Liz Schoenknecht.

Liz Schoenknecht: Hi. I'm a staff end user for a group of providers, and I have surrogacy on their accounts, but I just wanted to be clear about that. If I'm doing a revalidation for the provider, they would still need to login and have that MFA in order to sign off. Is that correct?
Carl Schell: Yes. So, this is Carl again. No, that's actually not correct. So, I'll give you an example. In your situation, you have your own I&A account and you're connected to each one of these individual accounts as a staff end user, you will have to setup MFA and you'll have to have that setup correctly. But when you go to login to, let's say, PECOS to do a read out, then you wouldn't have -- then you would have to use your MFA. But at no point in time would you have to go and get every single one of those people that you're connected to, to setup their MFA until they want to access their own account. Did I answer your question?

Liz Schoenknecht: I must not understand then because I thought when I do a revalidation for a provider, it is asking for them to sign off on that?

Carl Schell: If they -- Yes, correct, I'm sorry. I didn't realize that was the extent of question. If they need to come in and login to PECOS in order to do the signature, then yes, they would have to setup their MFA before they're

able to login, but if you use the electronic signature pin that is sent to them through email and they can click that link and sign, they wouldn't have to necessarily setup MFA.

Liz Schoenknecht: Oh okay. Thank you.

Carl Schell: You're welcome.

Leah Nguyen: Thank you. And we have another one from the webcast. As a surrogate, how might I assist our providers in keeping their accounts current if the passwords need to be reset for all providers every 60 days? Will I be able to keep current passwords for all of my providers?

Srini Kunnam: As a surrogate, you should have access to their accounts, the NPPES information, PECOS information and HITECH information. So technically, they don't have to login and change their passwords unless you want them to give you additional business functions or if you want to do a role change from staff end user to a delegated official. So, only time they need to login with an MFA is whenever they want to give you additional business functions or additional authorizations. Without that, you can just login and manage their information.

Carl Schell: On the off chance – Sorry. On the off chance that they do login after 60 days, they would then have to reset and change their password, but it is not necessary for you to force them to come in before every 59 days and reset their passwords across the board. It's just the idea that that password does need to be changed 60 days and beyond.

Leah Nguyen: Thank you. And can we take another question from the phone?

Operator: You have a question from the line of Kathleen Marcin.

Kathleen Marcin: Yes. I'd like to know we're staff end uses for a large group and we currently use DocuSign to have our physicians sign their verification statements and then we upload them. Can we continue to use that process?

Carl Schell: Yes, you should be able to.

Kathleen Marcin: Thank you.

Leah Nguyen: Thank you, and we have another question from the webcast. When can we start to register our phone and email addresses for MFA?

David Hong: You can start doing that after the system go live and that is September 9th.

Leah Nguyen: Thank you. Let me check to see if we have any more questions.

Okay. We have another question from the webcast. Regarding the E-signature process, wouldn't a provider just need to login with the sign-on link provided by CMS to e-sign their apps?

Carl Schell: Hi Jane, this is Carl. I think, yes, you are correct. They would only need to log on with that sign-in link. I think what you're saying so there's an e-signature process that's sends out a unique link with a code attached to it where they can click and then sign the application. That will not be tied to MFA. If they do need to sign in or login to PECOS in order to see what signatures are pending, then anytime you sign in with your username and password, you would have to do the MFA process.

Leah Nguyen: Thank you. We have another question from the webcast. I know it's unrelated, but rads can DocuSign for PECOS app?

Carl Schell: I'm sorry. I'm not exactly sure. I don't understand the terminology for rads.

Leah Nguyen: Can we see if we have any more questions?

Carl Schell: Maybe this is related to the previous question, but I believe that there is functionality in certain cases where you can upload a signed – a signature page for an application, but yeah that is off topic, and I don't have the full details for that.

Leah Nguyen: We have another question from the webcast. At a 180 days after password expires, doesn't the I&A account lock up somehow requiring a doctor to call in to unlock the account?

Srini Kunnam: No. After 180 days, you can reset your password if you remember your old password. If you don't remember your old password, you can use our reset functionality to -- by answering the security questions and answers or by entering the doctor's personal information. If you don't get them correct in three attempts, that's when you need to call.

David Hong: Regarding to the previous question, rads are the radiologist.

Carl Schell: I'm sorry what --?

David Hong: Regarding to the previous question, rads are the radiologist.

Carl Schell: Oh, okay.

David Hong: And they'll ask for your last name.

Carl Schell: My full name is Carl Schell. It's Carl.schell@cms.hhs.gov. I see the other question there that was asking about DocuSign. If you can send me that information, I can make sure it gets sent on to the right person.

Leah Nguyen: Thank you, and can we take another question from the phone?

Operator: We have a question from the line of Cheri Hooper.

Cheri Hooper: Hi. It's me again. So, what happens when a provider does not know their username or – that's it basically do they -- can they get in without an MFA setup?

David Hong: Yes. If they …

Srini Kunnam: Yeah. Hi. This is Srini. Let's say I forget my user ID. If you go to the login page on I&A, you can do the forgot user ID. You can click that link and then you can answer the security questions, the answers for the security questions or you can enter your personal information. So, you have three chances to get them right. If you don't get them right, that's when you need to call.

Cheri Hooper: Okay and you call EUS, is that what you're saying?

Srini Kunnam: Yes.

Cheri Hooper: Okay. Thank you.

Srini Kunnam: You're welcome.

Carl Schell: And I was just also going to answer the one additional question is how to spell my name. So, it carl C.a.r.l. schell S.C.H.E.L.L. @cms.hhs.gov. So, I think someone was breathing out at the exact same time I was saying that so I will say it again. Carl.schell@cms.hhs.gov.

Leah Nguyen: And we'll take another question from the webcast. So, once in a staff end user, the provider never needs to login and setup MFA as I would be able to complete updates correct?

David Hong: Correct, except when you need to have a role change or some other functions that the provider himself needs to do, but for the most part on a day-to-day, they don't have to.

Additional Information

Leah Nguyen: All right. Thank you. Unfortunately, it looks like that all the time we have for questions today. On Slide 33, you'll find information on how to evaluate your experience with today's event. We'll also push out the link to the evaluation to our webcast participants right now.

Evaluations are anonymous, confidential and voluntary, but we hope you'll take a few moments to evaluate your experience with today's event. As a reminder, disable your popup blockers for best results. An audio recording and transcript will be available in about 2 weeks at go.cms.gov/npc. I'd like to thank our subject matter expert and all our participants who joined us for today's Medicare Learning Network event on Enrollment Multi-Factor Authentication for the I&A System. Have a great day everyone.

Operator: This concludes today's call. Presenters, please hold.