



# **EPCS Provider On-Boarding Manual**

## Table of Contents

EPCS Identity Proofing Checklist .....	3
Considerations Before Starting Enrollment.....	4
EPCS Enrollment Steps .....	5
User Registration.....	11
Registering Tokens .....	14
Creating a Passphrase .....	17
Experian Transaction Number .....	19
Re-Authentication .....	21
EPCS Logical Access Control (LAC).....	23
Auditable Event Alerts.....	27
Frequently Asked Questions (FAQs).....	28
Resources .....	29

# EPCS Identity Proofing Checklist

Items marked with a \* are required, while the other items are recommended, optional or only necessary for specific circumstances.

1. Hard and/or soft EPCS token (recommended to have at least two tokens) \*
  - a. Hard token: Keychain device provided by DrFirst
  - b. Soft token: VIP Access by Symantec can be downloaded on a mobile phone, tablet or computer from this link <https://vip.symantec.com/>
2. Social Security Number\*
3. DEA number and state- DO NOT use a Narcotics Addiction DEA Number (NADEAN)\*
4. You will have to create a passphrase that is a minimum of 8 characters with at least one capital letter, one lowercase letter, and a number during the enrollment process\*
  - a. A passphrase is necessary for the two-factor authentication step required for sending controlled substance prescriptions
  - b. It is **HIGHLY** recommended you write down the passphrase to save in a secure location
5. You will have to create a security question and answer (necessary for resetting your passphrase)\*
  - a. Example: Mother's maiden name or make/model of your first car
  - b. Security answers are case sensitive so please note down your security question and answer exactly as you entered it
6. Valid personal phone number (mobile or residential—must be associated with home address)

**Please Note:** It is **HIGHLY RECOMMENDED** that you enter a mobile phone number so if it can be validated, you may receive your transaction ID instantly by SMS text message. Alternatively, you will receive a letter via USPS mail (takes approximately 5-6 business days).

7. First eight digits of a personal credit card (VISA or MasterCard) – no business or debit cards. This information is **NOT MANDATORY** and can be omitted

## Considerations Before Starting Enrollment

8. If you completed EPCS credentialing previously please skip to [Page 21](#).
9. If you have a security freeze in place for your Experian credit account, you MUST remove it before starting enrollment.

**Please Note:** IDP cannot be passed if there is a security freeze on your Experian credit account.

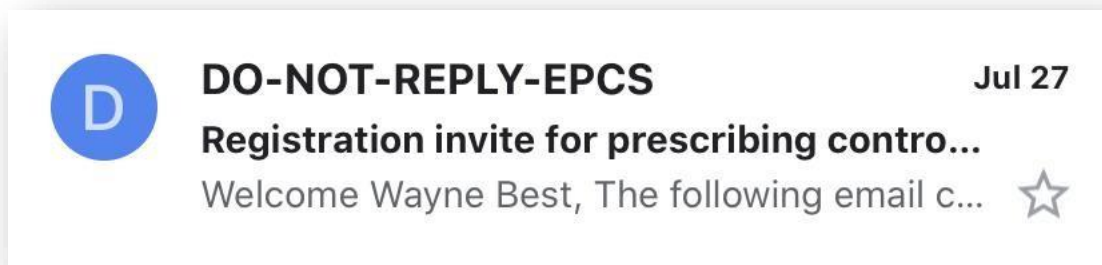
- a. Instructions on how to remove a security freeze can be found at [www.experian.com](http://www.experian.com) under "Credit Support".
10. In order to review the information that Experian has on record, you can obtain a Free Experian credit report from [www.annualcreditreport.com](http://www.annualcreditreport.com). If any discrepancies are noted, please contact Experian on the number in the report to resolve them.
  - a. Identity proofing questions are formulated based upon credit history. This includes but is not limited to questions about home/auto loans, bank accounts, places of residency, etc. Having a credit report available can assist in answering these questions.

# EPCS Enrollment Steps

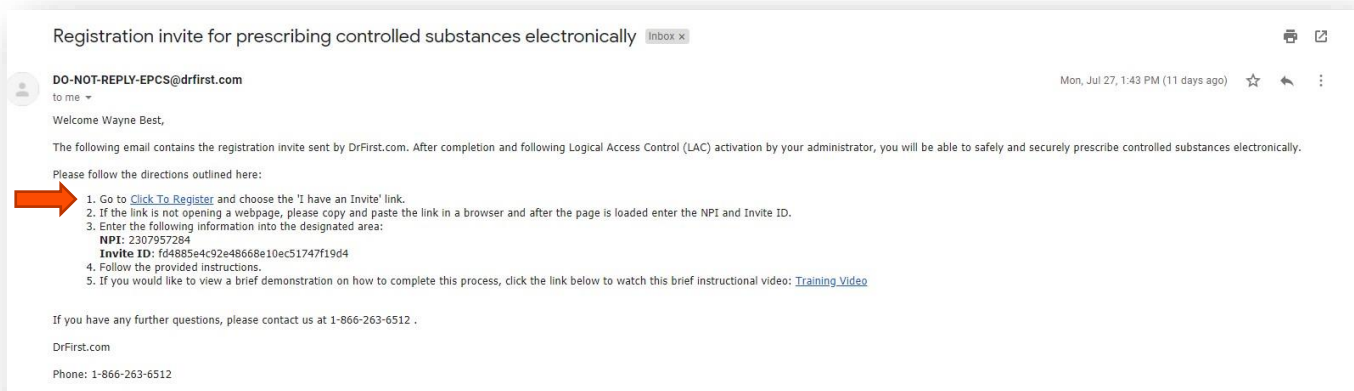
Every EPCS provider will receive an invite from DrFirst ([DO-NOT-REPLY-EPCS@epcsdrfirst.com](mailto:DO-NOT-REPLY-EPCS@epcsdrfirst.com)).

The provider must follow the instructions in this email in order to complete EPCS enrollment process, which includes the IDP Process (Identity Proofing) and activating token devices. If you are unable to find the email, please check your junk/spam folder.

**Please Note:** Do not begin without at least one EPCS token. Even if you complete the IDP process, you cannot complete the last step without your token present.



1. Upon opening the email, click the **Click To Register** hyperlink on step 1 of the email. The invite email contains an **Invite ID**. Please save this email with the **Invite ID** in case you are unable to complete the process and have to re-access this information later.



2. This link will take you to a page where your **NPI #** and **Invite ID** will be pre-populated in the **I have an Invite** box in the lower right hand corner of the page. Please confirm that these fields are correct, and click the orange **Proceed** button.

**DrFirst** **EPCSGold**

**EPCS Gold™**

EPCS Gold, provides a Simple, Secure, and Certified solution for sending Controlled Substance prescriptions electronically. EPCS Gold is a Certified solution, and has passed stringent auditing requirements set by the DEA. It is a Simple solution that fits with your current e-prescribing workflow, and a Secure solution which uses Two-Factor Authentication Protocol (TFAP) throughout the product to ensure a high level of trust and security for you as a provider.

If you are not yet enrolled for EPCS Gold, please make sure you have your Invitation ID and two factor authentication token in hand as you start the Identity Proofing process. Your invitation ID can be found in the email invitation that was sent to your email address. If you are already enrolled, please use your NPI number, the number that is currently showing on your One-time password token, and the password you setup during the identity-proofing process or enter the unique identifier for your biometric device to log-in to manage your tokens, and add a new token for prescribing.

For more information on EPCS Gold, the Identity-Proofing process, and how to manage your tokens, please click on the links below for short training videos. If you have any further questions, please contact us at <https://sdesk.drfirst.com/servicedesk> or at 1-866-263-6512.

[Training videos](#)

**Sign in**

NPI 2307957284

Passphrase

Next

[Forgot Passphrase](#) [Report Lost Token](#)

**I have an Invite**



NPI # 2307957284

Invite ID f04805e4c92e40608e10ec51747f19d4

Proceed

© 2013 - 2020 DrFirst.com. All rights reserved.

3. The next step will be to accept the **Terms of Use and Conditions** by selecting the individual gray checkboxes and clicking the **I Agree** button in the bottom right corner.



### Agreement for EPCS Gold Services

**TERMS OF USE AND CONDITIONS**

☒ I agree to retain sole possession of the OTP token, and will not share the login passphrase with any other person or allow any other person to use the OTP token or login passphrase in order to sign controlled substance prescriptions.

☒ I understand that any failure to secure the OTP token or login passphrase, or any sharing of the OTP token or login passphrase with any other person, may result in the revocation or suspension of my use and access of EPCS Gold.

☒ ☒ I agree that if using a hard token or software token application on a mobile device to generate a one-time password for the two-factor authentication process, the hard token or software token application on the mobile device must be separate from the device that I use to issue any electronic prescription for a controlled substance.

☒ I agree to notify the DEA, the persons in my organization designated to set logical access controls to the EPCS application, and my electronic prescription application or EHR/EMR vendor within one (1) business day upon discovery if one or more controlled substance prescriptions issued using my DEA number were not consistent with the prescriptions I signed, or were not signed at all.

☒ I agree to notify the persons in my organization designated to set logical access controls to the EPCS application and to notify my electronic prescribing or EHR/EMR vendor within one (1) business day of discovery if:

- I am contacted by a pharmacy because one or more of my controlled substance prescriptions are displaying the incorrect DEA number.
- It appears that any of the functions of the electronic prescription application are functioning improperly.
- My OTP token is lost, stolen, or the authentication protocol has been compromised in any way.
- I determine there is any other potential security problem not described above.

☒ I understand that in the event of misuse, I am responsible for any controlled substance prescriptions written using my two-factor authentication credential if I do not alert my electronic prescription application or EHR/EMR vendor as required in the provision above, and that I am responsible for any prescription information entered by an agent at my direction upon signing and authorizing the transmission of an electronic prescription for a controlled substance.

☒ I agree to promptly install all application updates of which I am made aware.

☒ I understand that the same responsibilities that apply to me when issuing paper or oral prescriptions also apply to me when issuing electronic prescriptions for controlled substances.

☒ I agree to prescribe controlled substances only for legitimate medical purposes.

☒ DrFirst may update these Terms of Use at any time upon providing notice to you.

☒ The following Terms apply regardless of how you access and your use of the prescription drug monitoring program (PDMP) data made available to you through your state, a third-party provider, or DrFirst:

- I agree that I am a licensed medical professional authorized to access PDMP data (all such data referred to as "PDMP Data") and shall only access or use PDMP Data in accordance with applicable state and federal laws and regulations, and that I am solely responsible for ensuring my access of the PDMP is authorized by the state in which I practice.
- I agree to provide proof of my state-issued authorization of accessing PDMP Data, if such authorization is required by applicable law.
- I have received all applicable consents or authorizations from current patients to access and/or use the PDMP Data.
- I agree to access and use PDMP Data solely for health care-related decision making related to a patient in accordance with applicable federal and state laws and regulations.
- I shall not engage in unlawful, objectionable, or malicious conduct or activities in accessing PDMP Data, including but not limited to, the transmission or distribution of viruses, computer worms, Trojan horses, malicious code, denial of service attacks, unsolicited commercial e-mail, the unauthorized entry to any other machine accessible via any platform, the unauthorized submission or transmission of data or material protected by a proprietary right of a third party, or the submission of otherwise objectionable information, material, or communications.
- I agree that I will not decompile, disassemble, deconstruct, or reverse-engineer any PDMP Data that is retrieved through PDMP Access.
- I agree not to sublicense, transfer, sell, disclose, export or otherwise permit access to or use of PDMP Data acquired through the software.
- To the extent that PDMP Data is access through APPRIS, I represent and warrant that I am not currently under formal investigation, indictment, or prosecution and have not been convicted, disciplined, or sanctioned within the preceding five (5) years by any governmental entity or self-regulation program for violation of any governmental laws or regulations under or related to health care, drugs, or criminal acts.
- I hereby agree to indemnify, hold harmless, and defend DrFirst, the National Association of Boards of Pharmacy, and Appriss, Inc. ("APPRIS"), and each of their respective officers, directors, employees, members, contractors, and affiliates from and against any losses, liabilities, costs (including reasonable attorneys fees), or damages resulting from any third party claim in which any above-named party is named as a result of my access or use of the PDMP Data.
- I acknowledge that to the extent that APPRIS is the source of the PDMP data, APPRIS and the National Association of Boards of Pharmacy shall be third-party beneficiaries to these terms.
- To the extent that the CURES network is the source of the PDMP Data, I agree that it shall be my responsibility to verify through the CURES portal that my CURES account profile is current, which shall include, at a minimum, completion of the annual update, and that I possess an active CURES account. I acknowledge that the failure to complete the annual update or maintain an active CURES account status will result in rejection of the query.
- For access to Washington State PDMP Data, I agree and acknowledge that I am required to have an account with OneHealthPort and retain full responsibility for maintaining an account with OneHealthPort and for any associated costs or fees.

☒ By clicking this box, you acknowledge and understand that you are subject to these terms of use and all applicable federal and state laws governing the electronic prescribing of controlled substances and applicable federal and state laws and regulations governing access and use of prescription drug monitoring program data.

PLEASE CHECK ALL CHECK BOXES AND CLICK THE AGREE BUTTON BELOW TO SIGNIFY THAT YOU HAVE READ AND AGREE TO THE ABOVE TERMS OF USE.

4. The next screen will present a temporary password. This allows you to resume the IDP session if you exit for any reason and should be recorded before proceeding.

**Please Note:** This temporary password can only be used if IDP has been passed and you have yet to bind a token. If the IDP session needs to be exited and completed later, this password can be used to access the session within 24 hours. To use this password, click on the original invite link and enter the password.

The screenshot shows the InfinID web interface. At the top right is the InfinID logo. Below the header, it says "Hi Wayne Best,". The main content area contains the following text:

DrFirst Inc has requested you to complete identity proofing (IDP).

InfinID, an identity and credential management service, leverages remote knowledge based authentication (KBA) technologies to provide a online method for providers to comply to NIST level of assurance (LOA) 3 requirements. This level of assurance requires a two-factor authentication token to be bound to your identity during this process. InfinID also enables you to verify your identity in the future without having to complete the KBA identity proofing steps again for other services that require identity proofing and/or multi-factor authentication such as electronic prescribing of controlled substances (EPCS).


If you are unable to complete binding your credentials to your identity during this session, you may resume your session with this temporary session password for up to 24 hours: **v7Y5d**. Please record this temporary password now to prevent the need to re-do identity proofing again in the event that you are unable to bind your credentials after completing identity proofing during this session.


Please click **Next** to proceed.

At the bottom right, there are two buttons: "Next" and "Cancel". At the bottom of the page, there is a copyright notice: "© 2013 - 2020 DrFirst.com. All rights reserved."




5. The next screen lists some pre-requisites of the IDP process:
- Token:** At least one hard or soft token is necessary to proceed.
  - Personal credit card:** This is NOT MANDATORY and can be omitted. If you are having a hard time passing IDP, entering this information may help you pass.






**BEFORE IDENTITY PROOFING, YOU WILL NEED THE FOLLOWING IN YOUR POSSESSION:**

### OneSpan and/or Symantec Token



- \* You must have at least one token
- \* It is highly recommended that you have 2 tokens for backup purposes
- \* OneSpan Digipass GO7 hard token can be supplied by your EHR/EMR vendor
- \* Symantec hard token can be supplied by your HER/EMR vendor and/or VIPACCESS app can be downloaded on your smart device

### Personal Credit Card




- \* You must be the primary account holder of the credit card.
- \* The credit card will not be charged.
- \* Must be a Visa or MasterCard registered under an address associated with your personal finances. (NOT debit card)
- \* Temporarily remove any credit freeze on your credit card or credit profile during this process.

\* Note: A credit card is strongly suggested to prevent identity proofing failures. If you do not use a credit card during the identity proofing process your identity may be able to be verified if there is sufficient financial account data associated with data entered on the next screen. (NIST Requirement)

[Continue](#) [Cancel](#)

6. Then, accept the **InfinID Application Terms of Use**.



**INFINID APPLICATION TERMS OF USE**

DrFirst.com, Inc. ("DrFirst," "we," or "us") provides online and mobile application services related to the practice of medicine, including secure information exchange, electronic prescribing, and other tools to assist physician practices, individual physicians, and other healthcare providers to perform a variety of healthcare activities. Many of these services require healthcare providers to undergo Identity Proofing during their initial registration process, in order to verify that the provider actually is the person that the provider claims to be in accordance with state and federal laws. InfinID ("the Application") is a web-based application which enables a Healthcare Administrator ("End User") to more efficiently manage and authorize those healthcare providers, identity, and credentials. The Application is provided to End User only under the applicable terms of use below (the "Terms").

PLEASE READ THE TERMS CAREFULLY. BY CLICKING ON THE "ACCEPT" BUTTON BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THESE TERMS, UNDERSTAND THEM, AND AGREE TO BE BOUND BY THEM.

IF YOU DO NOT AGREE TO ANY OF THE TERMS BELOW, YOUR SUBSCRIBER'S RIGHT TO ACCESS AND USE THE SERVICES WILL NOT COVER YOU AND YOU CANNOT BE GRANTED ACCESS TO THE SERVICES, THE SITE, OR ANY RELATED TOOLS OR SERVICES. IF YOU ARE IN THE PROCESS OF ELECTRONICALLY REGISTERING AND YOU DO NOT AGREE WITH THESE TERMS, YOU SHOULD CLICK ON THE "DO NOT ACCEPT" BUTTON TO DISCONTINUE THE REGISTRATION PROCESS OR EXIT THE APPLICATION REGISTRATION SCREEN.

**A. END USER REQUIREMENTS** By agreeing to these Terms as an End User, you represent that you are an End User at a healthcare entity, an authorized administrator appointed by a healthcare entity, or an authorized administrator appointed by an electronic medical record with the authority to access an entity's healthcare provider database in order to share provider identity verification information with DrFirst and authorized third parties. In the event that you cease to be an Authorized Credentialing Officer or an authorized administrator with the right to access and share healthcare provider information, these Terms will automatically terminate and you agree to discontinue your use of the Application immediately. You agree to use the Application to upload information for only those healthcare providers who have successfully completed your healthcare entity's identity proofing verification process in compliance with all applicable state and federal laws and regulations.

**B. ACCESS TO SERVICES** For so long as these Terms remain in effect and you remain a properly registered End User, the Application will remain available to you. You may access the Application only if the healthcare entity that you are affiliated with remains a DrFirst customer, subject to these Terms. During such time as you remain a properly registered End User, you are granted a limited, non-exclusive, nontransferable license to access and make use of the Application.

Version TOU 2.0, Last Modified 03/18/2016

☒ **I have read and understood this agreement, and I declare that I am authorized to sign this agreement.**

PLEASE SELECT THE ACCEPT BUTTON BELOW TO SIGNIFY THAT YOU HAVE READ AND AGREE TO BE BOUND BY THE PRECEEDING TERMS AND CONDITIONS OF USE.

7. Complete the **User Registration** form and verify that the pre-populated fields are correct. Here are some tips and notes on the fields within this forms:

### Required

- **NPI:** This will be pre-populated.
- **First / Last Name:** These fields will be pre-populated.
- **E-mail Address:** Must match the email where you received the EPCS invite.
- **DEA Number:** When entering your DEA number, please use all capital letters. For example, AA1234567 and not aa1234567. Please enter your primary DEA number, not a specialty DEA or DEA for prescribing addiction medications.
- **Date of Birth:** Please click on the calendar icon and select your birth year followed by the month and then day. This will make ensure formatting is correct.
- **Home Address** fields: Please enter the address related to your financial records. This is typically a home address. Please do not input any special characters within the address field.
- **Social Security Number:** Personal SSN number.
- **Mobile Phone Number:** While this is not required, if you enter a mobile phone number that Experian can validate, you will receive a text message with a confirmation code instead of a physical letter. This greatly speeds up the IDP process.

### Optional


- **Credit Card Number:** While this is not required, this can increase your chances of passing IDP if you fail the first time. Please enter a personal credit card that is either a VISA or MasterCard. You will NOT be charged; Experian requires only the first 8 digits.
- **Driver's License State, Driver's License #, and Residential Phone Number** are not required. If you enter your Driver's License #, please put the class of the license at the end of the number.

### Identity Proofing Process

Fields marked with \* are mandatory.

Fields marked with \*\* should be provided to prevent identity proofing failures or delays, see notes below form fields.

1
2
3
4
5
6


<p>➔ <b>NPI *</b> <input type="text" value="2307957284"/></p> <p>➔ <b>First Name*</b> <input type="text" value="Wayne"/></p> <p>➔ <b>Last Name*</b> <input type="text" value="Best"/></p> <p>➔ <b>Email Address *</b> <input type="text" value="waynebest@fakeemail.com"/></p> <p>➔ <b>DEA Number *</b> <input type="text" value="AP3306188"/></p> <p>➔ <b>Date of Birth (MMDDYYYY)*</b> <input type="text" value="01"/> <input type="text" value="01"/> <input type="text" value="1957"/></p> <p>➔ <b>Home Street Address*</b> <input type="text" value="1361 K ST SE APT 204"/></p> <p>➔ <b>Home City*</b> <input type="text" value="Washington"/></p> <p>➔ <b>Home State*</b> <input type="text" value="District of Columbia (DC)"/></p> <p>➔ <b>Home Zip*</b> <input type="text" value="20003"/></p> <p>➔ <b>Social Security Number*</b> <input type="text" value="890-62-9517"/></p> <p>➔ <b>Mobile Phone Number **</b> <input type="text" value="(202) 132-5831"/></p> <p><b>Credit Card Number **</b> <input type="text"/></p>	<p>The following fields are optional; however, if entered accurately will help confirm your identity.</p> <p><b>Driver's License State</b> <input type="text" value="Choose a Value"/></p> <p><b>Driver's License Number</b> <input type="text"/></p> <p><b>Residential Phone Number</b> <input type="text"/></p> <p>Powered by  </p>
---	---

\*\* A Experian Transaction Number will be sent to the mobile phone number provided. You will need to save and enter that code in later steps to complete the identity proofing process. If you do not provide a mobile number or if the mobile number can't be matched to your home address, the confirmation code will be mailed to your home address.

\*\* A credit card is strongly suggested to prevent identity proofing failures. If you do not use a credit card during the identity proofing process your identity may be able to be verified if there is sufficient financial account data associated with data entered on this screen. (NIST Requirement)  
 Your credit card will NOT be charged.  
 You must be the primary account holder of the credit card and it must be linked to your home address.

8. You will then be required to answer 3-4 security questions pertaining to your financial history

**Please Note:** If you are not presented with IDP questions, this could be due to a number of different factors. This includes but is not limited to a security freeze on your accounts. Instead of these questions, you will see a message that informs you of unsuccessful identity proofing.



### Identity Proofing Process

1

2

3

4

5

6

Please answer the following questions which are based on records from your credit profile:

1

According to your credit profile, you may have opened a mortgage loan in or around April 2019. Please select the lender to whom you currently make your mortgage payments. If you do not have a mortgage, select 'NONE OF THE ABOVE/DOES NOT APPLY'. \*

☐ FREDDIE MAC

☐ MID AMERICA MORTGAGE

☐ GMAC MORTGAGE

☐ BANK

☐ NONE OF THE ABOVE/DOES NOT APPLY

2

According to your credit profile, you may have opened an auto loan in or around October 2019. Please select the lender for this account. If you do not have such an auto loan, select 'NONE OF THE ABOVE/DOES NOT APPLY'. \*

☐ NISSAN MOTOR ACCEPTANCE

☐ CHRYSLER CREDIT

☐ ONYX ACCEPT

☐ GEC AUTO LEASE

☐ NONE OF THE ABOVE/DOES NOT APPLY

3


You may have opened an auto loan or auto lease in or around October 2019. Please select the dollar amount range in which your monthly auto loan or lease payment falls. If you have not had an auto loan or lease with any of these amount ranges now or in the past, please select 'NONE OF THE ABOVE/DOES NOT APPLY'. \*

☐ \$295 - \$394

9. Based on the answers to the questions presented, combined with the initial information entered by you on the **User Registration** screen, Experian will determine whether or not you have successfully passed IDP. If you fail IDP, you must start the IDP process over.

**Please Note:** If you fail three times, this will lock your account. You cannot attempt IDP again for a full 24 hours.

10. Once IDP has been completed successfully, you will receive a confirmation on the next screen that your identity has been successfully confirmed and will be prompted to add a token, click the orange **Add New** Token button. **It is HIGHLY RECOMMENDED that you add at least TWO tokens, in case one is lost or inaccessible.** If you cannot attach two tokens at this step, you can always add one token during the process and add another token at a later time from the EPCS Dashboard. You can have up to 5 tokens for your account.



Congratulations! Your identity has been confirmed but there are just a few more steps to complete the process of binding your identity to the credentials.

### Registering a Two Factor Authentication Token

This is required to complete identity proofing at NIST level of assurance 3 and will allow you to add additional services later which require multi-factor authentication without having to redo knowledge based authentication for identity proofing. You may download a free authentication token from one of the approved manufacturers listed in the drop down below or use an existing token from one of those manufacturers. Please see the tool tip for further instructions on each manufacturer.

#### Token Management

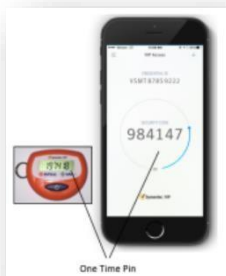
Fields marked with \* are mandatory

123456

Token Name	Credential ID	Manufacturer	Issuer	Type	Auth
<div>Add New TokenContinue</div>					

11. Select the manufacturer from the **Token Manufacturer** drop-down menu.

The screenshot shows the InfinID web interface. At the top, a blue header contains the InfinID logo. Below the header, a message states: "Congratulations! Your identity has been confirmed but there are just a few more steps to complete the process of binding your identity to the credentials." The main heading is "Registering a Two Factor Authentication Token". Below this, a paragraph explains that this step is required to complete identity proofing at NIST level of assurance 3 and allows adding additional services later. It mentions that users can download a free authentication token from one of the approved manufacturers listed in the drop-down below or use an existing token. A "Token Management" link is provided. Below the text is a progress bar with six steps, where step 4 is highlighted in orange. Below the progress bar is a table with columns: Token Name, Credential ID, Manufacturer, Issuer, Type, and Auth. To the right of the table are two buttons: "Add New Token" (orange) and "Continue" (grey). Below the table is a section titled "Add Two Factor Authentication Token". It contains a "Token Manufacturer" drop-down menu with a red asterisk indicating it is mandatory. The menu is open, showing options: "Select", "Symantec", "Symantec", and "OneSpan". At the bottom of the page, a copyright notice reads: "© 2013 - 2020 DrFirst.com. All rights reserved."



a. **Select SYMANTEC if:**

- i. You are using a soft token (VIP Access App on mobile phone/tablet/computer)
- ii. You are using a keychain hard token that has the Symantec name and logo on the face of the token.



b. **Select ONESPAN if:**

- i. You are using a keychain hard token that has the OneSpan name and logo on the face of the token.



12. Complete the rest of the fields with the following listed information to be entered per token:

- a. **Token Issuer:** DrFirst
- b. **Token Type:** OTP HARD TOKEN (key fob) or OTP SOFT TOKEN (VIP Access app)
- c. **Token Name:** Nickname for the token to help identify it (Ex. "iPhone token", "key fob", etc.).
- d. **Serial Number or Credential ID (include preceding letters):**
  - i. If using a **Symantec HARD token** (keyfob): enter the Serial Number (S/N) on the back of the token without any spaces.
  - ii. If using a **OneSpan HARD token**(keyfob): enter the Serial Number (S/N), which is the long string of numbers on the back of the token without any dashes.
  - iii. If using the **Symantec VIP Access app** SOFT token: enter the Credential ID that appears at the top of the screen without any spaces.
- e. **One Time Passcode (OTP):** The number generated on the hard token or the "Security Code" from the VIP Access app.

The image displays two side-by-side screenshots of the InfinID registration interface. Both screens show a progress bar at the top with steps 1 through 6, where step 4 is highlighted. Below the progress bar is a table with columns: Token Name, Credential ID, Manufacturer, Issuer, Type, and Auth. The left screenshot is for a OneSpan OTP HARD TOKEN, showing fields for Token Manufacturer (OneSpan), Token Issuer (DrFirst), Token Type (OTP HARD TOKEN), Token Name (White Tokens), and Serial Number or Credential ID (1518754364). The right screenshot is for a Symantec OTP SOFT TOKEN, showing fields for Token Manufacturer (Symantec), Token Issuer (DrFirst), Token Type (OTP SOFT TOKEN), Token Name (iPhone), and Serial Number or Credential ID (SYMCC2018052). Both screens include a 'Save New Token' button at the bottom.

**Please Note:** Your screen may look like either of these images depending on which token was selected.



13. Once all of the required fields have been entered, click the **Save New Token** button. Upon successfully registering a token, a green success message will appear on the screen. You may save additional tokens or click **Continue** to proceed.

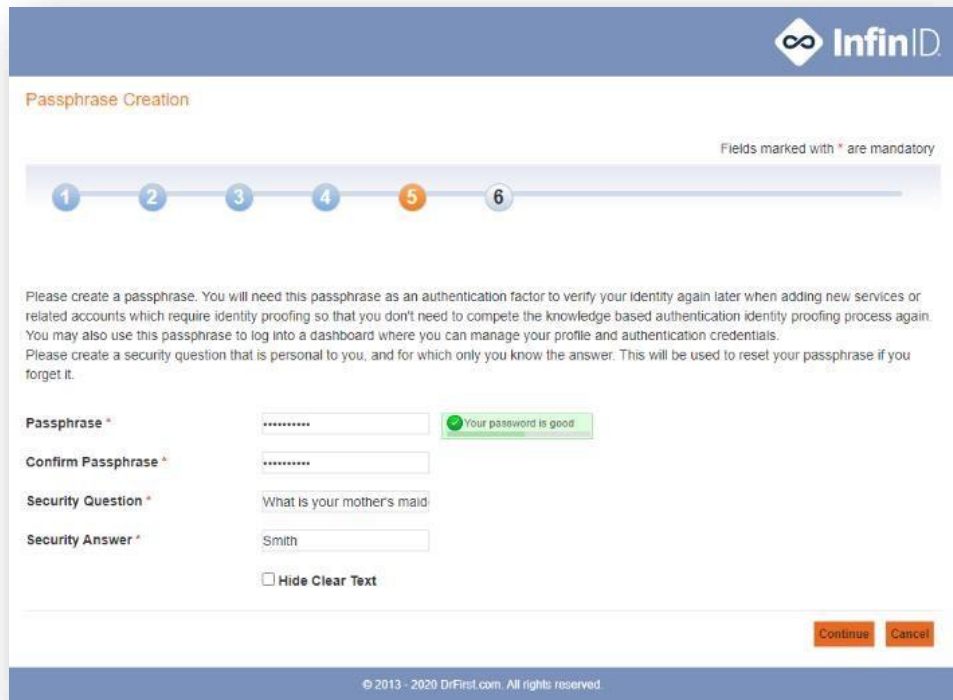
The screenshot shows the 'Token Management' section of the InfinID interface. At the top, a blue header contains the InfinID logo. Below it, a message states: 'Congratulations! Your identity has been confirmed but there are just a few more steps to complete the process of binding your identity to the credentials.' This is followed by the heading 'Registering a Two Factor Authentication Token' and a paragraph explaining the requirement for NIST level of assurance 3 and the option to download a free authentication token. A progress bar with six steps is shown, with step 4 highlighted in orange. Below the progress bar, a green success message reads: '✓ Successfully added token SYMC46242133'. A table lists the added tokens:

Token Name	Credential ID	Manufacturer	Issuer	Type	Auth
White Token	3510754364	ONESPAN	DRFIRST	OTP HARD TOKEN	ACTIVATED
iPhone	SYMC46242133	SYMANTEC	DRFIRST	OTP SOFT TOKEN	ACTIVATED

At the bottom right of the table area, there are two buttons: 'Add New Token' and 'Continue'. The footer of the page reads: '© 2013 - 2020 DrFirst.com. All rights reserved.'

14. Next, a passphrase, security question, and security answer must be created for the account. This passphrase is a password that will be used to prescribe controlled substances. The security question and answer will be necessary if you ever have to reset your passphrase.
  - a. The passphrase must be at least 8 characters long, be mixed case, and contain at least one number—avoid special characters.
  - b. A security question and security answer (**case sensitive**) will need to be entered as well. Since it is case sensitive, the security answer has to be remembered exactly as it was entered. This will be used in the event the passphrase is forgotten.

**Please Note:** We strongly recommend that the passphrase and security question/answer are written down to be stored in a secure location. DrFirst cannot reset a passphrase. The passphrase can only be reset by correctly answering your security question. In the event that the passphrase is forgotten and cannot be reset, your account will be **DISABLED**, and you will be required to complete IDP again from the beginning.



The image shows a web form titled "Passphrase Creation" for InfinID. At the top right is the InfinID logo. Below the title, a progress bar shows six steps, with step 5 highlighted in orange. A note states "Fields marked with \* are mandatory". The form contains the following fields: "Passphrase \*" with a green feedback message "Your password is good", "Confirm Passphrase \*", "Security Question \*" with the text "What is your mother's maid", and "Security Answer \*" with the text "Smith". There is a checkbox labeled "Hide Clear Text". At the bottom right are "Continue" and "Cancel" buttons. The footer contains the copyright notice "© 2013 - 2020 DrFirst.com. All rights reserved."

Passphrase Creation

Fields marked with \* are mandatory

1 2 3 4 5 6

Please create a passphrase. You will need this passphrase as an authentication factor to verify your identity again later when adding new services or related accounts which require identity proofing so that you don't need to complete the knowledge based authentication identity proofing process again. You may also use this passphrase to log into a dashboard where you can manage your profile and authentication credentials. Please create a security question that is personal to you, and for which only you know the answer. This will be used to reset your passphrase if you forget it.

Passphrase \*  ✔ Your password is good

Confirm Passphrase \*

Security Question \*

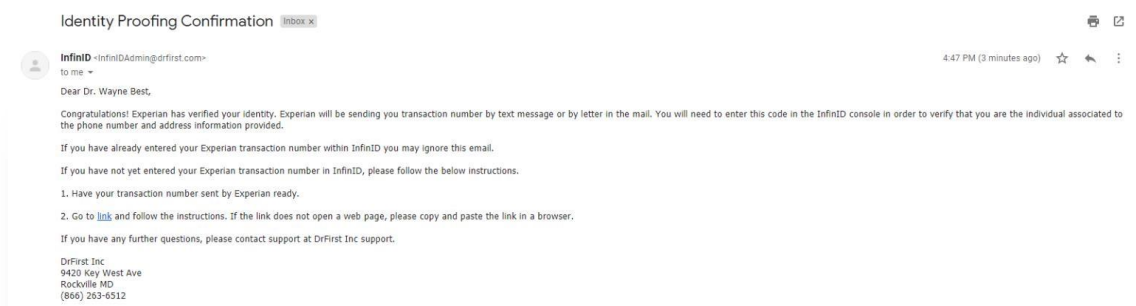
Security Answer \*

☐ Hide Clear Text

© 2013 - 2020 DrFirst.com. All rights reserved.

15. After entering the **Passphrase**, **Security Question**, and **Security Answer**, click Continue to move forward.

16. Once the Identity Proofing and registration steps have been completed, the next screen displays information in regards to the **Experian Transaction Number**. This step must be completed in order to finalize your EPCS credentialing. You will receive either a letter by USPS mail or an SMS text message with the Experian Transaction number. The workflow for each is as follows:



**Please Note:** If you must navigate away from this screen, it is safe to do so at this time. Experian sends an email congratulating you on completing identity proofing. Within this email is a link to enter the transaction number later. **PLEASE DO NOT DELETE THIS EMAIL.**

**Identity Proofing Process**

Thank you! Your credentials have successfully been bound to your identity. An Experian Transaction Number has been sent to you by one of the below methods. If you have received your code by text message, please enter it now. This is required to complete remote identity proofing at NIST standards to verify your identity using a second channel of verification.

**SMS Text/Voice**

**Mailed Letter**

If you entered a phone number but have not received your text message, please contact support to resend your Experian transaction number.

If your code cannot be sent by text message, within the next 5-6 business days, you should receive a mailed letter from our identity verification vendor, Experian. **PLEASE DO NOT THROW THIS LETTER AWAY.**

**Experian Transaction Number \***

**Verify Code**

**Cancel**

- a. **SMS Text Message:** If you entered a mobile phone that was successfully validated by Experian, the Experian Transaction Number will arrive immediately via SMS text message. Enter the **Experian Transaction Number** and click **Verify Code**.

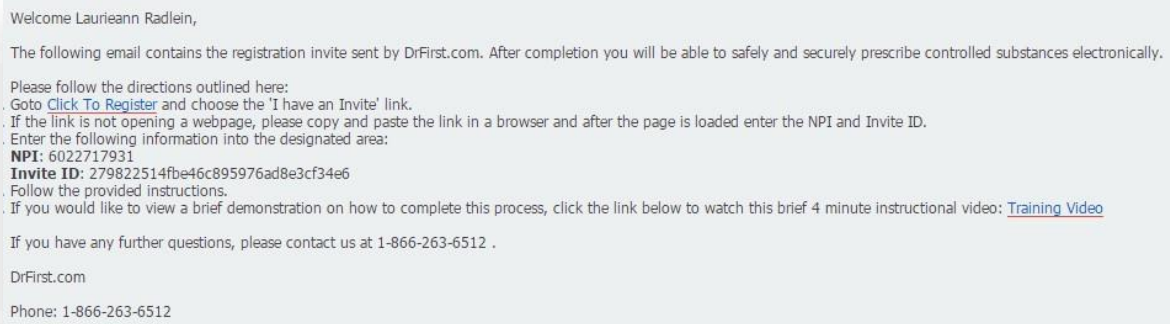
- b. **USPS Mail:** If a mobile phone number was not entered or if Experian is unable to validate the mobile number, Experian will send a letter via USPS mail containing the number that typically arrives in 5-6 business days.
- Once the letter arrives, you should access the IDP confirmation email and click the link in step 2 (see image above) to enter the **Experian Transaction Number**.
  - Enter the Experian Transaction Number, passphrase, and pin from your selected token. Then, click the **Submit** button to complete.

# Re-Authentication

If you are already an active EPCS prescriber and are on-boarding for EPCS at another organization, your account can be re-authenticated by leveraging your existing credentials. This prevents you from having to complete the IDP process for each organization you are in.

Once you have been invited for the new organization, please follow the steps below.

1. Once you receive the invite from DrFirst, click the **Click To Register** link within the email. If you are unable to find the email, please check your junk/spam folder.



2. Within the **I have an invite** section, click the orange **Proceed** button.

A screenshot of a web form titled 'I have an Invite'. The form has two input fields: 'NPI #' with the value '2911511675' and 'Invite ID' with the value '74a31c402a2a4a1d900702b1a0fb3'. An orange 'Proceed' button is located at the bottom right of the form.

3. Next, accept the **Terms of Use and Conditions**.

4. You will then be prompted to re-authenticate yourself by leveraging your existing credentials. Make sure to choose the **Use my existing authentication credentials** option to prevent having to complete identity proofing again from the beginning.

Hi LAURIEANN RADLEIN,

Rcopia has requested you to complete identity proofing. InfiniD brokers connections to Experian, credentialing offices and credential service providers to facilitate this process.

Our records indicate you have already completed the identity proofing process. You may verify your identity using the two-factor authentication credentials you previously bound to your identity as an alternate to completing the knowledge based authentication(KBA) identity proofing process again. Please select below if you would like to attempt to authenticate your identity using your existing credentials, or if you would like to start the identity proofing process again.

If you have forgotten your password and are unable to reset it you must start the KBA identity proofing process again.

[Use my existing authentication credentials](#) [Complete the identity proofing process again](#)

5. Finally, you will enter your existing passphrase, choose a token, enter the one-time pin (OTP), and click the **Submit** button.

Please authenticate with your password and one of your registered credentials to verify your identity

NPI: 6022717931

Password:  [Forgot Password?](#)

Select token: (iPhone) SYMC64666728 ▼

One time password:

☐ Show Clear Text

[Submit](#) [Cancel](#)

[Unable to verify your authentication credentials?](#)

At this point in time, enrollment at the new organization is complete. However, you will need to work with an administrator to have your EPCS account activated by completing Logical Access Control (LAC) before you can begin e-prescribing controlled substances for this additional organization.

# EPCS Logical Access Control (LAC)

Through the Rcopia application, the designated practice administrator must authorize a provider for EPCS and change the provider's grant status to active. In order to successfully complete this step, the designated administrator and the provider should be at the computer together because the provider will need to enter in their passphrase and token information.

**Please Note:** An administrator should have been designated during implementation, but if you are unsure of who the practice administrator is, would like to add a new individual as an administrator or if the administrator needs their username/password reset, please call the ICANotes Support Team at 443-569-8778 during business hours (Monday – Thursday, 8:30 EDT – 7:30 EDT & Friday 9 EDT – 6:30 EDT).

1. The designated practice administrator must log in to their ICANotes account and access DrFirst using either the Pending e-Rx or Pharmacy Msg buttons in the Chart Room.

Sign Out Edit View Format Reports Chat/Help ICANotes 1.04

Lock Screen Log Off

Chart Room for [ ] working at Hospital (Inpatient) Show Charts: All Sites Working At Site Only

No VO(s) Show Charts: 19 Pending e-Rxs No Pharmacy Msg

Enter Patient Name, ID, Maiden name, DOB (xx/xx/xx), Phone or SSN remove ""

Last Chart Enter Patient Name, ID

First Name Last Name DOB

Quarterly Report EOC

Match Test Results

Make a New Chart 2 Portal Updates Portal Reminder Service

Calendar Quick Calendar

MAR Schedule Rounds/VITALS Therapy Groups

Messaging Center 13 Unread Internal Msg No Unread Patient Msg

Patient Accounts EOC/UB04

Settings + Directories

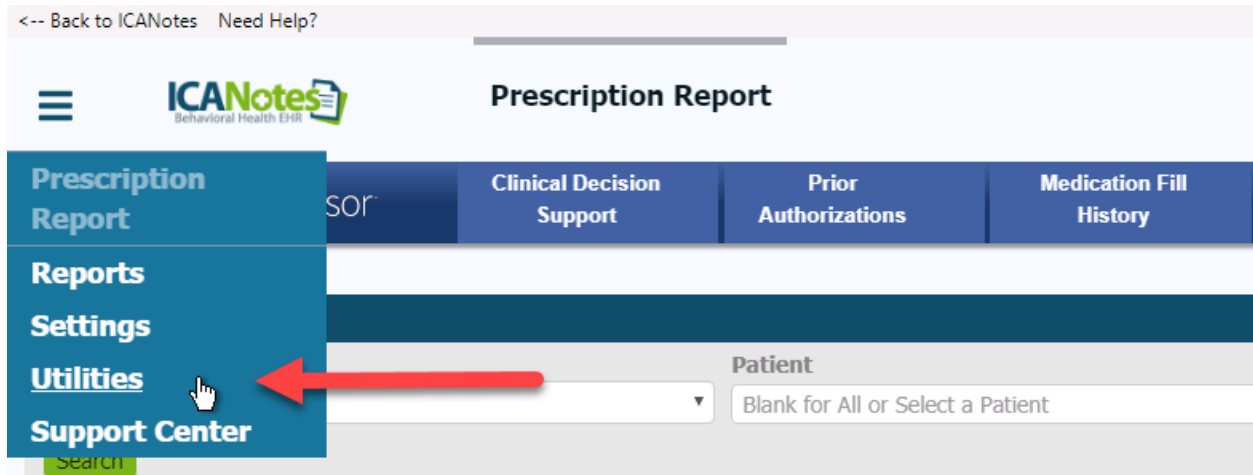
Inactive/Pending Charts

Click on the name to get the patient's chart. Hover cursor over name for more details.

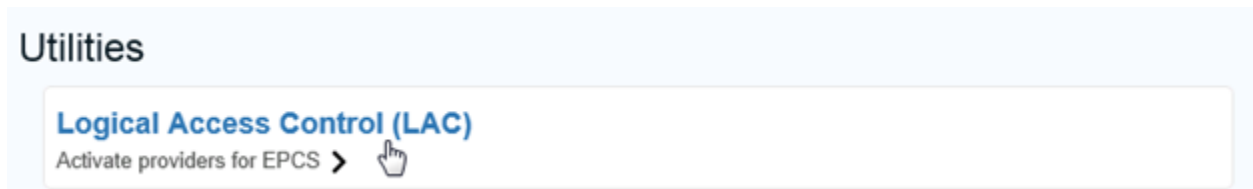
Daily Report Beta Testing

Start Telehealth Session Contact Us

2. Upon accessing DrFirst, navigate to the hover menu at the top left of the screen and select **Utilities**.



3. Click on **Logical Access Control (LAC)**.



4. This link will launch the administrator into the Logical Access Control (LAC) screen. This screen will list only providers who are enrolled, meaning that they have completed the IDP process with Experian, activated their token(s), and entered their Experian Transaction Number. Any providers with an **Inactive** grant will be listed first.

**Please Note:** This screen will display no more than 50 providers, so if the administrator cannot find the provider to activate, they will search for the provider at the top of the page.



5. Next, the administrator will need to change the EPCS grant to **Active** for any providers that need authorization to electronically prescribe controlled substances. The administrator will find the provider to activate and toggle **Active** under the **Grant** column.

**Logical Access Control** **EPCSGold™**

Logical Access Control Activity Report | Auditable Event Alert Report | Alert Email Configuration | Exit

Organization: DrFirst Inc Administrator: Ayesha Faisal (2632061631) Address: 16 One Half Mile Road Sterling Heights IL 48312

Two separate individuals are required to approve logical access control information in order to activate a prescriber's electronic prescribing of controlled substances privileges within each organization in accordance with DEA requirements. One individual must be an identity proofed registrant (Authorizing Prescriber) who will enter their two-factor authentication credentials to complete the authorization at the bottom of this screen. The other individual (Granting Administrator) must be someone who can verify that the prescriber(s) selected for activation are authorized to prescribe controlled substances for the organization with the DEA number selected and that the DEA license is active and in good standing.

**Search Prescribers**

First Name Last Name NPI

Prescriber	NPI	DEANumber	Last Change	Grant Status	Grant
BEST, WAYNE	7754352145	AB7246259	Mon Jul 20 12:53:50 EDT 2020	DEACTIVATED	<input checked="" type="radio"/> Active <input type="radio"/> Inactive

6. Once the administrator has changed the EPCS grant to **Active**, they will need to enter their (the designated practice administrator's) first and last name in proper case into the **Granting Administrator** section on the LAC screen. This acknowledges that the administrator confirms the provider has valid licenses. Not entering the first and last name in proper case will cause this process to fail.

**Search Prescribers**

First Name Last Name NPI

Prescriber	NPI	DEANumber	Last Change	Grant Status	Grant
BEST, WAYNE	7754352145	AB7246259	Mon Jul 20 12:53:50 EDT 2020	DEACTIVATED	<input checked="" type="radio"/> Active <input type="radio"/> Inactive

**Granting Administrator** [EPCS Logical Access Control Help](#)

I have verified that each prescriber selected for activation above is authorized to prescribe controlled substances for this organization using the DEA number listed and that the DEA license for that DEA number is active and in good standing.

Please confirm your first and last name: Admin Name

\* Subject to DEA regulations, this will be audited within DEA auditable event records for each digitally signed access change

7. Then, the provider will need to identify themselves on the LAC screen by entering in their NPI number. Normally, the practice administrator will be completing this step with the provider currently being activated. In the event that the provider is not available, the validating provider can be any provider that has an EPCS Status of **ENROLLED**. This could be the provider currently being activated, another provider within the practice, **or** a provider at any practice who is **ENROLLED** with EPCS Gold.
8. Finally, the provider will choose the OTP token they wish to use from the dropdown box, enter his/her passphrase, and enter the OTP from the token.

**Granting Administrator** EPCS Logical Access Control Help

*I have verified that each prescriber selected for activation above is authorized to prescribe controlled substances for this organization using the DEA number listed and that the DEA license for that DEA number is active and in good standing.*

Please confirm your first and last name:

\* Subject to DEA regulations, this will be audited within DEA auditable event records for each digitally signed access change

---

**Authorizing Prescriber**

Wayne Best      Enter NPI:

By entering your two-factor authentication details above, you are agreeing to change access for the prescribers and locations listed above.  
This transaction will be digitally signed.

Choose your Device from list      Enter your signing passphrase      Enter the pin from your OTP token

☐ Show Clear Text

9. Once the fields have been filled, the provider will click **Authorize**. This will activate their EPCS grant, and they can begin electronically prescribing controlled substances.
10. If necessary, it is possible for the administrator to see the history of providers that have gone through this process via the **Logical Access Control Activity Report**.

**Logical Access Control** EPCS Gold

EPCS Logical Access Control Help

**Logical Access Control Activity Report**    Auditable Event Alert Report    Alert Email Configuration    Exit

Organization: DrFirst, Inc.      Administrator: LAC Staff (222516832)

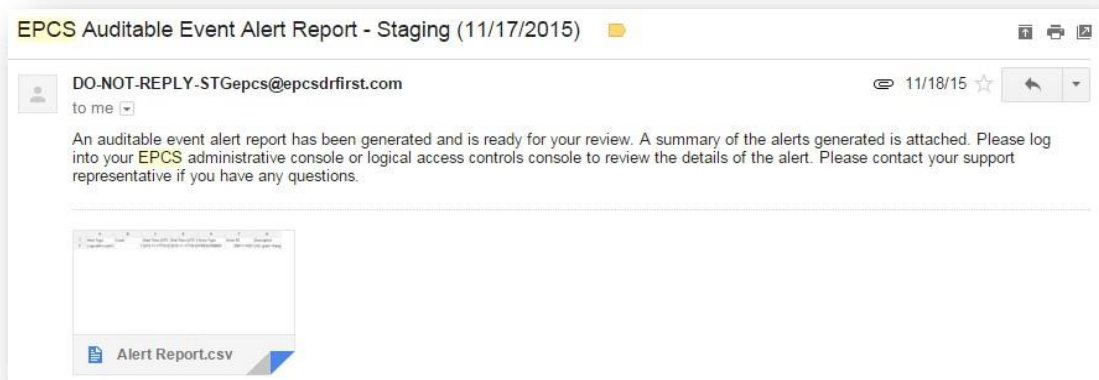
# Auditable Event Alerts

Any time there is a grant status change, meaning a provider's grant status has changed from **Inactive** to **Active** or vice versa, an automatic report is generated and sent to the provider's email. Per DEA requirements, this report is sent for a provider to have for auditing purposes.

Within the Logical Access Control (LAC) screen, an administrator can view the **Auditable Event Alert Report** from the top toolbar. Additionally, the **Logical Access Control Activity Report** shows LAC activity. An administrator is able to add other users to receive the **Auditable Event Alert Report** by clicking on **Alert Email Configuration** and adding emails.



Below is a screenshot of the email a provider will receive.



A sample of the CSV file attached to the above email is shown below.

Alert Report.csv						
Alert Type	Count	Start Time (UTC)	End Time (UTC)	Actor Type	Actor ID	Description
LogicalAccessC	1	2015-11-17T15:5	2015-11-17T16:0	PRESCRIBER	2981111091	LAC grant change

# Frequently Asked Questions (FAQs)

## Where can I check what information Experian has on file for me?

In order to check the information that Experian has on record, you can obtain a Free Experian credit report from [www.annualcreditreport.com](http://www.annualcreditreport.com). Identity proofing questions are formulated based upon credit history. This includes but is not limited to questions about home/auto loans, bank accounts, places of residency, etc. Having a credit report available can assist in answering these questions.

## What can I do if I am locked out of my account after three failed identity verification attempts within a 24 hour period?

You will have to wait 24 hours from the last time identity verification was attempted and failed. Any attempts made during the lockout period (whether it be an hour or 23 hours) will extend the time that you will have to wait. DrFirst DOES NOT have the ability to unlock your account.

## What is Serial Number (S/N) and Credential ID?

- Serial Number or (S/N): the series of numbers and/or letters on the back of the hard token that is the unique identifier for that token. S/N refers to Serial Number—not to be confused with SSN which refers to your Social Security Number and will only have to be entered in the User Information page.
- Credential ID: is the series of letters and numbers (might start with “SYMC”) that appears at the top of screen when you open the soft token VIP Access app. It is a unique identifier for your soft token every time it is downloaded. So, if you delete the app and redownload it, you will have to attach another token.

## What happens if I forget my passphrase and cannot answer my security question?

In the event that the passphrase is forgotten and cannot be reset, your account will be DISABLED, and you will be required to complete EPCS onboarding again. We strongly recommend that the passphrase and security question / answer are written down to be stored in a secure location. DrFirst cannot reset a passphrase. The passphrase can only be reset by correctly answering your security question.

## Can I complete Identity Proofing if I have a Security Freeze on my account?

If you have a security freeze in place for your credit accounts, you MUST remove them before starting enrollment by contacting Experian. Instructions on how to remove freezes/alerts can be found at [www.experian.com](http://www.experian.com) under “Credit Support”.

## What are some factors that result in failed Identity Proofing?

There are several factors that can hinder your ability to successfully complete Identity Proofing, these include but is not limited to the following:

- Security Freeze
- Fraud Alert
- Inability to answer security questions accurately
- Personal information entered does not match what Experian has on file

# Resources

Support is available for DrFirst On-Boarding from Monday through Thursday, 8:30am – 7:30pm EDT and Friday 9:00am – 6:30pm EDT. If you are failing the identity proofing process or need further assistance, please call the ICANotes Support Team at 443-569-8778.

- [ePrescribing with DrFirst Video Tutorial](#)
- [ePrescribing in ICANotes Guide](#)
- [Schedule a Training](#)