CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Healthcare Quality Information System (HCQIS) Access Roles and Profile (HARP) Training

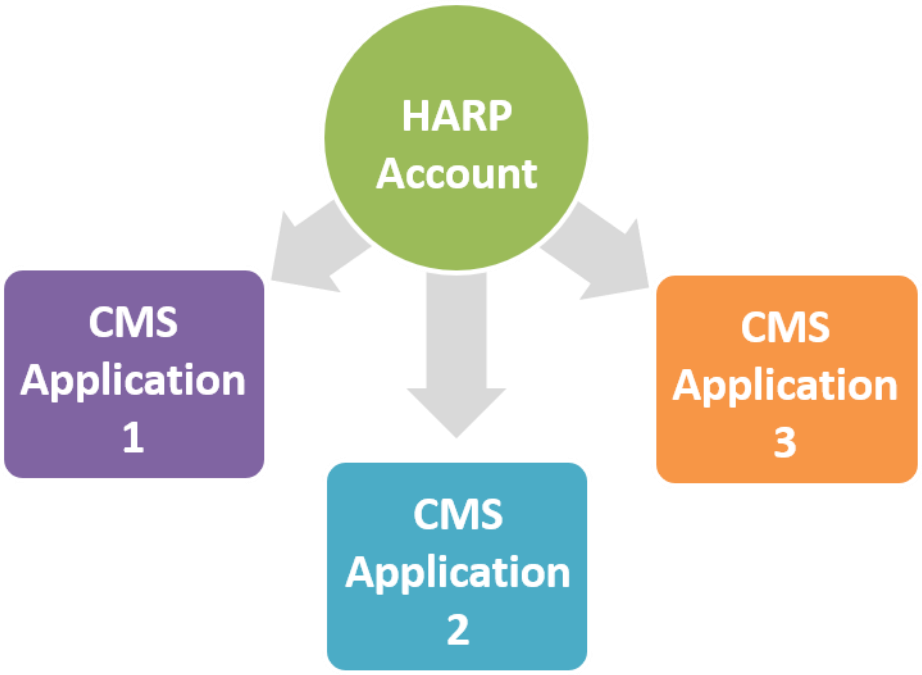
With End-Stage Renal Disease (ESRD) Outreach, Communication, and Training (EOCT) Team

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

HARP Overview

What is HARP?

HARP is a secure identity management portal provided by the Centers for Medicare and Medicaid Services (CMS). Creating an account via HARP provides users with a user ID and password that can be used to access many CMS applications.



HARP Overview and Benefits

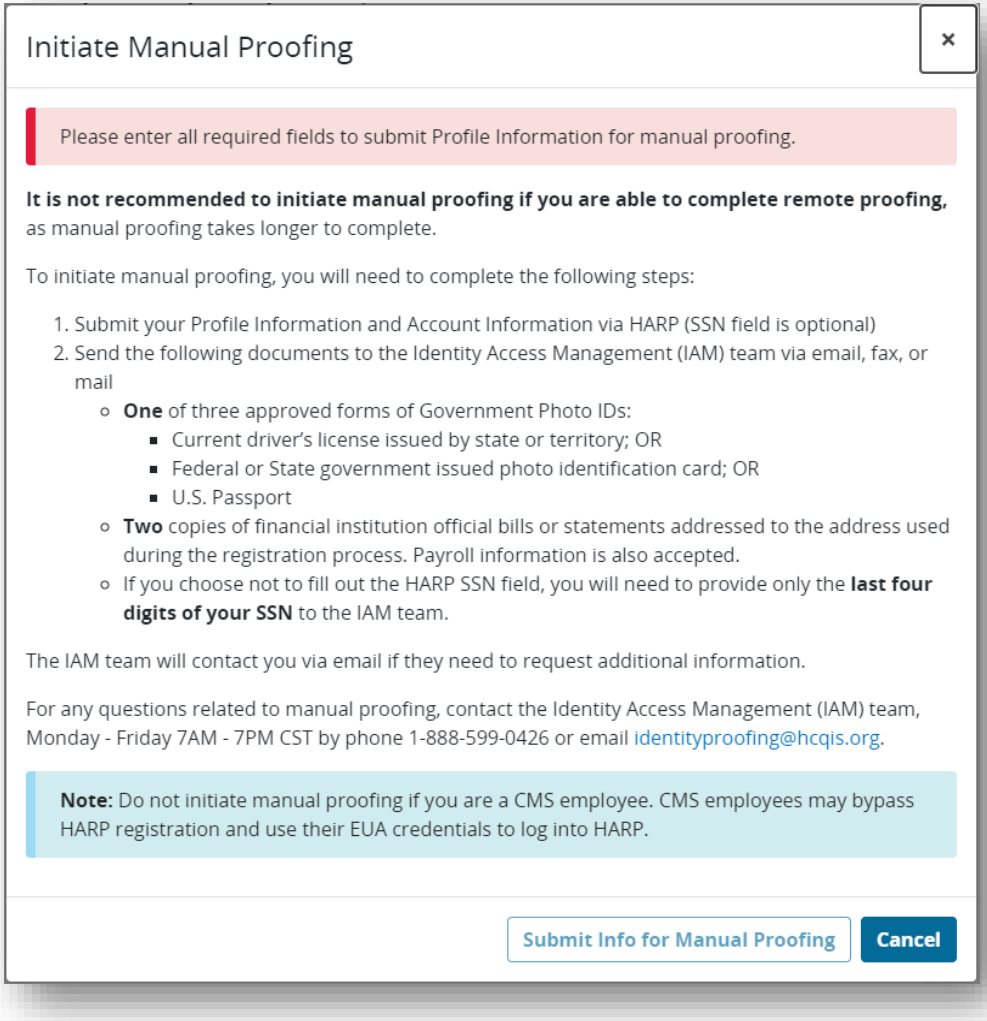
- HARP provides a single location for users to:
  - Modify their user profile.
  - Change their password.
  - Update their Challenge Question.
  - Add or remove two-factor authentication devices.
- All ESRD Quality Reporting System (EQRS) users must complete a HARP account setup.
- Users can manage their profile information via HARP and manage roles via EQRS.
- When registering for a HARP account, users complete identify proofing via Remote Identity Proofing (RIDP) or manual proofing.

What is RIDP?

- Anyone requesting electronic access to protected CMS information or systems must be identity proofed to gain access.
- RIDP is the process of validating sufficient information that uniquely identifies you (e.g., credit history, personal demographic information, and other indicators).
- This method is used for verifying the identity of a user as opposed to manual or in-person proofing.
- CMS uses the Experian identity verification system to identity proof remotely.
- **HARP does NOT store your personal information.**
- **RIDP does NOT affect your credit.**

What is Manual Proofing?

Users who are unable to be proofed remotely, or do not wish to enter their social security number, may initiate manual proofing.



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

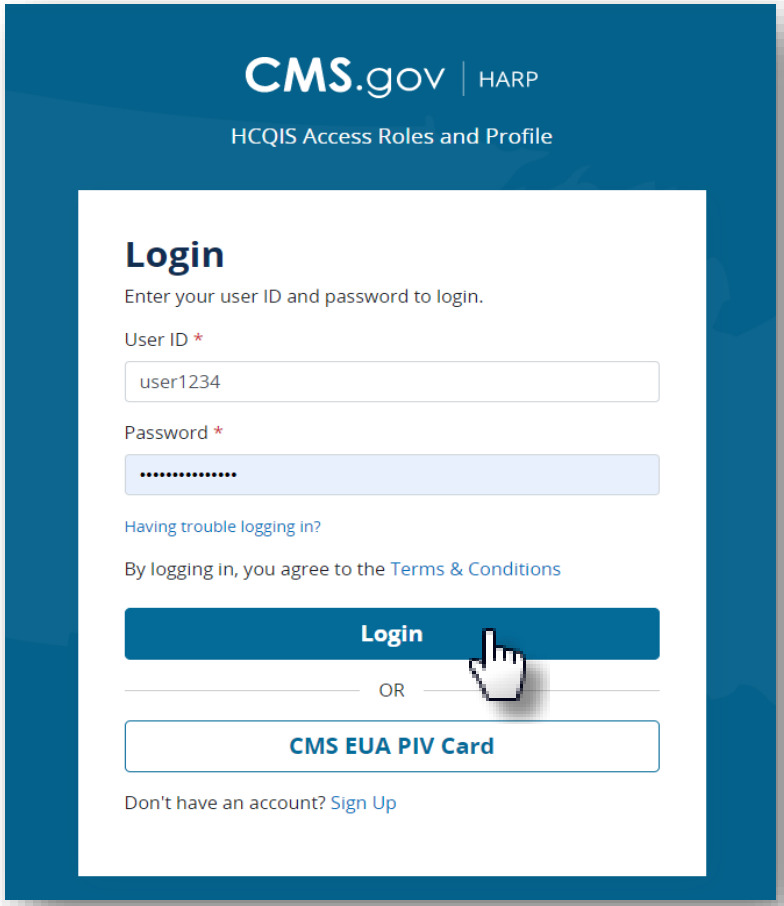
HARP Roles

HARP Roles

User Role	Description
Security Official (SO)	• Can serve as the SO over multiple organizations. • Approves or denies additional SO and End User role requests for a specific organization. • Must have an End User role to perform tasks in the EQRS application. • Cannot approve their own End User role request.
End User	• Performs tasks within CMS applications, such as EQRS. • May have a user role and scope over multiple organizations.

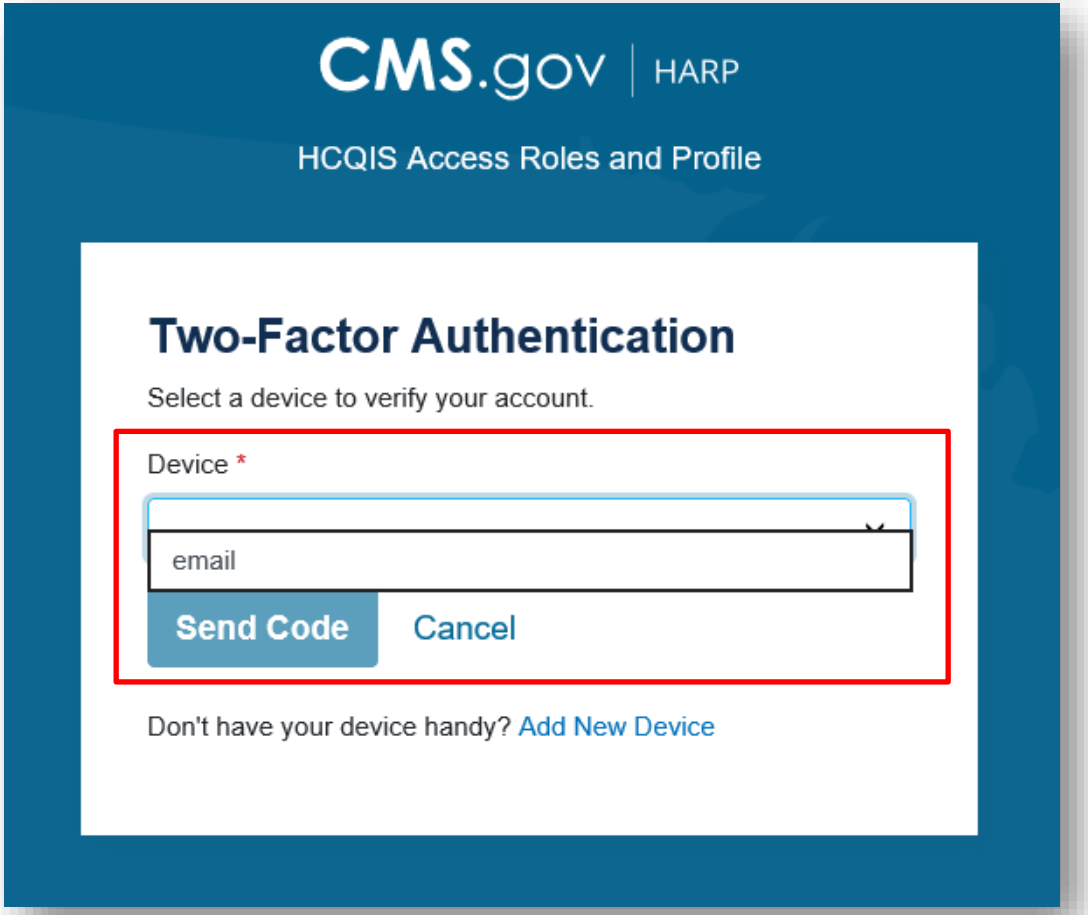
Log in to HARP

1. Go to https://harp.cms.gov/login/login.
2. Enter your HARP Username and Password.
3. By logging in, you agree to the Terms & Conditions.



Two-Factor Authentication Drop-Down

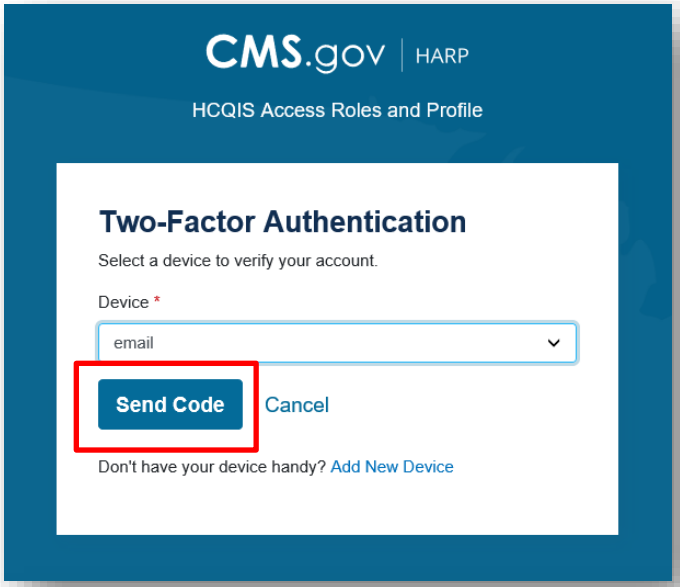
4. A Two-Factor Authentication screen displays. Click the Device drop-down.
5. "Email" displays as the only two-factor authentication device option. Select "email."



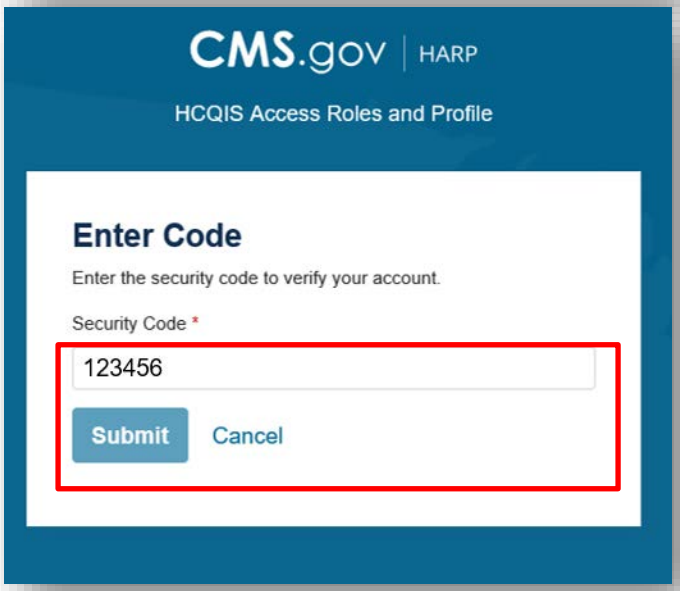
NOTE: HARP automatically sets the email address used to establish the account as the initial two-factor authentication device. Users must select email during the initial HARP login attempt. The email address may be changed after the initial log in.

Enter Security Code

6. Click “Send Code.” A one-time verification code is sent to the email address associated with the account. The Enter Code screen displays.

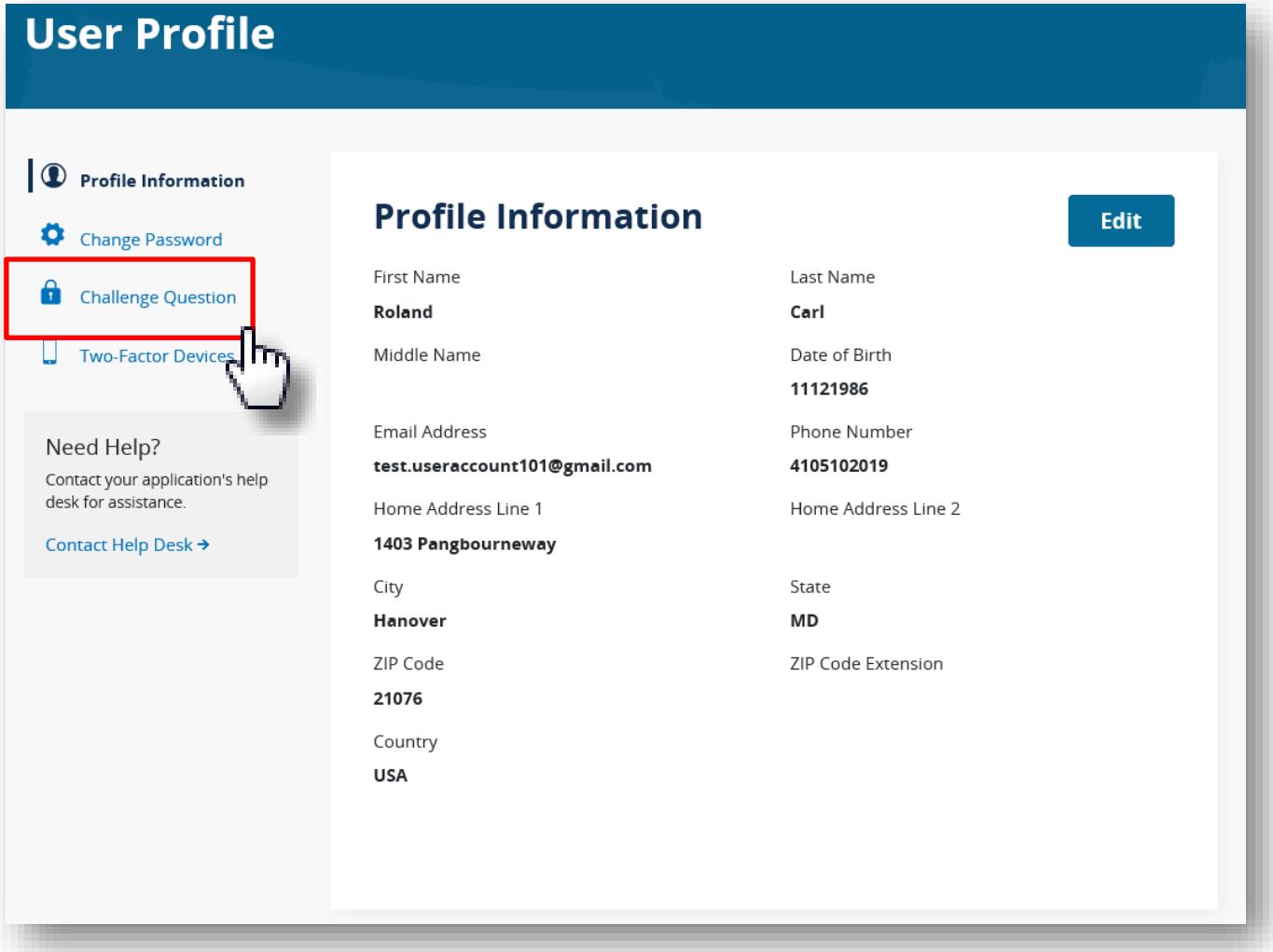


7. Enter the one-time verification code. Click “Submit.” The User Profile screen displays.



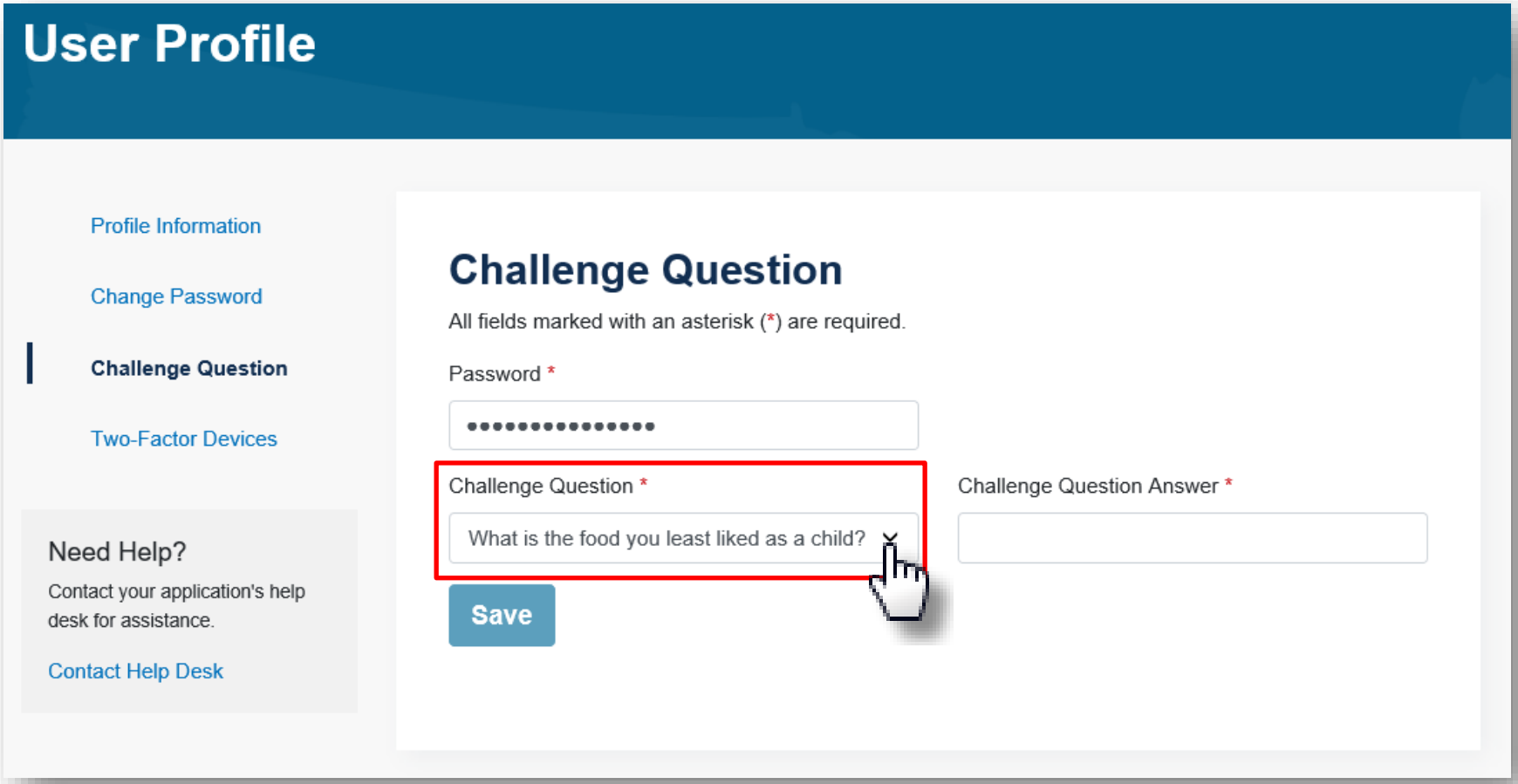
Review User Profile

8. Review the profile information for accuracy. Click “Challenge Question.”



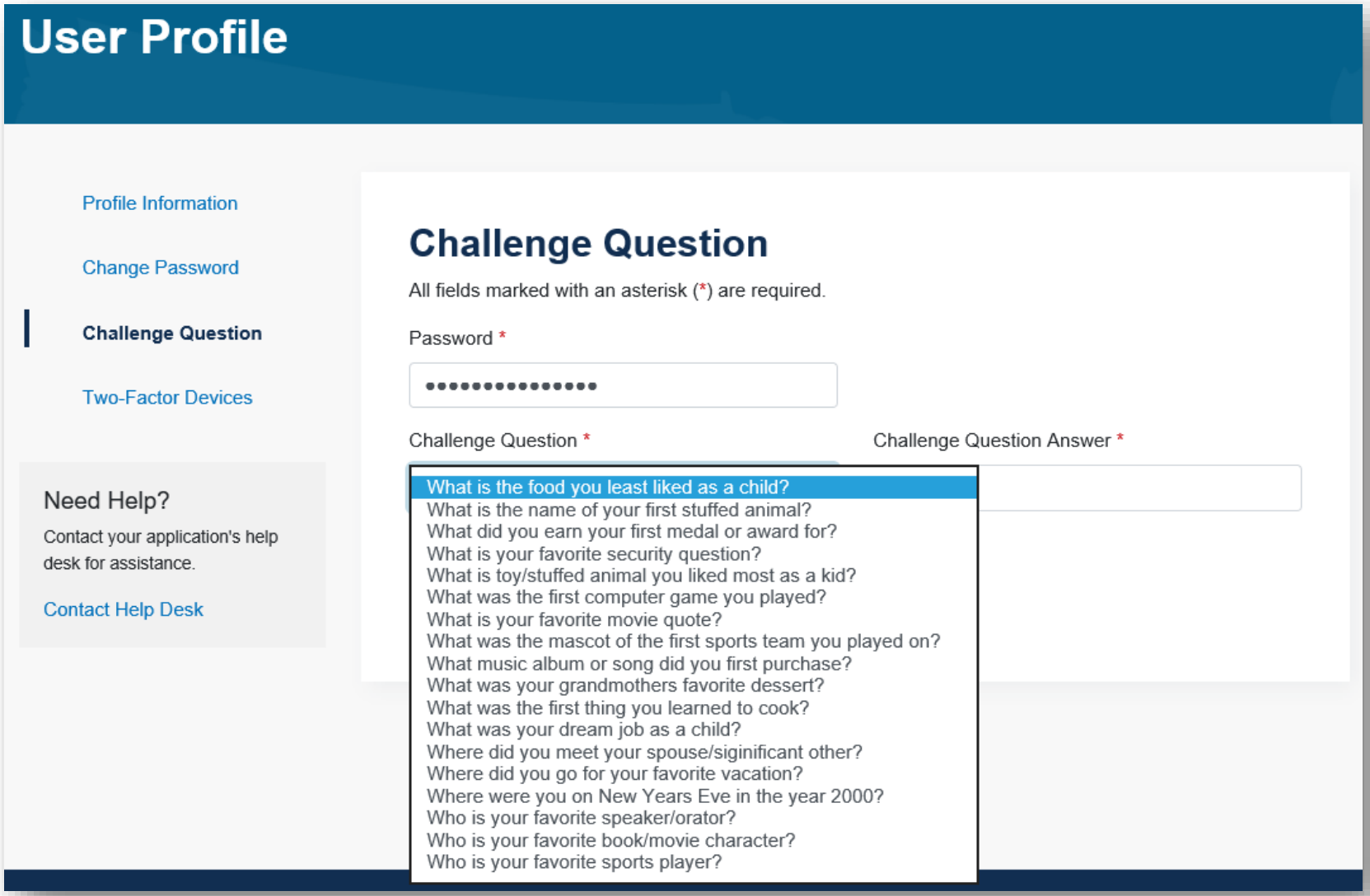
Enter Password

9. Enter Password.
10. Click the Challenge Question drop-down arrow.



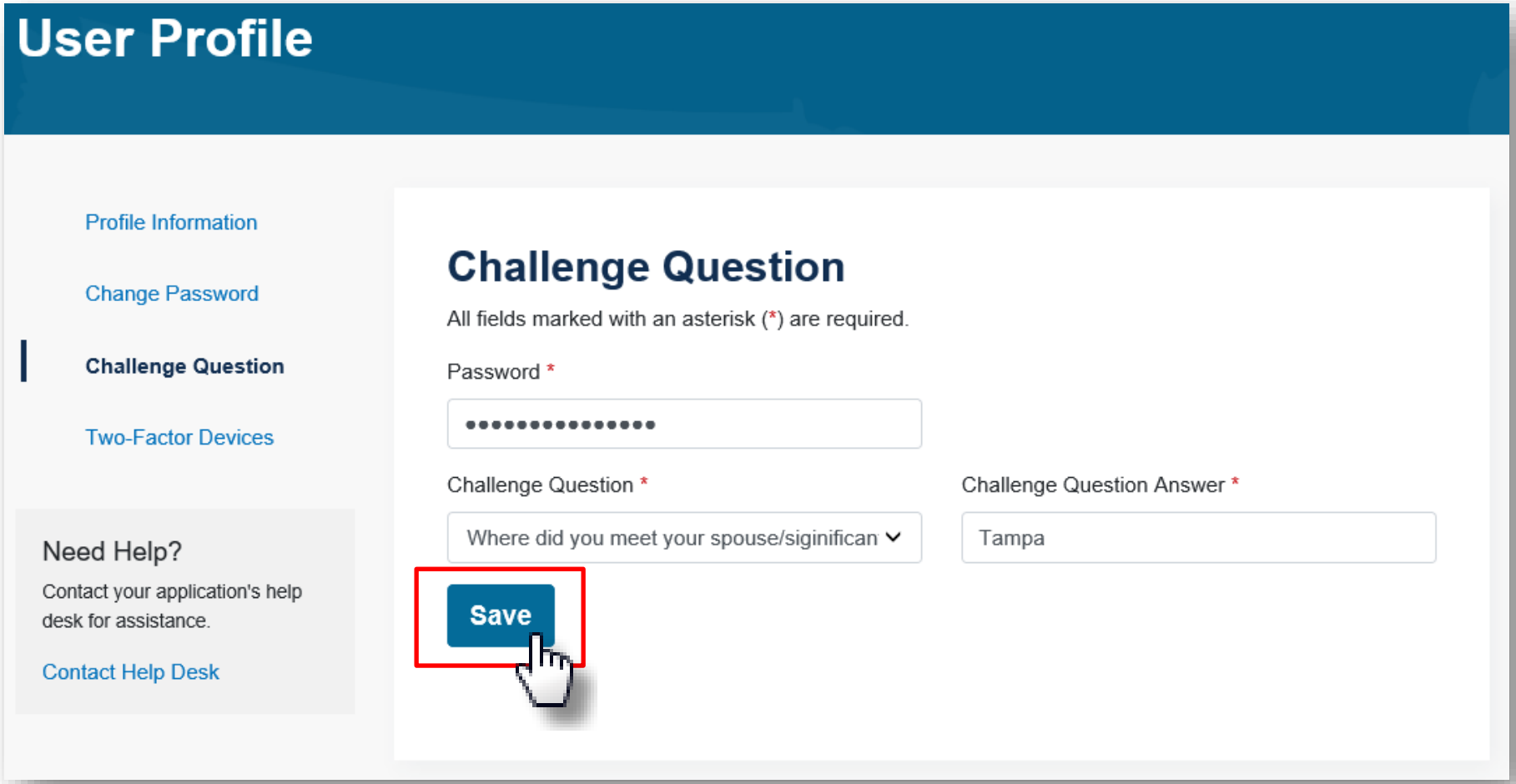
Select Desired Challenge Question

11. Select the desired Challenge Question.



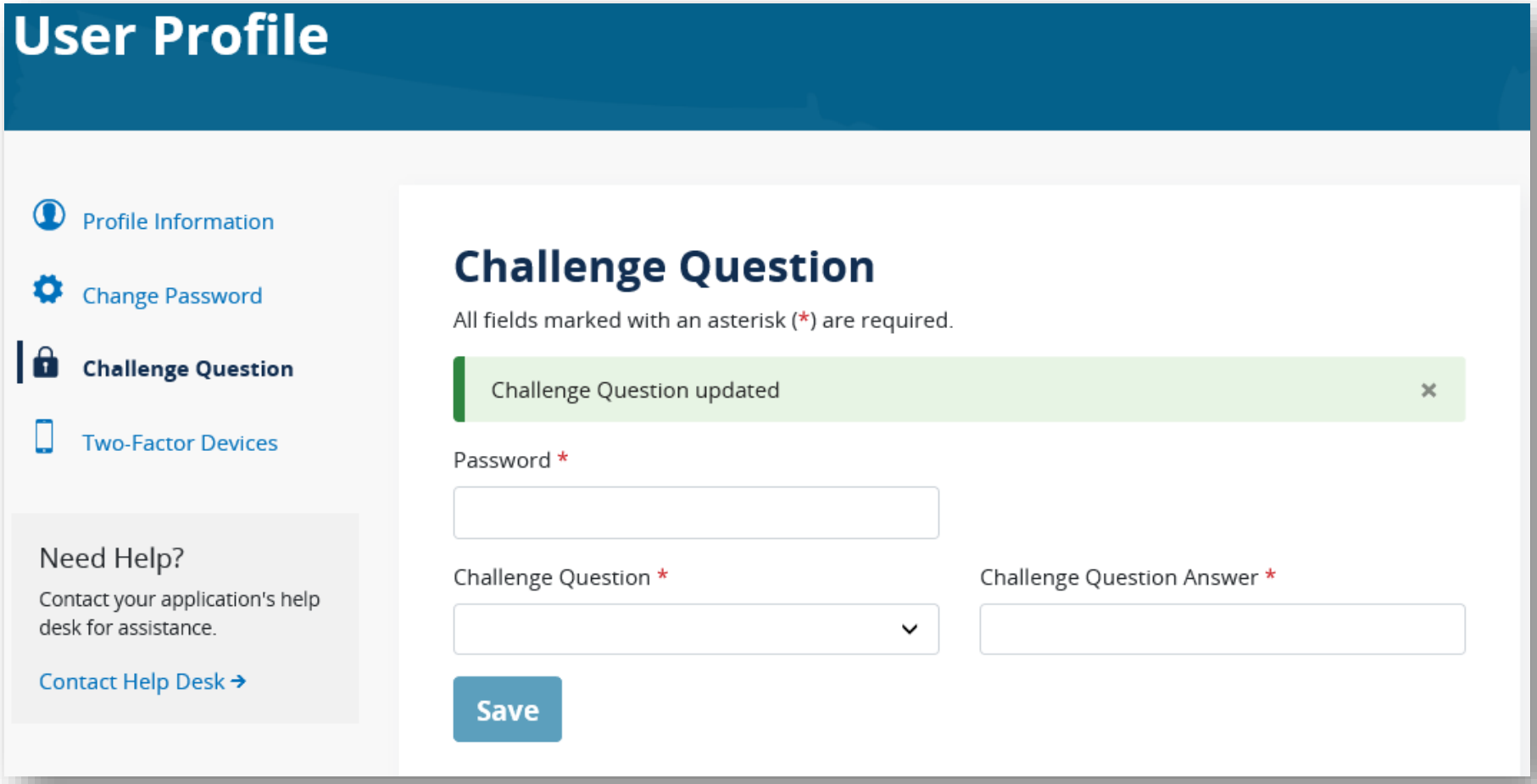
Enter Challenge Question Answer

12. Enter the Challenge Question Answer.
13. Click “Save.”



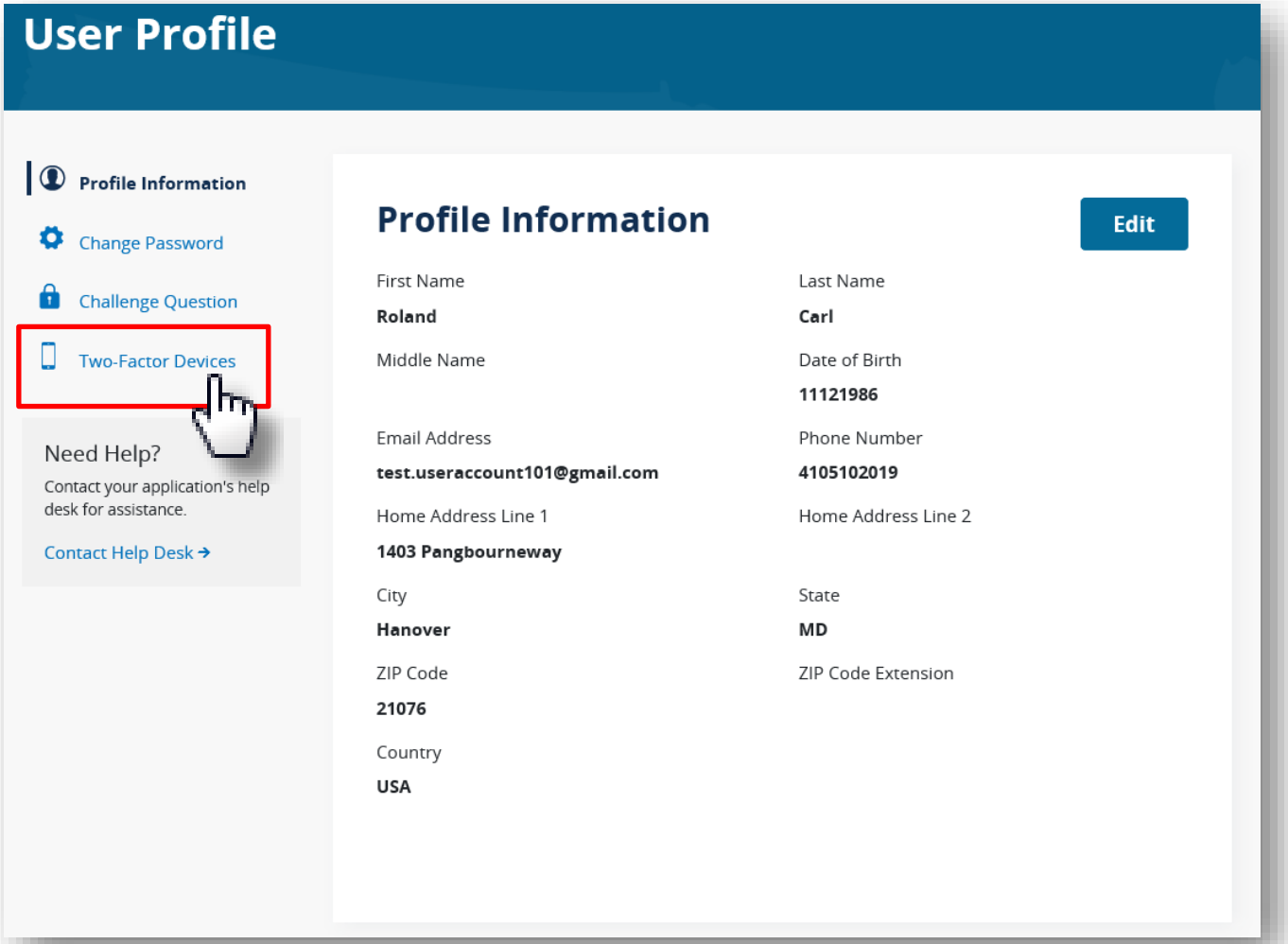
Successfully Saved Challenge Question

14. HARP refreshes with “Challenge Question updated” message.



Setting Additional Two-Factor Device

1. Click “Two-Factor Device.” A list of current two-factor authentication devices displays.



Selecting Additional Device

2. Click the Device Type drop-down arrow.

Select Two-Factor Authentication Device

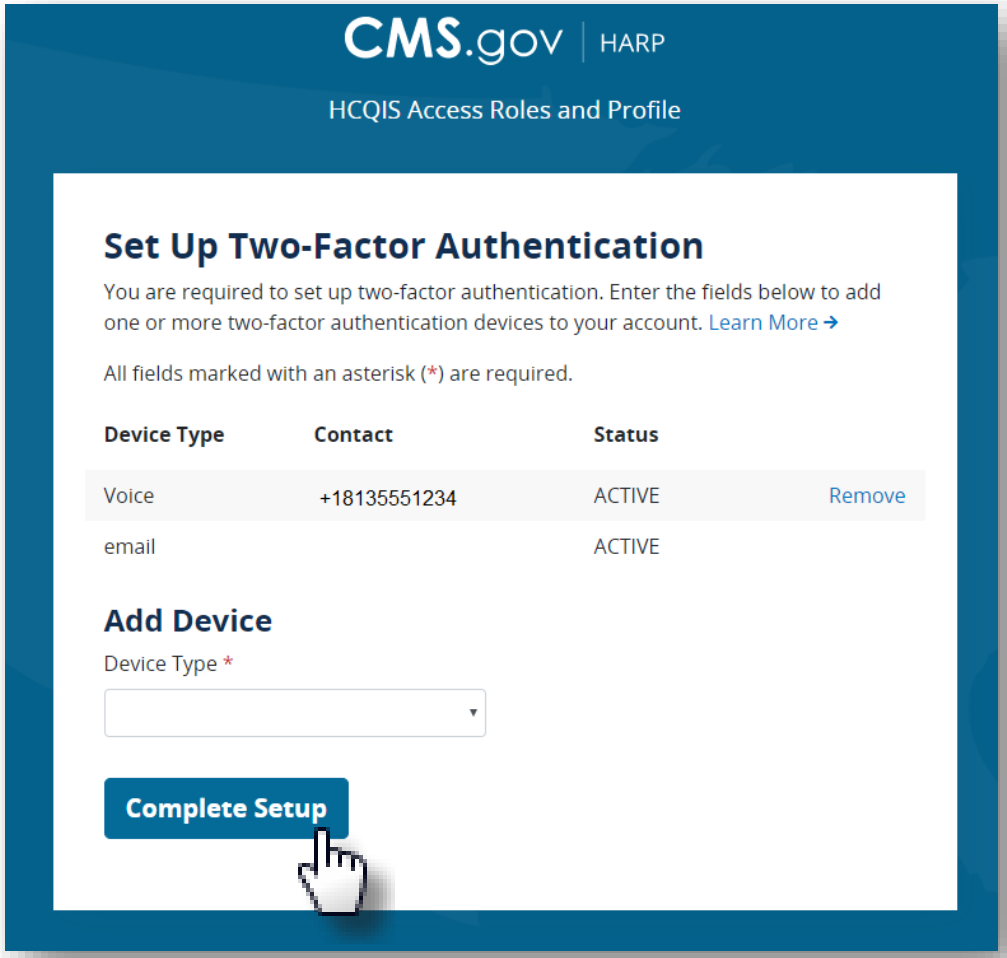
3. Select the desired additional two-factor authentication device.

Two-Factor Authentication Device Type

Device Type	Description
Email	Default two-factor authentication device. Cannot be removed. You can edit this to another email address.
SMS	Enter your mobile phone number to receive a text with a security code.
Voice	Enter your phone number to receive a call with a security code.
Google Authenticator	The Google Authenticator application generates two-factor authentication codes on your mobile device.
Okta Verify	The Okta Verify application generates two-factor authentication codes on your mobile device.
Okta Verify Push	The Okta Verify Push application generates two-factor authentication codes on your mobile device.

Click Complete Setup

4. Follow the configuration requirements for the selected two-factor authentication device. The Status indicates "ACTIVE" once successfully configured.
5. Click "Complete Setup."

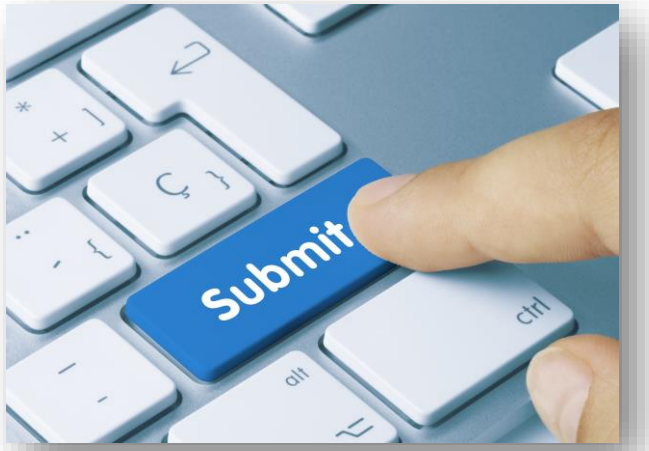


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Registering for a New HARP Account

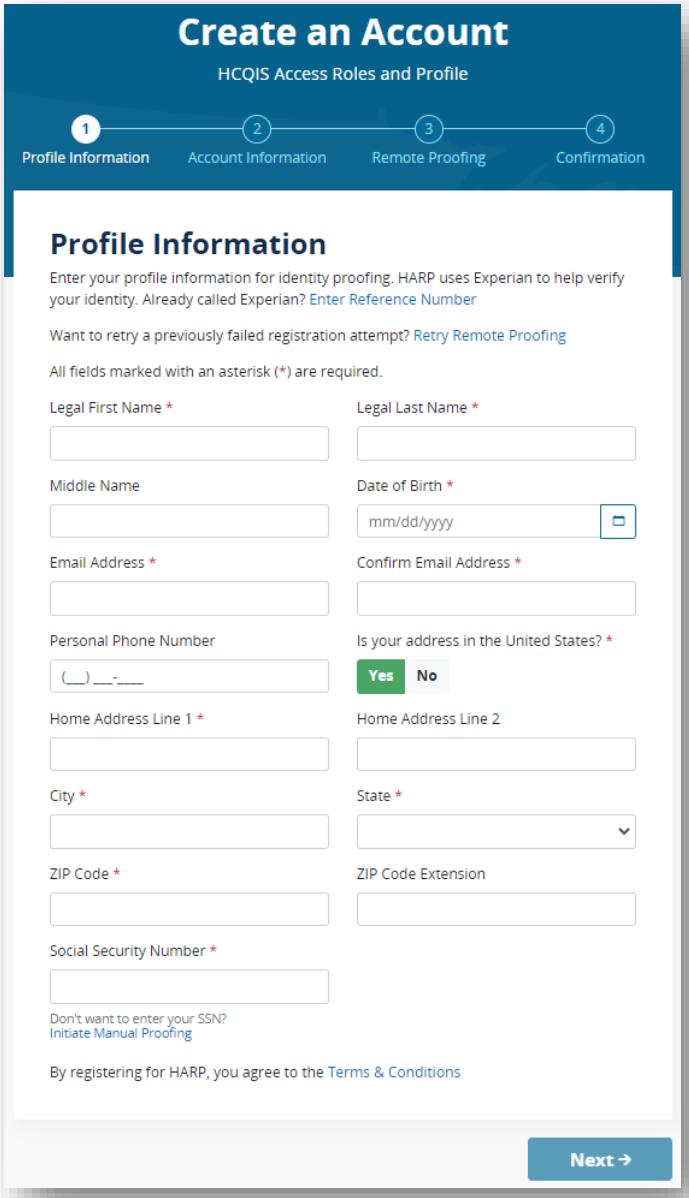
New HARP Account Registration

- New users can create a HARP account by going to https://harp.cms.gov/register/profile-info.
- When creating a HARP account, users must:
  - Enter profile information, which includes: name, date of birth, social security number, and home address.
  - Create a user ID, password, and Challenge Question.
  - Complete RIDP or manual proofing.
  - Register additional two-factor authentication devices, if desired.



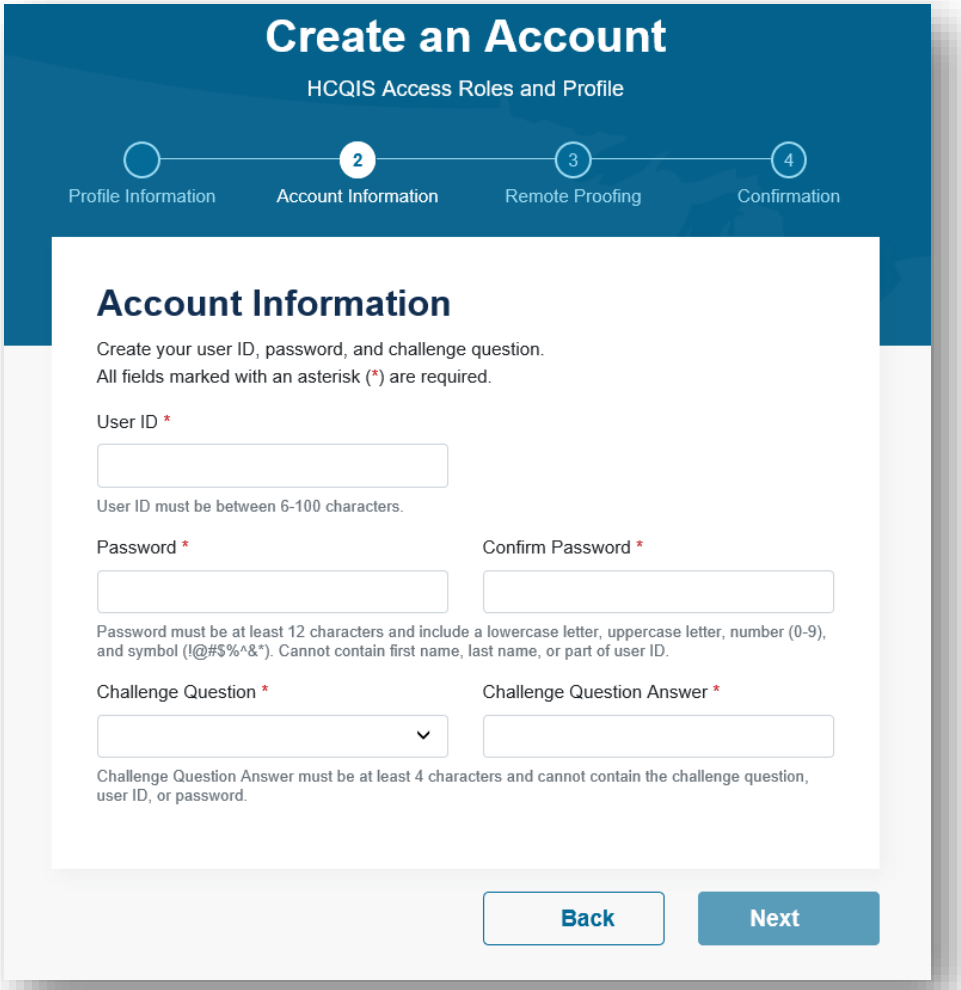
Enter Profile Information

1. Go to: https://harp.cms.gov/register/profile-info.
2. Enter your Profile Information to begin the account creation process. The following fields are required:
   a. First Name
   b. Last Name
   c. Date of Birth
   d. Email Address
   e. Home Address
   f. City
   g. State
   h. ZIP Code
   i. Social Security Number (SSN)
3. By registering for HARP, you agree to the Terms & Conditions



Enter Account Information

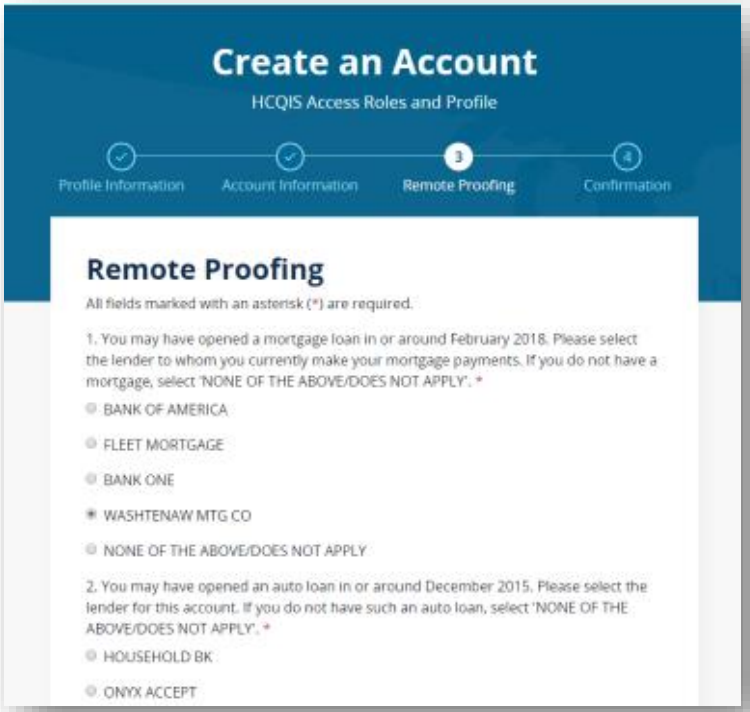
4. Enter a valid User ID, Password, and complete the Challenge Question fields.
5. Click “Next.”

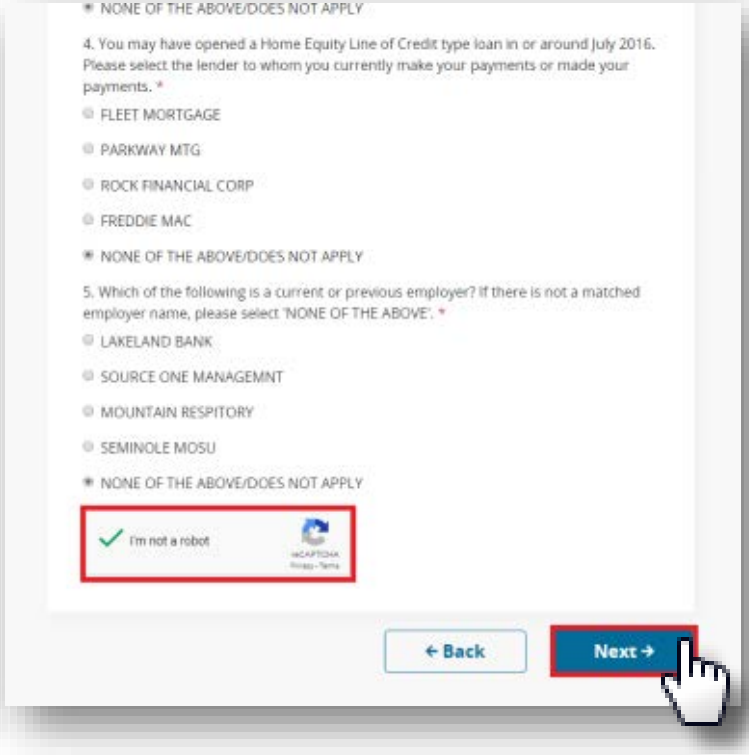


Complete Remote Proofing

6. Answer the Remote Proofing questions.
7. Click “I’m not a robot,” and click “Next.”

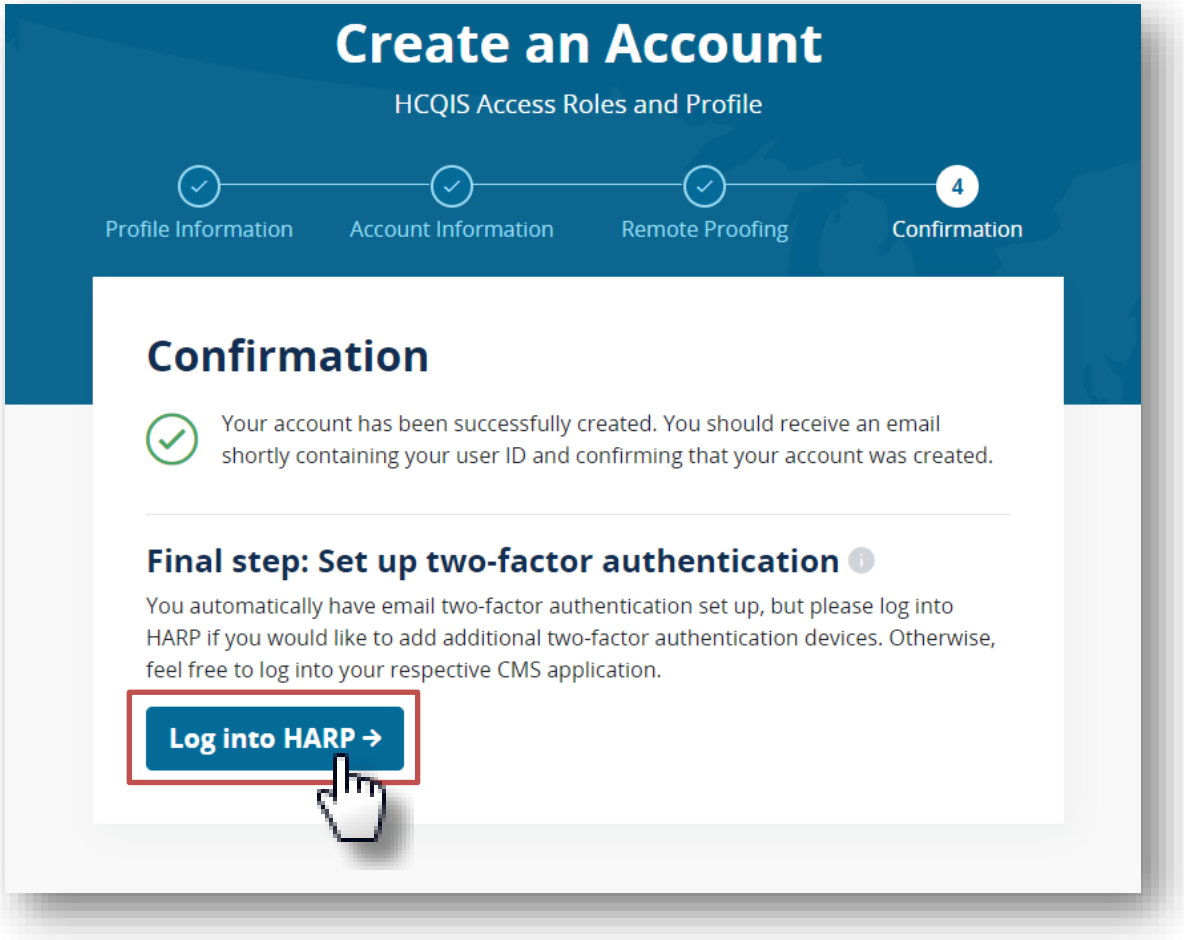
Note: Users who receive an error message while remote proofing are directed to contact Experian to verify their information. If, after contacting Experian and verifying their information, users continue to experience issues with HARP registration, they should contact the QualityNet Service Center via email at qnetsupport-esrd@hcqis.org or via phone at (866) 288-8912.





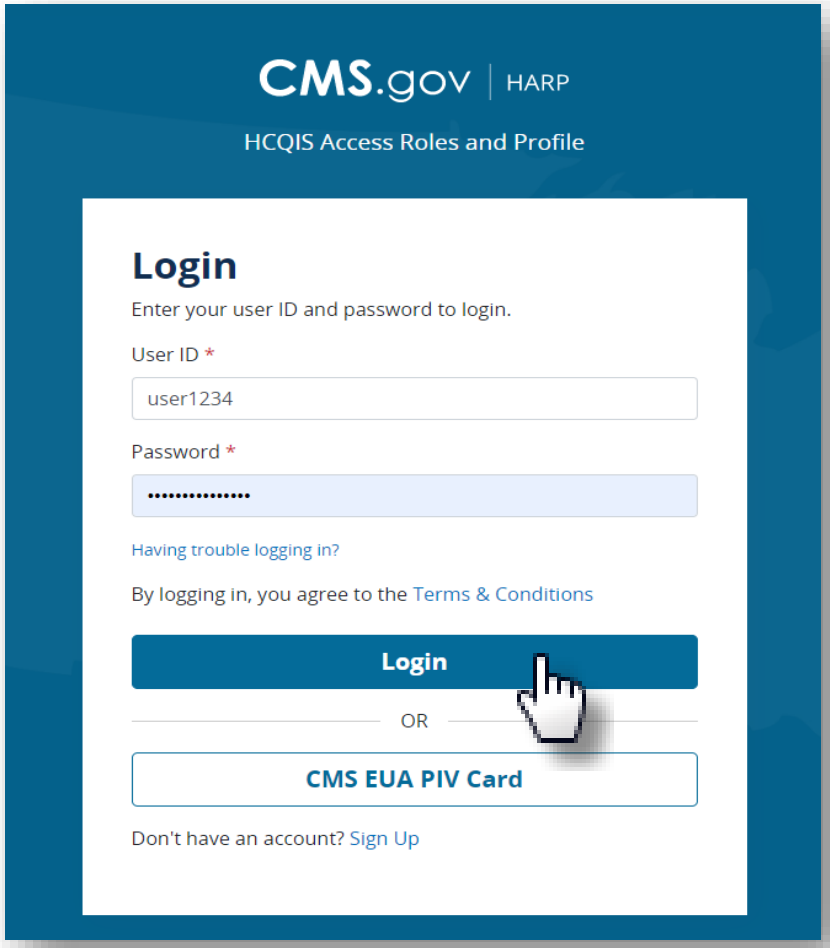
Account Created Confirmation

8. Your account is created. Click “Log into HARP” to access HARP and register additional two-factor authentication devices, if desired.



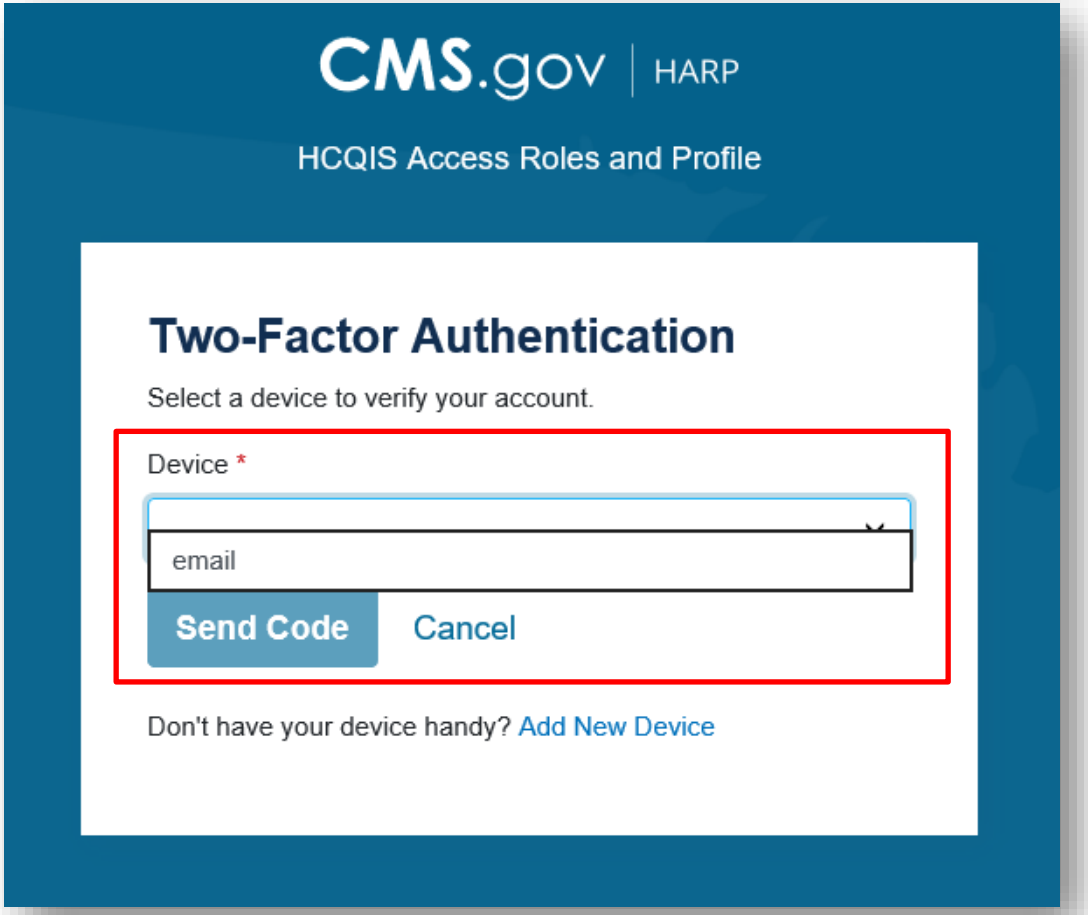
Log in to HARP

1. Enter your newly created User ID and Password. Agree to the Terms & Conditions and click “Login.”



Two-Factor Authentication Drop-Down

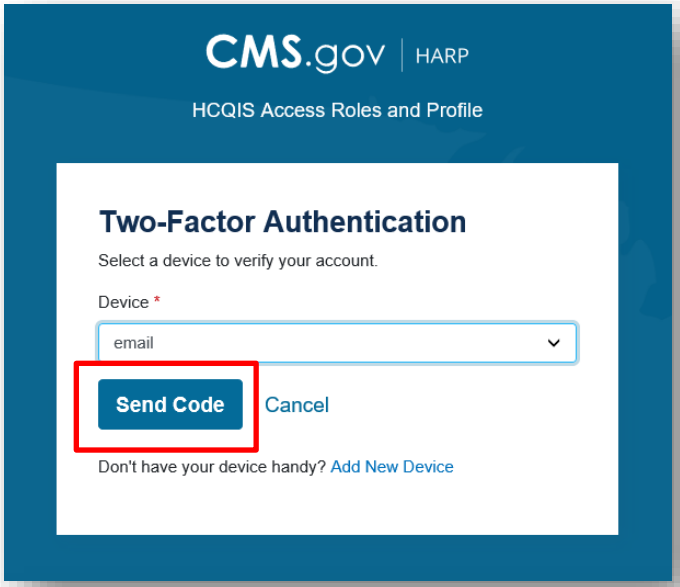
2. A Two-Factor Authentication screen displays. Click the Device drop-down.
3. "Email" displays as the only two-factor authentication device option. Select "email."



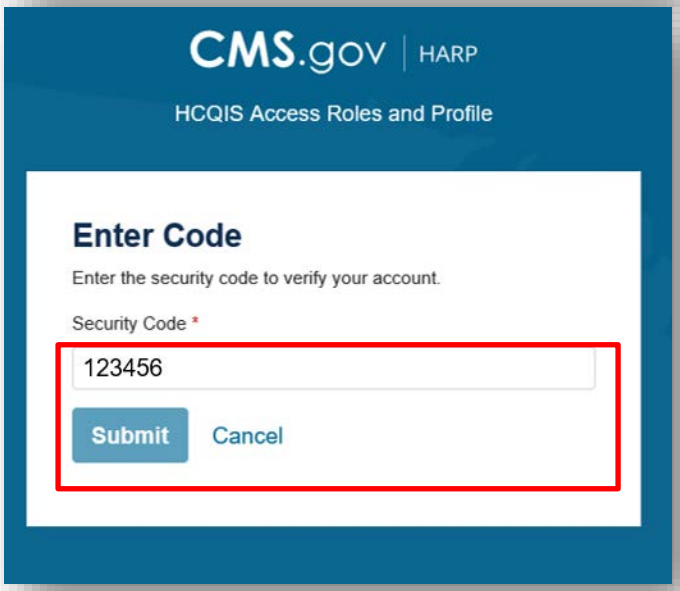
NOTE: HARP automatically sets the email address used to establish the account as the initial two-factor authentication device. Users must select email during the initial HARP login attempt. The email address may be changed after the initial log in.

Enter Security Code

4. Click “Send Code.” A one-time verification code is sent to the email address associated with the account. The Enter Code screen displays.

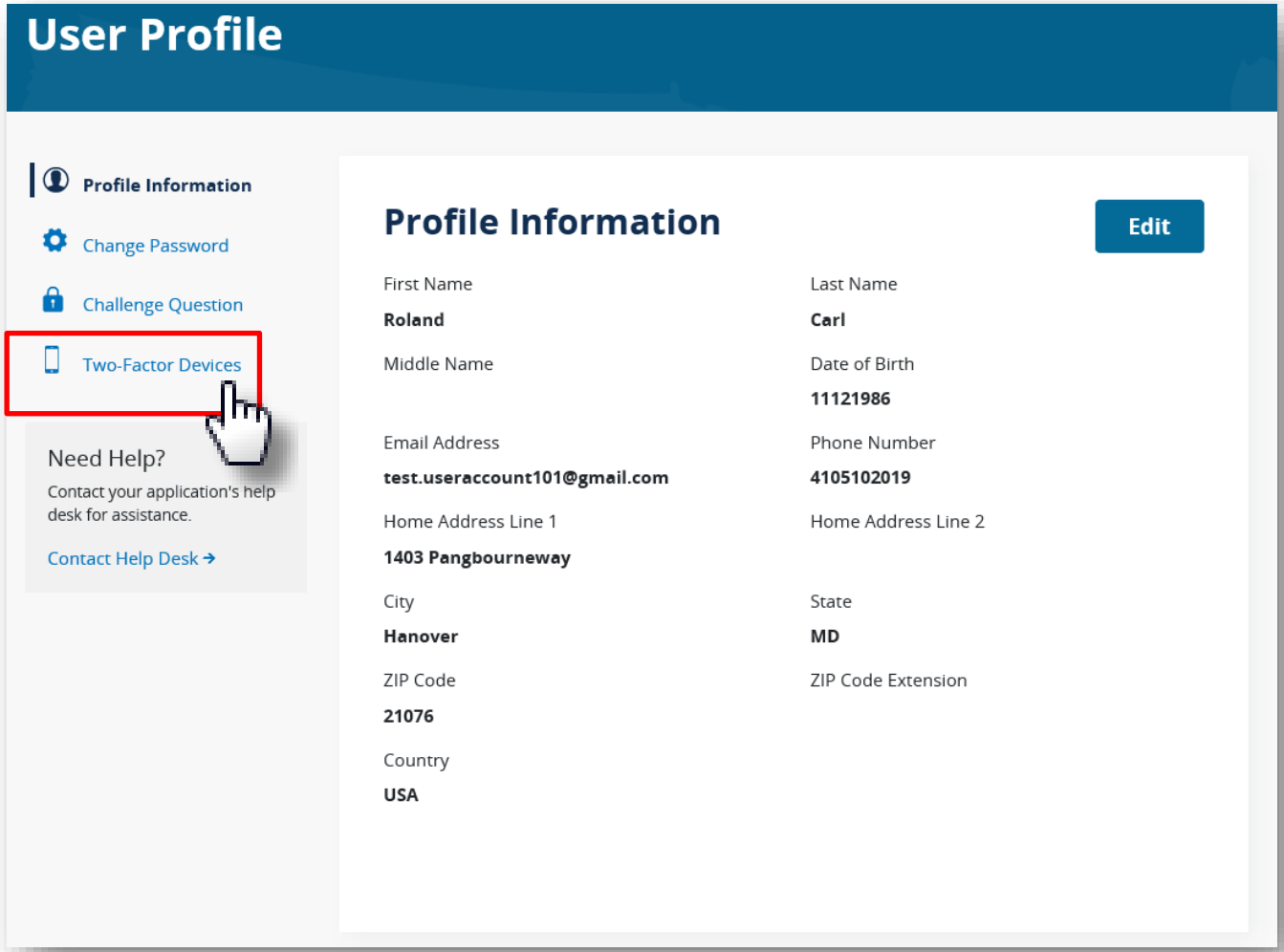


5. Enter the one-time verification code. Click “Submit.” The User Profile screen displays.



Setting Additional Two-Factor Device

6. Review the profile information for accuracy. Click "Two-Factor Device." A list of current two-factor authentication devices displays.



Selecting Additional Device

7. Click the Device Type drop-down arrow.

Select Two-Factor Authentication Device

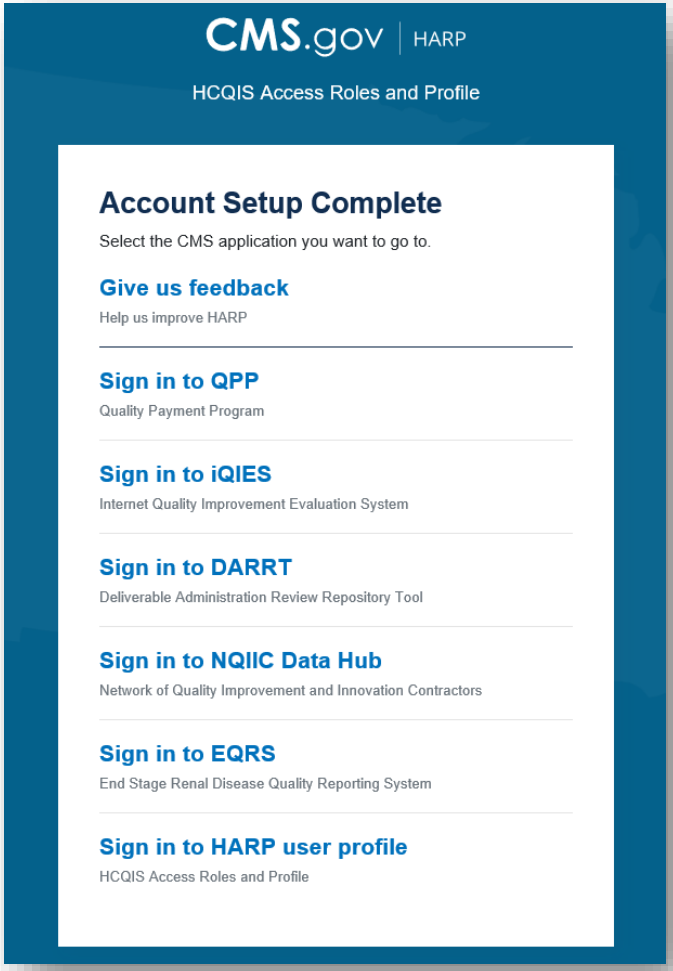
8. Select the desired additional two-factor authentication device.

Click Complete Setup

9. Follow the configuration requirements for the selected two-factor authentication device. The Status indicates “ACTIVE” once successfully configured.
10. Click “Complete Setup.”

Account Setup Complete

11. You have successfully created your account and can log in to your desired CMS application.

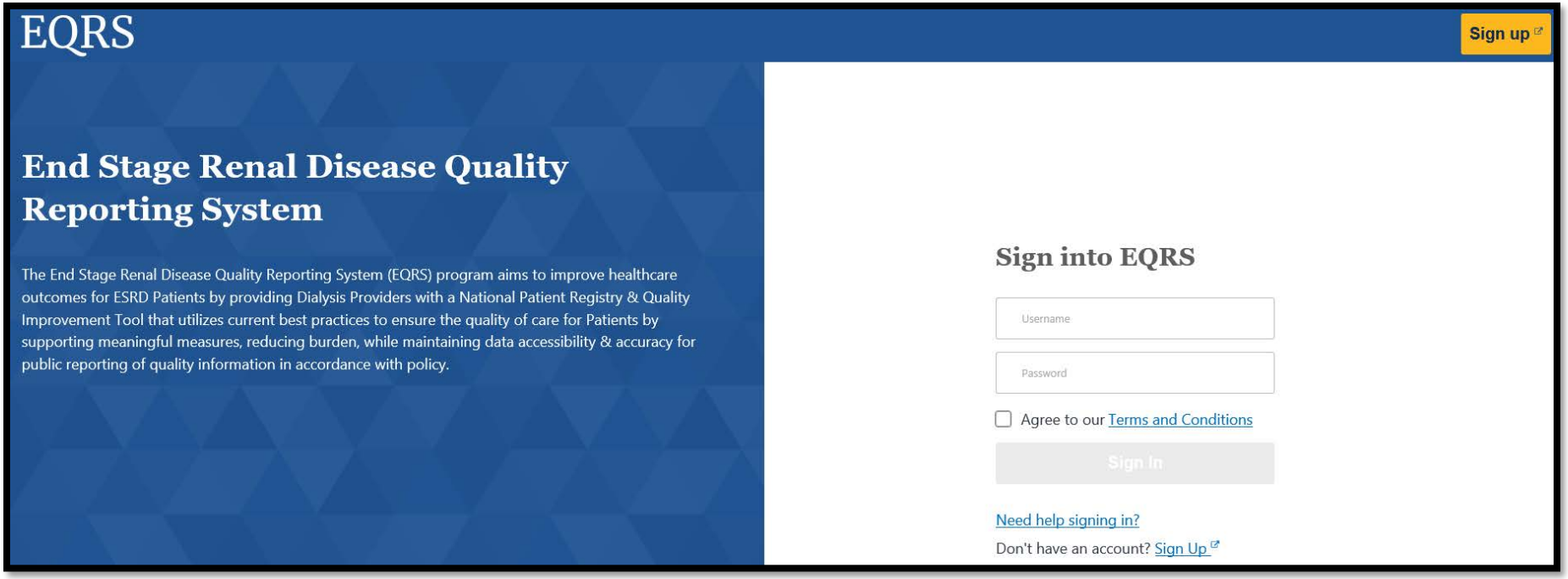


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Requesting Roles in EQRS

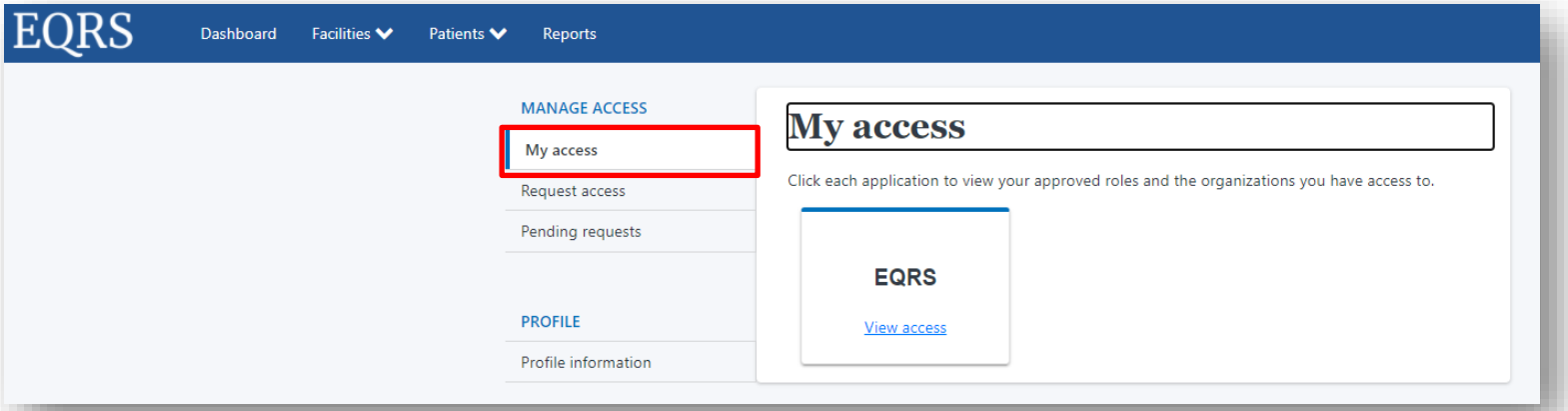
How to Access EQRS

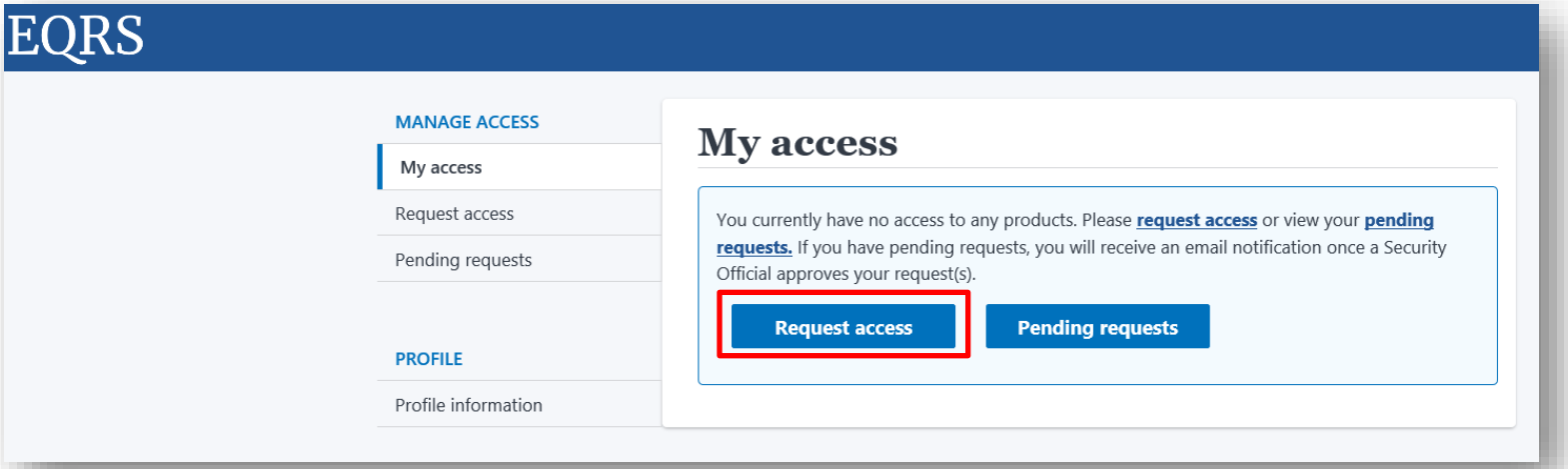
- Direct Link: https://eqrs.cms.gov/globalapp
- Users are currently redirected to https://eqrs.cms.gov/globalapp from QualityNet.cms.gov.



Go to My Access

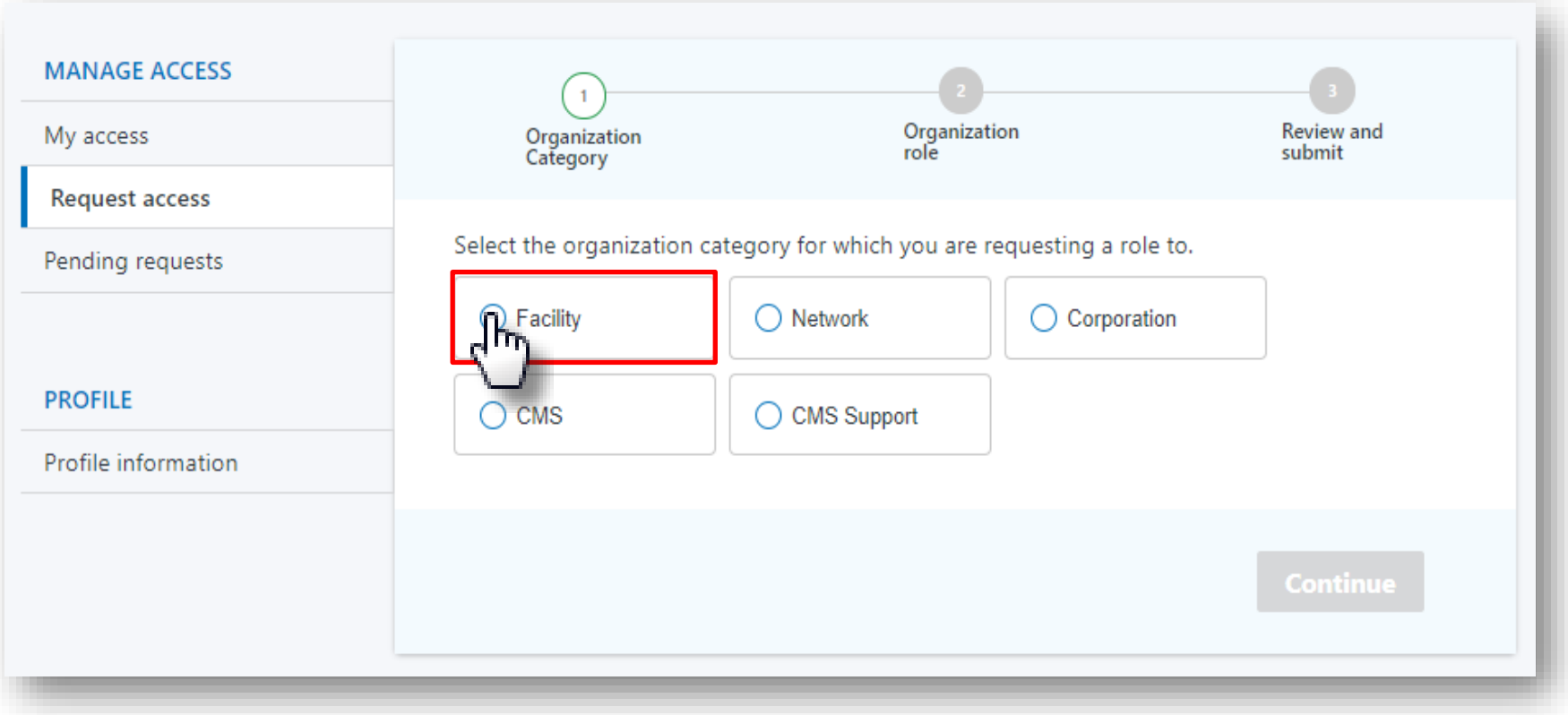
1. Log in to the ESRD Quality Reporting System (EQRS) via https://eqrs.cms.gov/globalapp. The My Access page displays.
2. Click "Request Access."





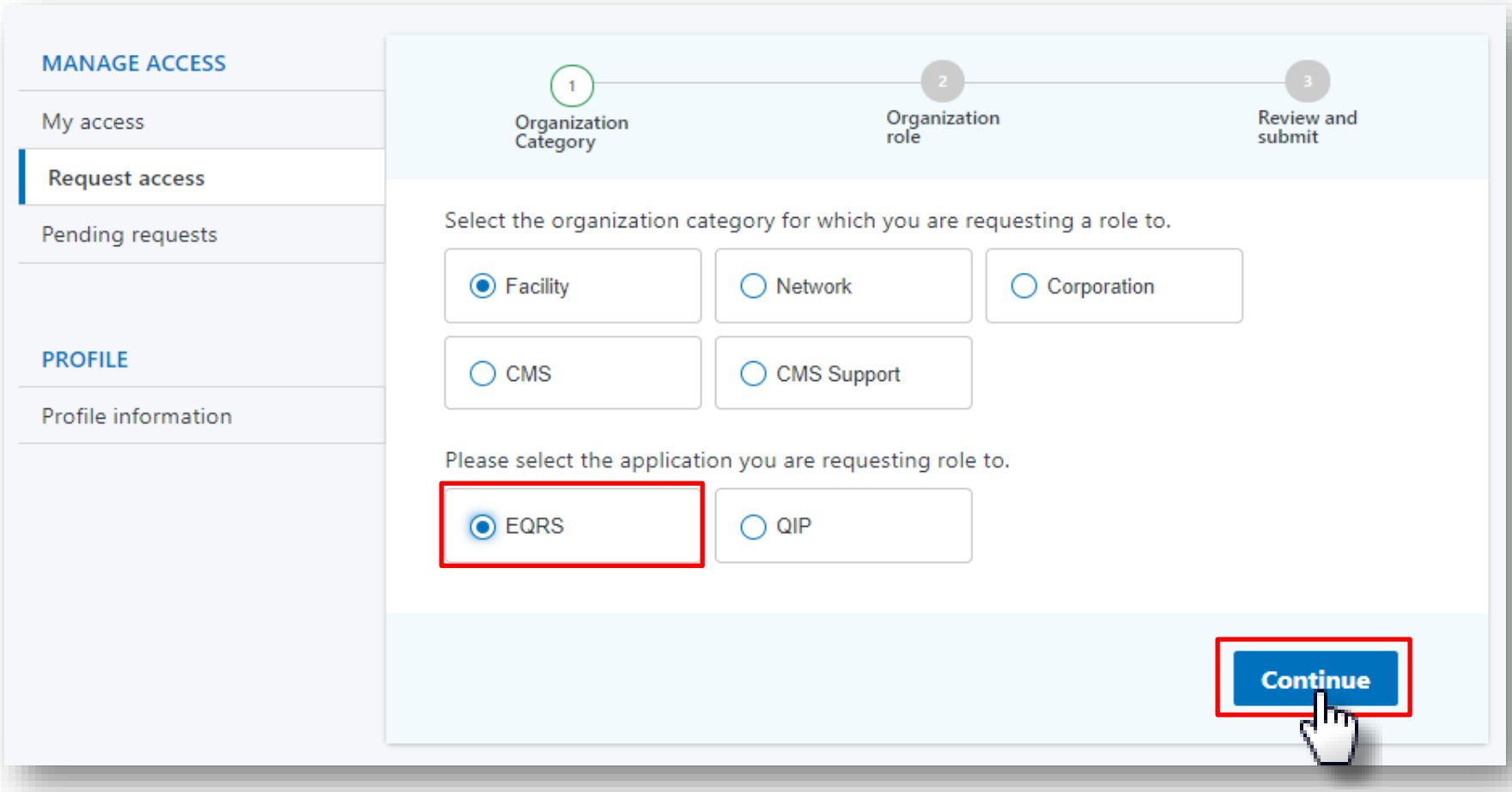
Select Organization

3. Select the organization category for which you are requesting a role.



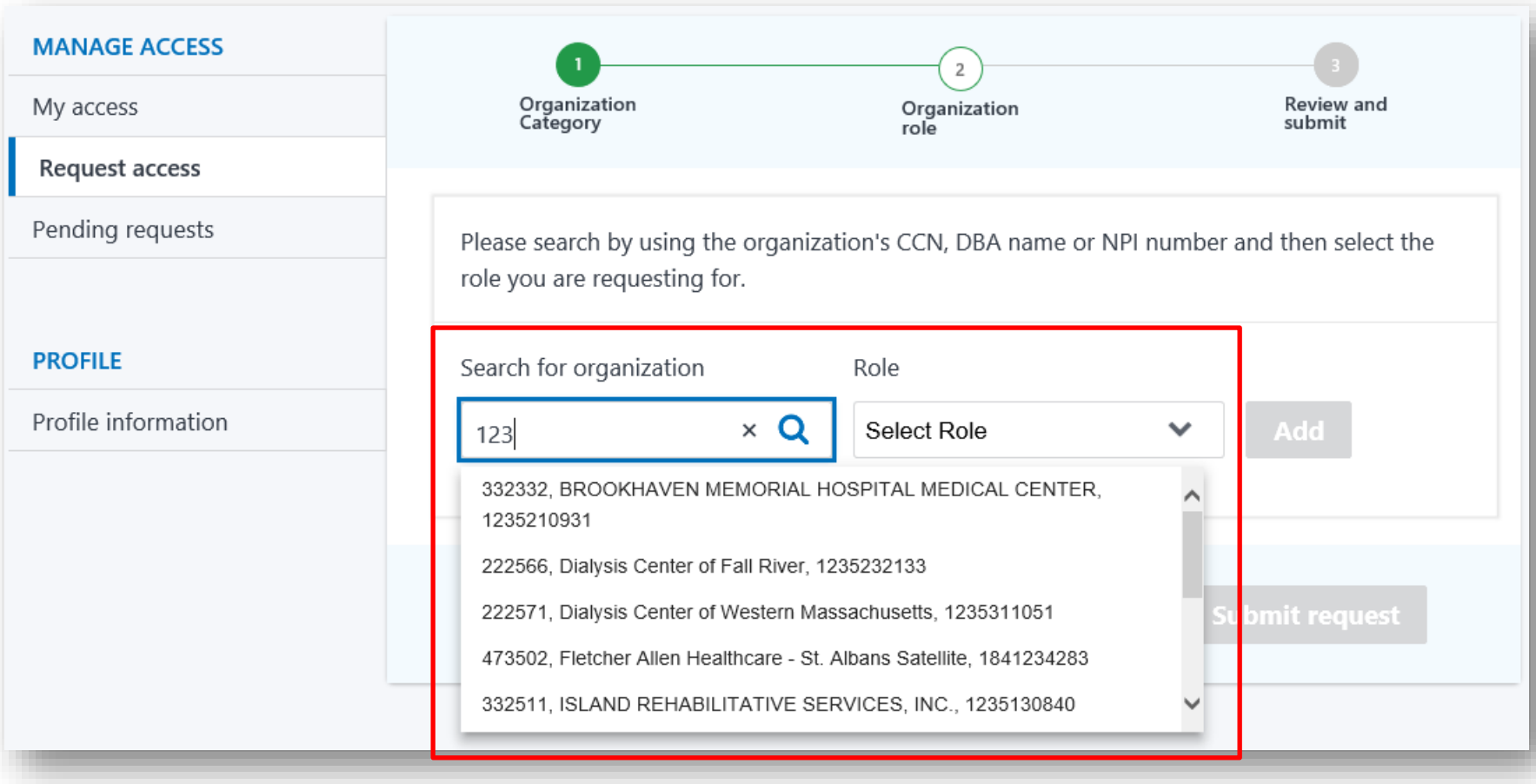
Select Application

4. Select the application to which you are requesting access and click “Continue.”



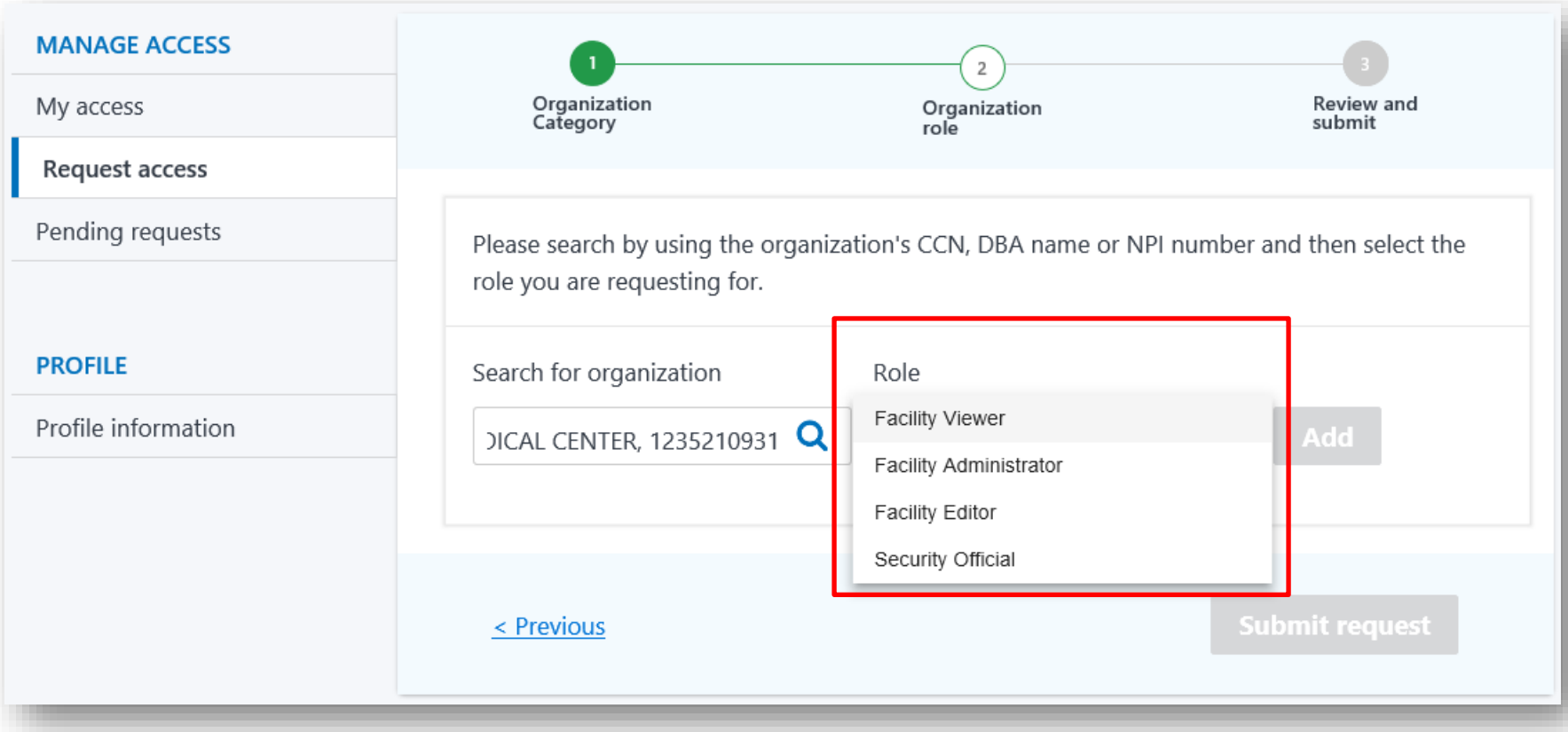
Search for Organization

5. Search for your organization.



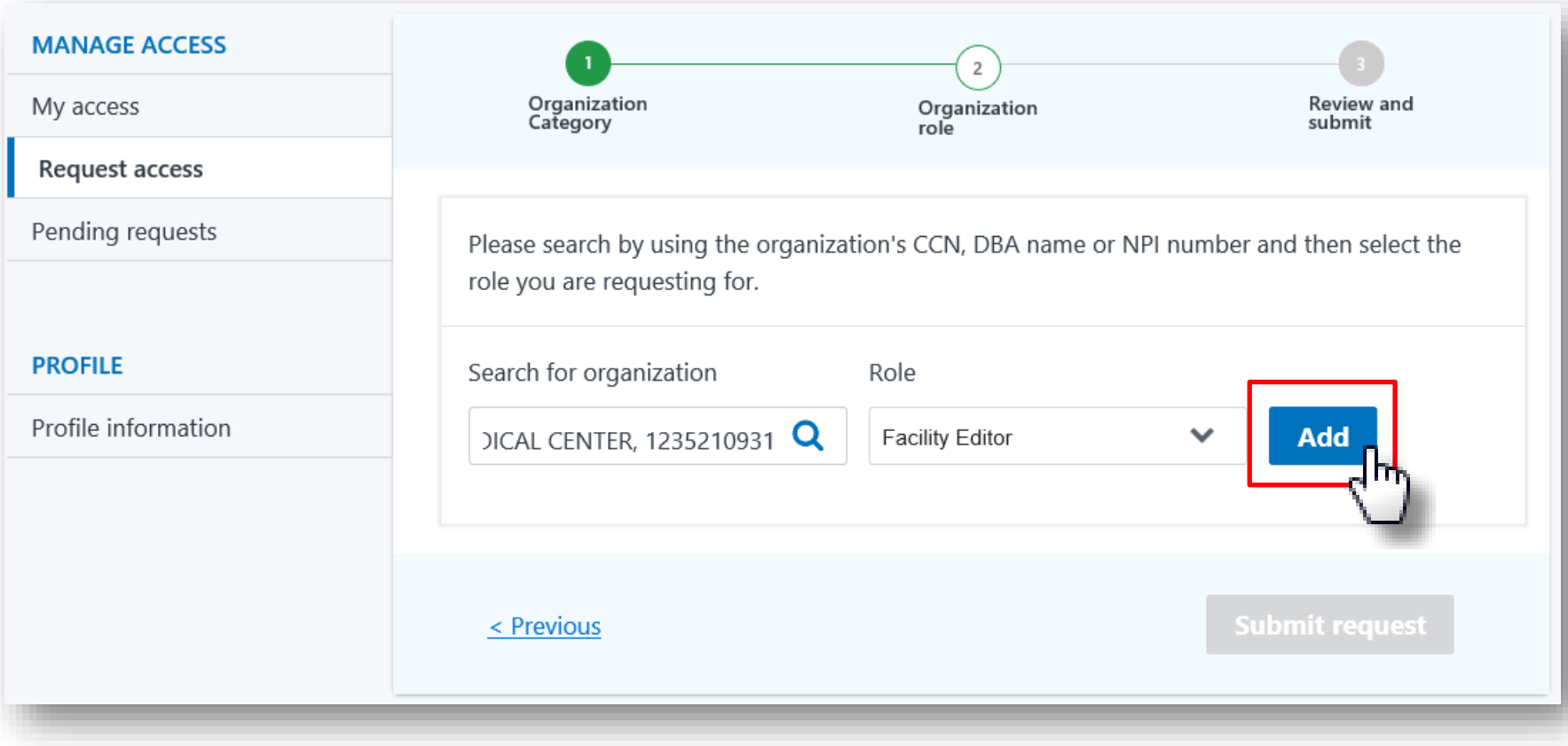
Select Role

6. Select desired role.



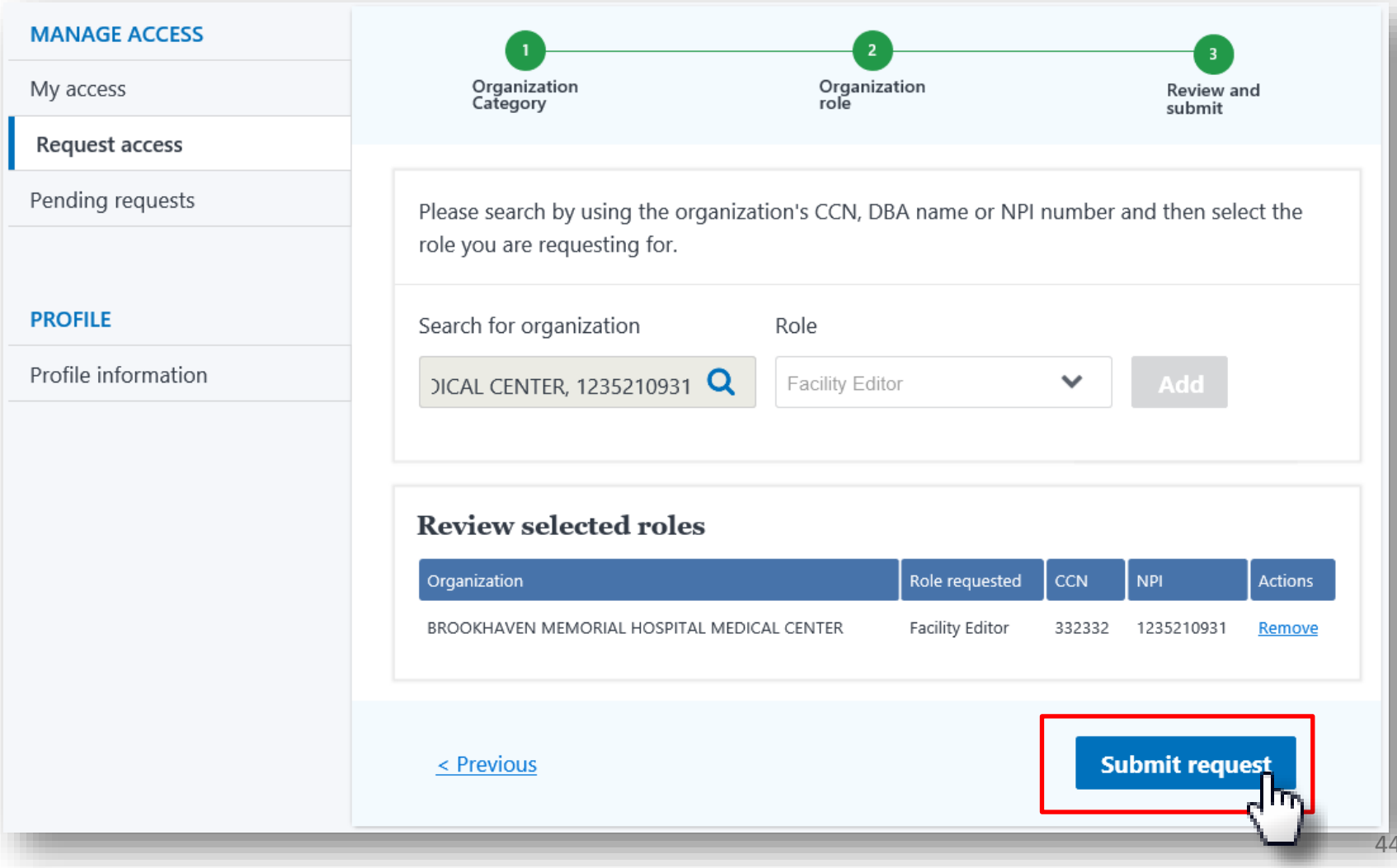
Click Add

7. Click “Add.”



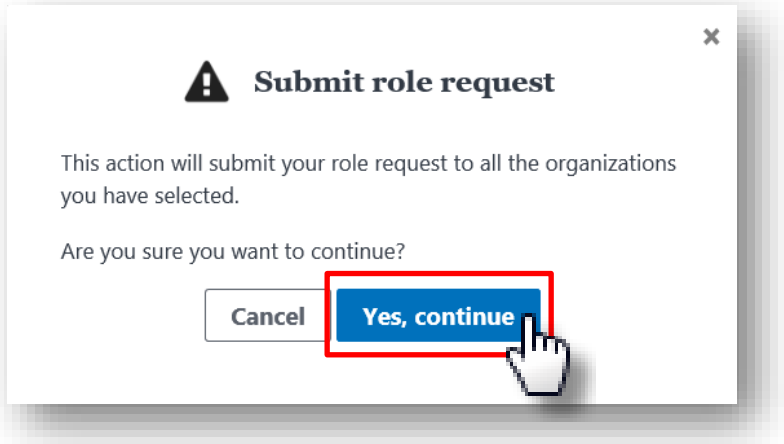
Submit Request

8. Review the selected role and click “Submit Request.”

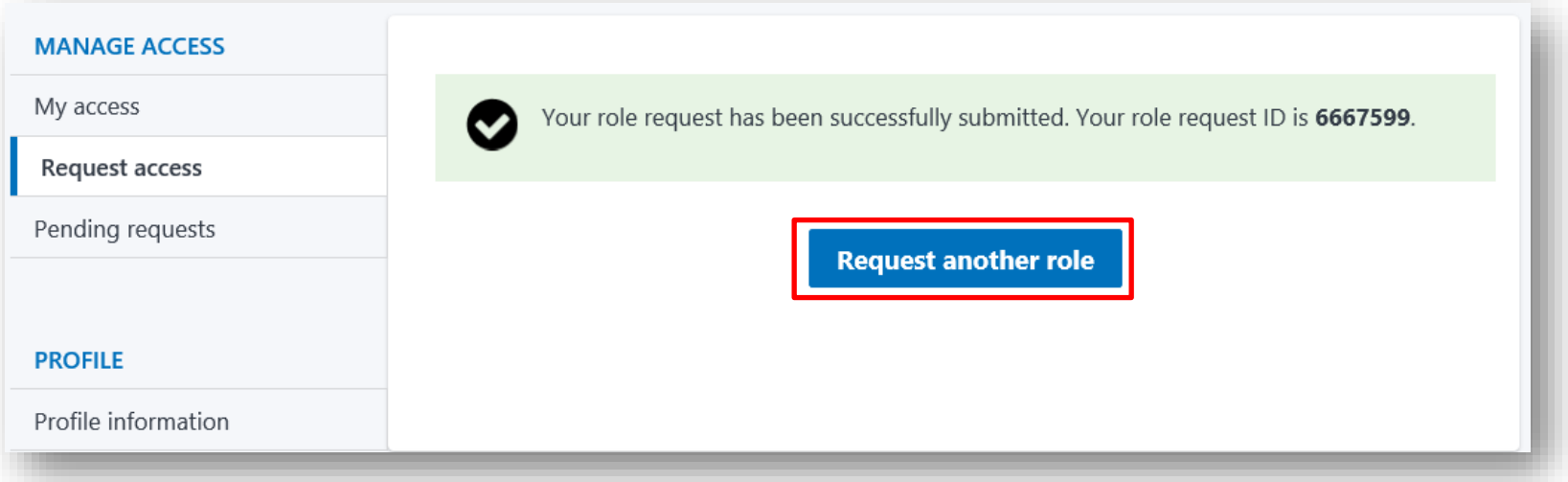


Request Submitted

9. Click “Yes, continue” to continue.



10. Request another role, if needed.

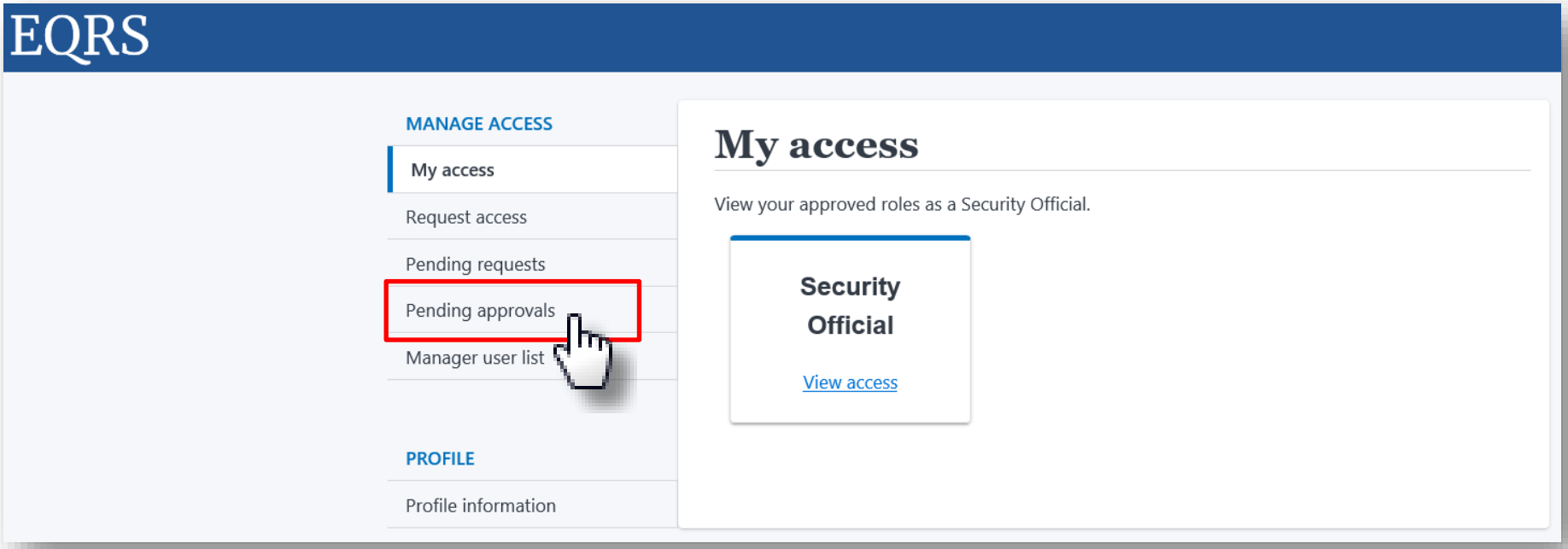


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Approving or Rejecting Requests as a Security Official in EQRS

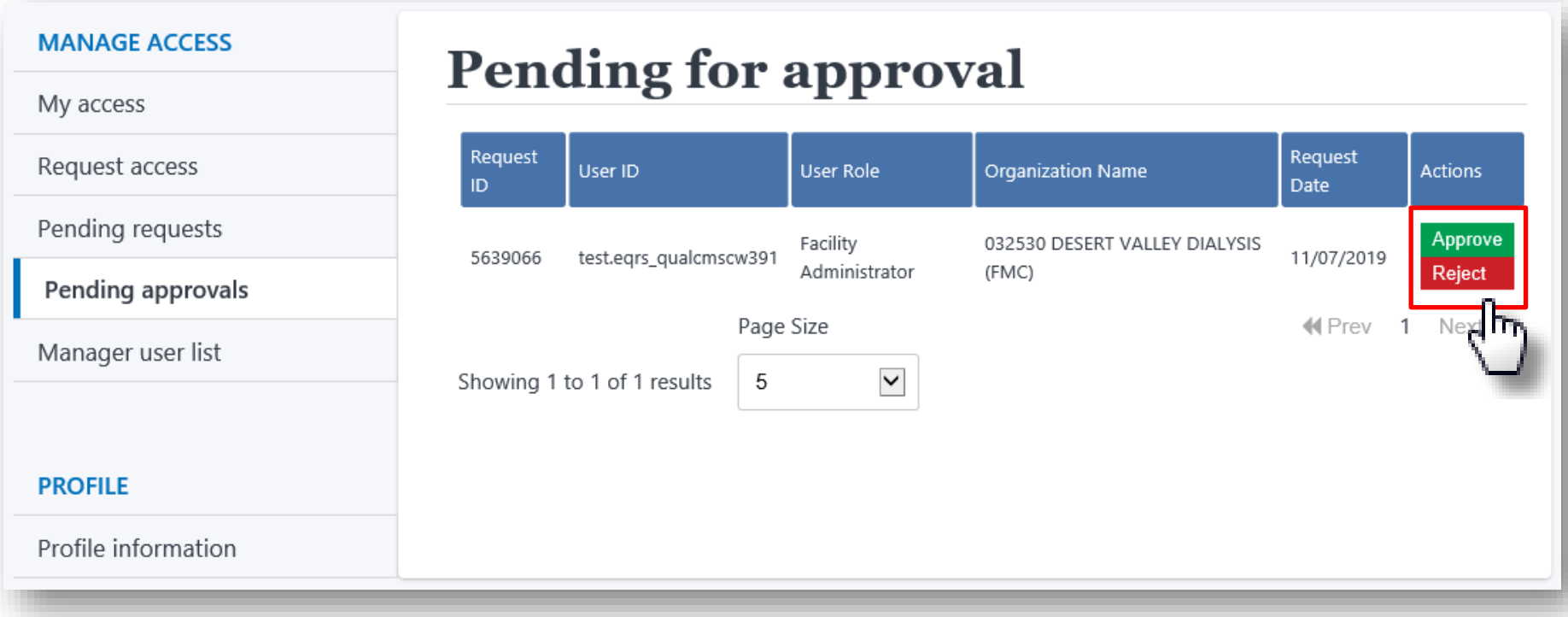
Go to My Access

1. Log in to EQRS. The Manage Access page displays.
2. Click “Pending Approvals.”



Approve or Reject Request

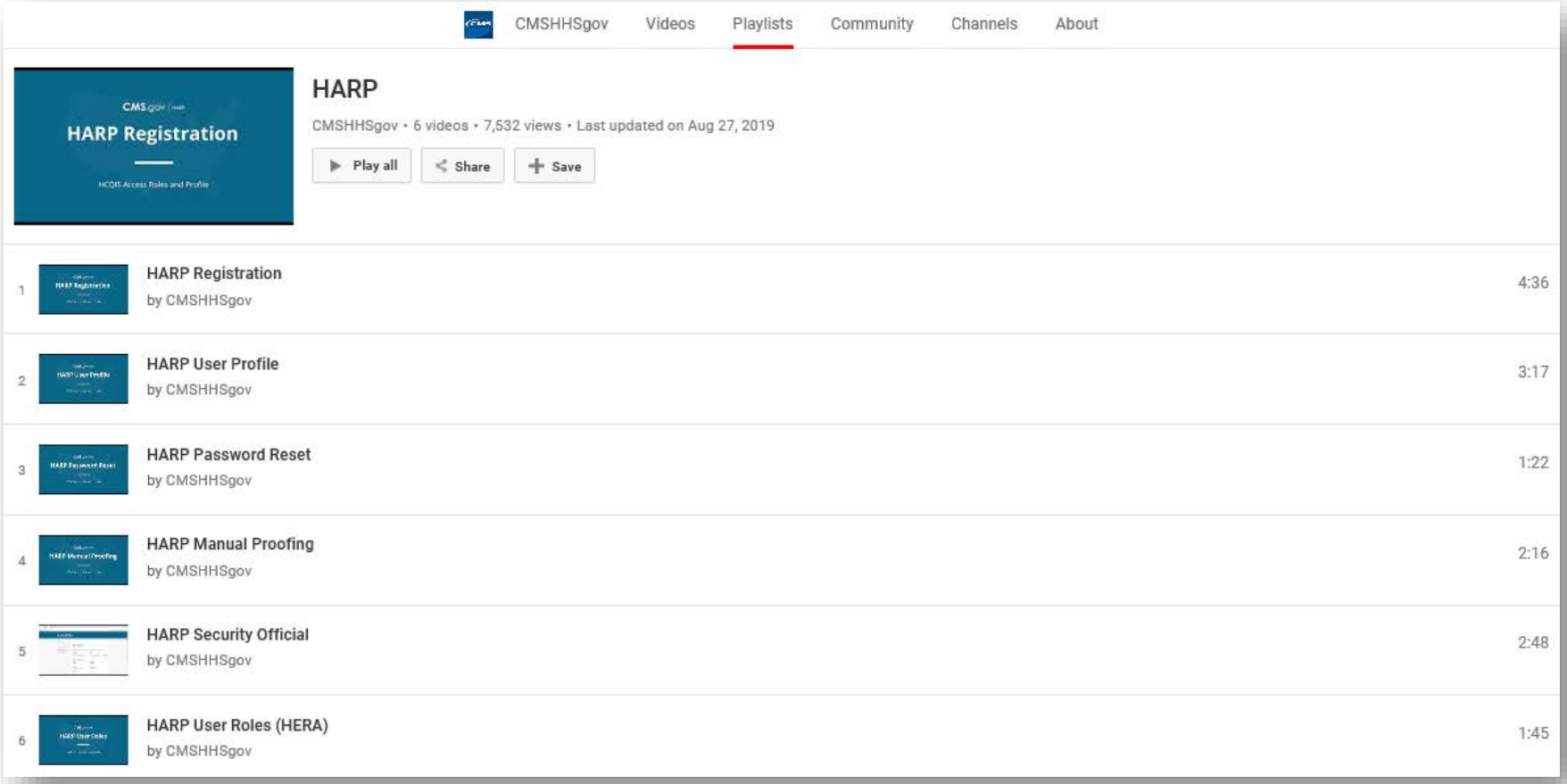
3. Review approval requests.
4. Click the “Approve” or “Reject” option in the Actions column.
5. The user is notified via email regarding if the request was approved or rejected.



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

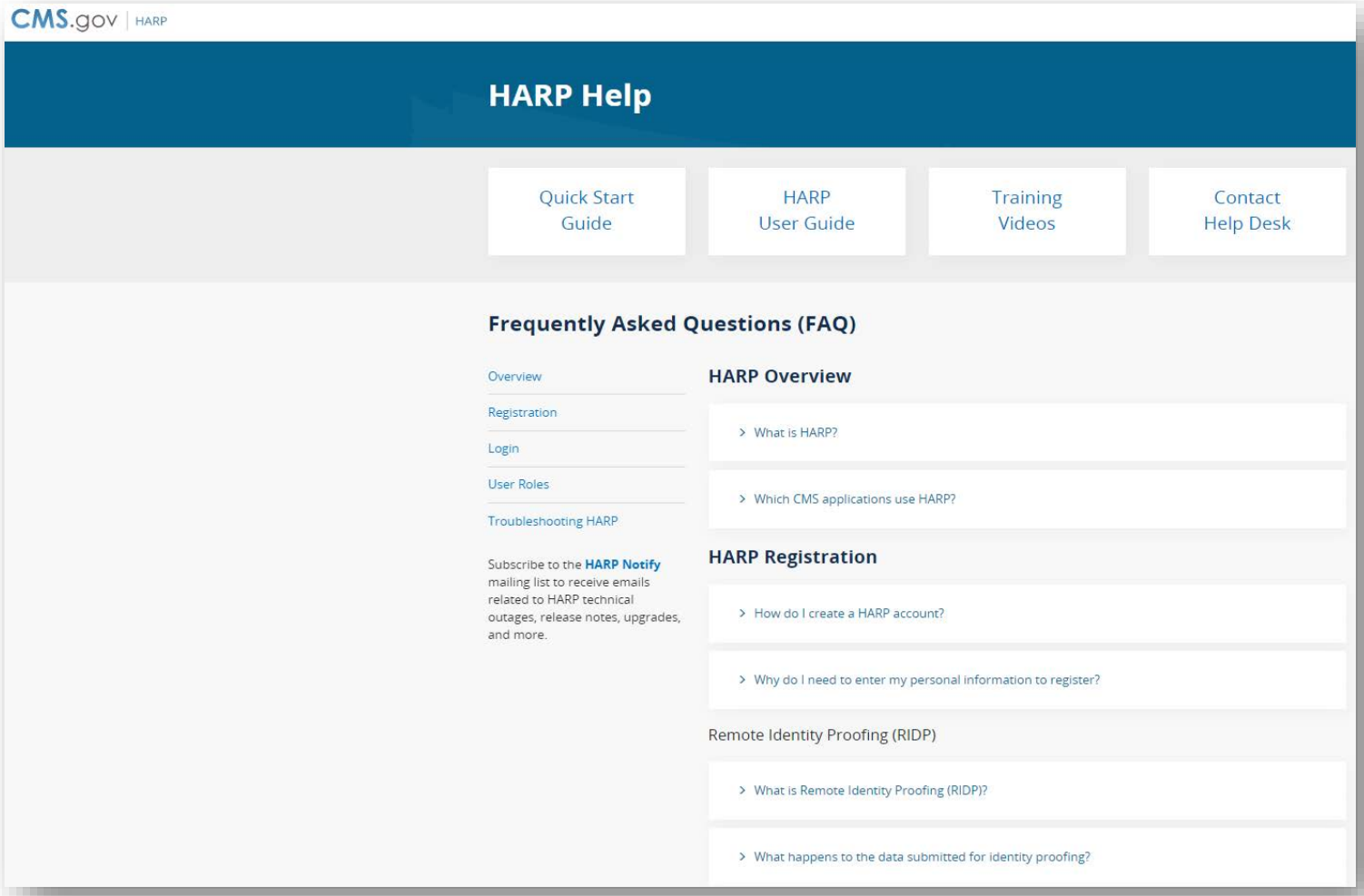
HARP Resources

HARP YouTube Videos



https://www.youtube.com/playlist?list=PLaV7m2-zFKphoCXj7sIx2G1fwMZQQ0EJP

HARP Help Webpage



https://harp.cms.gov/login/help

For Further Information…

- **Website: http://www.MyCROWNWeb.org**
- **Center for Clinical Standards and Quality (CCSQ) Service Center:**
  - **Phone: 1-866-288-8912**
  - **Email:** qnetsupport-esrd@cms.hhs.gov
  - **CCSQ Support Central**: https://cmsqualitysupport.servicenowservices.com/ccsq_support_central
- **General EQRS/ESRD QIP Questions: ESRD QIP Q&A Tool**