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

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

Type questions in the “Q&A” section, located to the right of your screen.

Send all Q&A questions to “All Panelists”

Note: Some questions may require additional research. Unanswered questions may be submitted to CRAFT@MyCROWNWeb.org.
Today’s Trainer

ESRD Outreach, Communication, and Training (EOCT) Team

Oniel Delva, MS, CTT+
Communications Director

Note:
Data used in this presentation is fictitious.
HARP Overview
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. Previously, users created accounts through the Enterprise Identity Data Management (EIDM) system.

• 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.

Initiate Manual Proofing

It is not recommended to initiate manual proofing if you are able to complete remote proofing, as manual proofing takes longer to complete.

To initiate manual proofing, you will need to complete the following steps:

1. Submit your Profile Information and Account Information via HARP (SSN is optional)
2. Send the following documents to your application's help desk via email, fax, or mail
   - **One** of three approved forms of Government Photo IDs:
     - Current driver's license issued by state or territory; OR
     - Federal or State government issued photo identification card; OR
     - U.S. Passport
   - **Two** copies of financial institution official bills or statements addressed to the address used during the registration process. Payroll information is also accepted.

The help desk will contact you via email if they need to request additional information.
HARP Roles
## HARP Roles

<table>
<thead>
<tr>
<th>User Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.  |
EIDM Accounts to HARP
CMS automatically migrated existing EIDM accounts and user roles to HARP. To complete the migration, EIDM account holders should:

– Log in to HARP.
– Select a Challenge Question.
– Register additional two-factor authentication devices, if desired.
1. Go to [https://harp.qualitynet.org/login/](https://harp.qualitynet.org/login/).
2. Enter your EIDM Username and Password.
3. Check the box next to “I agree to the Terms & Conditions.” Click Login.
Two-Factor Authentication 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.
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.
8. Review the profile information for accuracy. Click “Challenge Question.”
9. Enter Password.
10. Click the Challenge Question drop-down arrow.
11. Select the desired Challenge Question.
12. Enter the Challenge Question Answer.
13. Click “Save.”
14. HARP refreshes with “Challenge Question updated” message.
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.

Set Up Two-Factor Authentication

You are required to set up two-factor authentication. Enter the fields below to add one or more two-factor authentication devices to your account. Learn More

All fields marked with an asterisk (*) are required.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Contact</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td></td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

Add Device

Device Type *

Select the device type from the dropdown menu.
3. Select the desired additional two-factor authentication device.

Set Up Two-Factor Authentication

You are required to set up two-factor authentication. Enter the fields below to add one or more two-factor authentication devices to your account. Learn More

All fields marked with an asterisk (*) are required.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Contact</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td></td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

Add Device

Device Type *

- SMS
- Voice
- Google Authenticator
- Okta Verify
- Okta Verify Push
<table>
<thead>
<tr>
<th>Device Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Default two-factor authentication device. Cannot be removed. You can edit this to another email address.</td>
</tr>
<tr>
<td>SMS</td>
<td>Enter your mobile phone number to receive a text with a security code.</td>
</tr>
<tr>
<td>Voice</td>
<td>Enter your phone number to receive a call with a security code.</td>
</tr>
<tr>
<td>Google Authenticator</td>
<td>The Google Authenticator application generates two-factor authentication codes on your mobile device.</td>
</tr>
<tr>
<td>Okta Verify</td>
<td>The Okta Verify application generates two-factor authentication codes on your mobile device.</td>
</tr>
<tr>
<td>Okta Verify Push</td>
<td>The Okta Verify Push application generates two-factor authentication codes on your mobile device.</td>
</tr>
</tbody>
</table>
4. Follow the configuration requirements for the selected two-factor authentication device. The Status indicates “ACTIVE” once successfully configured.
5. Click “Complete Setup.”
Registering for a New HARP Account
New HARP Account Registration

• New users can create a HARP account by going to https://harp.qualitynet.org/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.

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. Agree to the Terms & Conditions, and click “Next.”
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 Desk 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.
1. Enter your newly created User ID and Password. Agree to the Terms & Conditions, and click “Login.”
Two-Factor Authentication 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.
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.

User Profile

Profile Information

First Name
Roland

Middle Name

Email Address
test.useraccount101@gmail.com

Home Address Line 1
1403 Pangbourneway

City
Hanover

ZIP Code
21076

Country
USA

Last Name
Carl

Date of Birth
11121986

Phone Number
4105102019

Home Address Line 2

State
MD

ZIP Code Extension
7. Click the Device Type drop-down arrow.

**Set Up Two-Factor Authentication**

You are required to set up two-factor authentication. Enter the fields below to add one or more two-factor authentication devices to your account. [Learn More](#)

All fields marked with an asterisk (*) are required.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Contact</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td></td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

**Add Device**

Device Type *

[Drop-down arrow]
Select Two-Factor Authentication Device

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

Set Up Two-Factor Authentication

You are required to set up two-factor authentication. Enter the fields below to add one or more two-factor authentication devices to your account. Learn More

All fields marked with an asterisk (*) are required.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Contact</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td></td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

Add Device

Device Type *

- SMS
- Voice
- Google Authenticator
- Okta Verify
- Okta Verify Push
9. Follow the configuration requirements for the selected two-factor authentication device. The Status indicates “ACTIVE” once successfully configured.
10. Click “Complete Setup.”
11. You have successfully created your account and can log in to your desired CMS application.
Requesting Roles in EQRS
How to Access EQRS/CROWNWeb

- Direct Link: https://eqrs.cms.gov/globalapp
- Users are currently redirected to https://eqrs.cms.gov/globalapp from QualityNet.org.
2. Click “Request Access.”
3. Select the organization category for which you are requesting a role.
4. Select the application to which you are requesting access and click “Continue.”
5. Search for your organization.
6. Select desired role.
Click Add

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

<table>
<thead>
<tr>
<th>Organization</th>
<th>Role requested</th>
<th>CCN</th>
<th>NPI</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BROOKHAVEN MEMORIAL HOSPITAL MEDICAL CENTER</td>
<td>Facility Editor</td>
<td>322332</td>
<td>1235210931</td>
<td>Remove</td>
</tr>
</tbody>
</table>
9. Click “Yes, continue” to continue.

10. Request another role, if needed.
Approving or Rejecting Requests as a Security Official in EQRS
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.
HARP YouTube Videos

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

HARP Help
Frequently Asked Questions (FAQ)

Check out our HARP training videos on YouTube.

HARP Overview

- What is HARP?
- Which CMS applications use HARP?

HARP Registration

- How do I create a HARP account?
- Why do I need to enter my personal information to register?

Remote Identity Proofing (RIDP)

- What is Remote Identity Proofing (RIDP)?
- What happens to the data submitted for identity proofing?

https://harp.qualitynet.org/login/help
Questions
For Further Information...


Website: https://www.mycrownweb.org/

QualityNet Service Desk: 1-866-288-8912

QualityNet Service Desk Email: qnetsupport-esrd@hcqis.org

ESRD QIP Questions: ESRD QIP ServiceNow Q&A Tool

A survey will pop up in your browser when the session ends.

Please follow the link and let us know what you think and what you would like to be covered in future training events, thank you!