

5 SECURE QUALITYNET PORTAL

Note: This section applies only to ASCQR, PCHQR, and IPFQR program users who will access the new Secure QualityNet Portal.

This section provides the following instructions:

- How to prepare for first-time login
- First-time login process: proofing one's identity and enrolling a credential
- Logging into Secure QualityNet Portal
- Navigating Secure QualityNet Portal
- Managing users of Secure QualityNet Portal
- Logging out of Secure QualityNet Portal

There is no file exchange capability within the Secure QualityNet Portal. Security Administrators are able to access the QualityNet System File Exchange applications (see Section 7.5 in this manual) and can securely exchange files for users if this capability is required prior to Data Service availability with the portal.

5.1 New User Enrollment Process - Prerequisite for Secure Portal Usage

Before you log in to the Secure QualityNet Portal for the first time, you must complete the New User Enrollment Process. The prerequisites for this process are:

- A completed QualityNet [Registration](#) that in turn has allowed your organization's Security Administrator to provide you with a QualityNet user ID and password.
- A Symantec VIP multifactor credential application downloaded to your PC, tablet, or smartphone.
 - To download the multifactor authentication application to your PC or tablet, access the [Verisign ID Protection Center](https://idprotect.verisign.com/desktop/download.v) web site:
<https://idprotect.verisign.com/desktop/download.v>
 - To download the multifactor authentication application directly to your smartphone, type the following into your default mobile browser: m.verisign.com

Important:

You will only complete this new user enrollment process once; you will not do this every time you log into the Secure QualityNet Portal. This one-time process is a six-step procedure that should take you no longer than five minutes to complete if you have all of your prerequisites in hand.

Some users will find they cannot complete the proofing part of the new user enrollment process as they will experience errors. Here are some explanations of why this might happen:

- The identity proofing steps of this process include identity verification by Experian, an external service that CMS has engaged to verify user identities. Experian uses your credit

history within their extensive financial databases to confirm that you are who you say you are. If you do not have much credit history or if you have had problems with credit in the past, the online steps of the process may not work for you. If this happens, there are alternative options. If you find you cannot complete the proofing process online, you may be given the option to complete the proofing process with Experian via a phone call. This option will be offered if you have some credit history.

- If you have little or no credit history, you will be offered the option to prove your identity directly, in-person, with your Security Administrator.

While you are on the Identity Proofing screen during the enrollment process (see Figure 5-4), please review the **Remote Proofing FAQ** link for more details and Q&A about the proofing process. You may also visit [Experian's PreciseID](http://www.experian.com/whitepapers/precise_id_whitepaper.pdf) web site, http://www.experian.com/whitepapers/precise_id_whitepaper.pdf, for more details about the proofing process.

Note: The proofing process makes what is known as a soft inquiry on your credit history. The process will not adversely affect your credit rating.

5.2 First-Time Login to Secure QualityNet Portal

1. Have your Symantec VIP multifactor authentication application open and ready to use.
2. Access the [QualityNet](https://www.qualitynet.org) web site: <https://www.qualitynet.org>. The QualityNet home page appears, with a link to the Secure QualityNet Portal in the upper-right corner of the page.

Figure 5-1. QualityNet Home Page and LOGIN Link

The screenshot displays the QualityNet Home Page. At the top, there is a header with the QualityNet logo, a sign-in button, and a search bar. Below the header is a navigation bar with tabs for Home, My QualityNet, and Help. Under the My QualityNet tab, there are links for Hospitals - Inpatient, Hospitals - Outpatient, Physician Offices, ASCs, ESRD, and Quality Improvement. The main content area is divided into several sections: QualityNet Registration (listing various facility types), Getting started with QualityNet (listing system requirements and guides), Join ListServes, Known Issues - Hospital Reporting, QualityNet News (featuring a headline about the FY 2014 IPPS rule), About QualityNet, Login to Secure QualityNet Portal, Know the Security Policy, Questions & Answers, Downloads, and Training.

QualityNet
Sign in to My QualityNet (formerly QNet Exchange)
Sign In

Home My QualityNet Help

Hospitals - Inpatient Hospitals - Outpatient Physician Offices ASCs ESRD Quality Improvement

QualityNet Registration

- Hospitals - Inpatient
- Hospitals - Outpatient
- Physician Offices
- ASCs
- Cancer Hospitals
- ESRD Facilities
- Inpatient Psychiatric Facilities
- QIOs

Getting started with QualityNet

- System Requirements
- Test Your System
- Registration
- Sign-In Instructions
- Security Statement
- Password Rules
- QualityNet User's Guide, PDF
- QualityNet Reports User's Guide, PDF

Join ListServes
Sign up for Notifications and Discussions.

Known Issues - Hospital Reporting

- Inpatient
 - Hospital Value-Based Purchasing
- Outpatient

QualityNet News [More News »](#)

FY 2014 IPPS proposed rule posted, open for public comment
The proposed rule for changes to the hospital Inpatient Prospective Payment Systems (IPPS) for acute care hospitals and Fiscal Year (FY) 2014 rates is on display and open for public comment. To be assured consideration, comments must be received no later than 5 p.m. EDT on June 25, 2013.

Included in the regulation are proposed changes to quality reporting requirements for: the Hospital Inpatient Quality Reporting (IQR) Program; the PPS-Exempt Cancer Hospital Quality Reporting (PCHQR) Program; Inpatient Psychiatric Facilities Quality Reporting (IPFQR) Program; the Hospital Value-Based Purchasing (VBP) Program; and Ambulatory Surgical Centers (ASCs).

[Full Article »](#)

Headlines

- [Hospital Compare Preview Reports now available](#)
- [Inpatient hospitals selected for FY 2015 validation](#)
- [Contact Help Desk regarding OQR pledge changes](#)
- [CMS seeks comment on conversion to ICD-10 specifications for OIE measures](#)
- [Inpatient Psychiatric Facility Quality Reporting webinar set for March 14](#)
- [New programs added to CMS Questions and Answers tool](#)
- [Notice of Participation Form available for Inpatient Psychiatric Facility Quality Reporting](#)
- [Cancer Measures Specifications published](#)
- [Members named to HVBP Monitoring and Evaluation Strategies Technical Expert Panel](#)

About QualityNet

Established by the Centers for Medicare & Medicaid Services (CMS), QualityNet provides healthcare quality improvement news, resources and data reporting tools and applications used by healthcare providers and others.

QualityNet is the only CMS-approved website for secure communications and healthcare quality data exchange between: quality improvement organizations (QIOs), hospitals, physician offices, nursing homes, end stage renal disease (ESRD) networks and facilities, and data vendors.

[More »](#)

Login to Secure QualityNet Portal
[Login](#)

Know the Security Policy
Before transmitting or receiving healthcare information or data, read the QualityNet System Security Policy, PDF

Questions & Answers

- Hospitals - Inpatient
- Hospitals - Outpatient
- Ambulatory Surgical Centers
- Inpatient Psychiatric Facilities
- PPS-Exempt Cancer Hospitals

Note: First-time registration required

Downloads

- CART - Inpatient
- CART - Outpatient
- CART Module Designer

Training

- QualityNet Training
- QualityNet Event Center

3. Click the Secure QualityNet Portal **Login** link.

4. **ASCQR, IPFQR, and PCHQR Program users will** see the following two-factor authentication login page. Note that this is not the same as a MyQualityNet login page.

Figure 5-2. Secure QualityNet Portal Log In Page – New User

The screenshot shows the CMS.gov QualityNet login page. At the top, the CMS.gov logo is on the left and 'QualityNet' is on the right, with 'Centers for Medicare & Medicaid Services' below. The main content area is titled 'Log In to QualityNet' with a red asterisk and 'Required Field'. Below the title, it says 'Please enter your CMS User ID and password, followed by your Symantec VIP Security Code, then click Submit.' There are three input fields: '* User ID', '* Password', and '* Security Code'. Below these fields are 'CANCEL' and 'SUBMIT' buttons. To the right of the login form is a yellow 'Help' box with a question mark icon. The 'Help' box contains the text 'Start/Complete New User Enrollment', 'Forgot your password?', 'Trouble with your Security Code?', and 'Need to register for a QualityNet account?'.

5. Click **Start/Complete New User Enrollment** in the yellow **Help** box. The following page appears (see Figure 5-3):

Figure 5-3: Starting and Completing New User Enrollment

The screenshot shows the CMS.gov QualityNet 'Starting and Completing New User Enrollment' page. At the top, the CMS.gov logo is on the left and 'QualityNet' is on the right, with 'Centers for Medicare & Medicaid Services' below. Below the header is a progress bar with six steps: 'Login', 'Verify Identity', 'Identity Questions', 'Identity Confirmed', 'Enroll Credential', and 'Enrollment Confirmed'. The main content area is titled 'Starting and Completing New User Enrollment'. It contains a paragraph explaining the enrollment process, a paragraph about the login process, and a paragraph about the progress bar. To the right of the main content area is a blue box titled 'Log In to QualityNet' with a red asterisk and 'Required Field'. It contains two input fields: '* User ID' and '* Password'. Below these fields are 'CANCEL' and 'SUBMIT' buttons. To the right of the login box is a yellow 'Help' box with a question mark icon. The 'Help' box contains the text 'Forgot your password?'. To the right of the 'Help' box is a white box with a black border containing the text 'User ID is not case-sensitive; Password is case-sensitive.'

6. Type your User ID, which is not case-sensitive, and your password, which is case-sensitive, and then click **SUBMIT**. The Verify Identity page appears (see Figure 5-4).

Figure 5-4. Verify Identity Page

CMS.gov | QualityNet
Centers for Medicare & Medicaid Services

Login **Verify Identity** Identity Questions Identity Confirmed Enroll Credential Enrollment Confirmed

Verify Your Identity

To verify your identity, CMS uses an Identity Proofing Service provided by Experian.

You will be asked for personal information about yourself; this information will be securely encrypted and sent to Experian. Experian will return a series of personal questions for you to answer. After you answer the questions, Experian will confirm whether you provided the right information to prove you are who you say you are. For a better understanding on the data collected and how it is used, please visit the identity proofing frequently asked questions:

[Remote Proofing FAQs](#)

Please enter the answers to the following information and click Submit.

Personal Information * Required Field

* First Name Middle Name * Last Name

Suffix

* Street Address Additional Address Information

* City * State/Province * ZIP/Postal Code

* Country

* Personal Phone Number Full Social Security Number * Date of Birth

☐ * "CMS is highly aware of the privacy concerns around disclosure of your personal data including your Social Security Number. CMS is collecting the Personally Identifiable Information (PII) on this screen and on the identity question screen to verify your identity only. Your information will be disclosed to Experian, an external authentication service provider to help us verify your identity. Your Social Security Number will be masked and encrypted during this transaction to assure it is secure. Other than your name, none of the PII data collected in this process is retained."

CANCEL SUBMIT

- Enter your personal information in all the required fields (those marked with a red asterisk).

Notes:

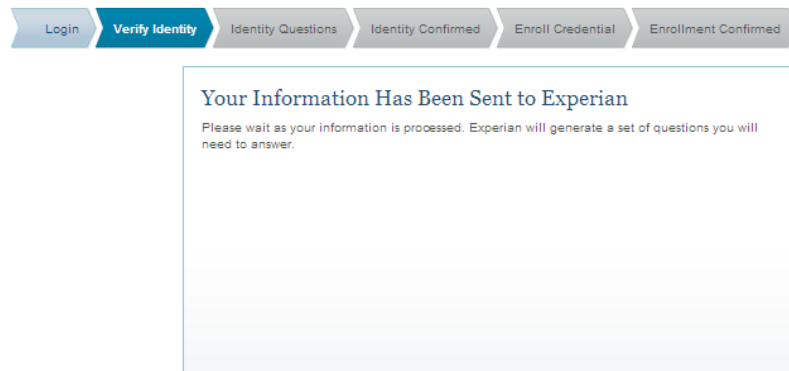
There is a link in the left column of this page for **Remote Proofing FAQs** in the left column on the screen. Access this link if you have questions or concerns about the proofing process.

Although not marked with a red asterisk, the **Social Security Number** must be entered for all users except those from Canada. If you are entering your country as Canada, you cannot complete online identity proofing; **you must complete this process in person with your Security Administrator**.

In the **Full Social Security Number** field, enter your Social Security Number. Hatch marks (###) will mask the number from view after you tab to the next field.

- Next, place a checkmark in the checkbox at the bottom of the page that advises how CMS protects personal data.
- Click **SUBMIT**. The following acknowledgement page appears (see Figure 5-5):

Figure 5-5. Identity Information Submittal Acknowledgement



You will continue to see this screen until Experian is able to either send you identity questions (success), or will provide an informative error message that gives you alternatives for completing the proofing process.

If you are offered an alternative method for proofing, you will be asked to either call the Experian service directly via a toll-free number or you will be directed to meet with your Security Administrator to prove your identity in-person.

10. Next, a series of four identity questions appear (see Figure 5-6). These questions are specific to your credit history and will ask you for details about purchases you have made or other facts Experian would have in their financial databases. The intent of these questions are that they ask you information only *you* should know, thus if you answer them correctly, you have “proven” your identity. For technical detail on the identity proofing process, please visit the Experian [PreciseID website](http://www.experian.com/whitepapers/precise_id_whitepaper.pdf), http://www.experian.com/whitepapers/precise_id_whitepaper.pdf

Figure 5-6. Identity Challenge Questions

CMS.gov | **QualityNet**
Centers for Medicare & Medicaid Services

Login Verify Identity **Identity Questions** Identity Confirmed Enroll Credential Enrollment Confirmed

Identity Challenge Questions from Experian

On this screen you will find four (4) questions about yourself. All questions must be answered.

Please answer the following questions and click Submit when you are finished.

VeriSign Secure Site
click to verify

Identity Challenge Questions * Required Field

*1. You may have opened an auto loan or auto lease in or around September 2012. 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
- ☐ \$395 - \$494
- ☐ \$495 - \$594
- ☐ \$595 - \$694
- ☐ NONE OF THE ABOVE/DOES NOT APPLY

*2. Please select the number of bedrooms in your home from the following choices. If the number of bedrooms in your home is not one of the choices please select 'NONE OF THE ABOVE'.

- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5
- ☐ NONE OF THE ABOVE

*3. According to our records, you currently own, or have owned within the past year, one of the following vehicles. Please select the vehicle that you purchased or leased prior to April 2009 from the following choices.

- ☐ AUDI ALLROAD
- ☐ MAZDA B SERIES PICKUP
- ☐ FORD F100 PICKUP
- ☐ SUBARU BRAT
- ☐ NONE OF THE ABOVE

*4. Which of the following is the highest level of education you have completed? If there is not a matched educational level, please select 'NONE OF THE ABOVE'.

- ☐ HIGH SCHOOL DIPLOMA
- ☐ SOME COLLEGE
- ☐ BACHELOR DEGREE
- ☐ GRADUATE DEGREE
- ☐ NONE OF THE ABOVE

Click the radio button next to the correct answer for each question, then click **SUBMIT** when you have answered all of the questions. The following screen appears (see Figure 5-7):

Figure 5-7. Successful CMS Identity Proofing

The screenshot shows the CMS.gov QualityNet portal with a progress bar at the top indicating the steps: Login, Verify Identity, Identity Questions, Identity Confirmed (highlighted), Enroll Credential, and Enrollment Confirmed. The main content area displays the message "You Have Successfully Completed CMS Identity Proofing" with an icon of a magnifying glass over a document and a large green checkmark. Below this, it says "Thank you for confirming your identity. You are now ready to enroll your two-factor credential ID with QualityNet portal. Please click Continue." and a "CONTINUE" button. The footer includes "QualityNet Home", "CMS.gov", "QualityNet", and a small disclaimer about the federal government website.

11. Click **Continue**. The Enroll Two Factor Credential page appears (see Figure 5-8):

Figure 5-8. Enroll Two-Factor Credential Entry Page

The screenshot shows the CMS.gov QualityNet portal with a progress bar at the top indicating the steps: Login, Verify Identity, Identity Questions, Identity Confirmed, Enroll Credential (highlighted), and Enrollment Confirmed. The main content area is divided into two sections. On the left, a box titled "Enroll Your Two-Factor Credential With QualityNet" provides instructions: "Please enter the two-factor credential ID you downloaded to your computer or phone, and your Symantec VIP Security Code. Click Submit to enroll your two-factor credential with QualityNet." Below this is a "Help" section with a "VIP Access" image showing a sample two-factor credential ID "VSMT0080889" and a security code "082263". On the right, a form titled "Enroll Your Credential *Required" contains fields for "Account ID" (pre-filled with "kj6207"), "* Credential ID", and "* Security Code", followed by a "SUBMIT" button. The footer includes "QualityNet Home", "CMS.gov", "QualityNet", and a small disclaimer about the federal government website.

12. Please ensure that you have your Symantec VIP application available and running. It can be on the PC you are using, on a tablet, or on a smartphone.
13. Type your Symantec VIP Credential ID (the static blue number on the application screen), and a fresh security code, and then click **SUBMIT**. A fresh security code is one that has not expired. Each security code presented on the application screen is valid for 30 seconds. A timer appears above the field with the security code. It counts down from 30 seconds to zero. Once the timer is under 10 seconds, you might want to wait for the next code to appear (unless you are a very fast typist!)

Upon submission of a fresh security code, the following screen appears (see Figure 5-9):

Figure 5-9. Successful Two-Factor Enrollment Screen



14. You can now enroll an additional credential for your User ID, log in to the QualityNet Portal System, or exit.

Note: You are able to enroll up to five credentials for use with your QualityNet ID. You might have one on a work PC, one on a smartphone, and one for use at home if you do any work with QualityNet at home. You have the option now to enroll the additional credentials now or you can do so later from within the Portal (see Section 5.4.4.1).

Table 5-1. Online Proofing Errors and Required User Action

Issue	On-Screen Message	User Action	Security Administrator Action
Your identity cannot be verified via online authentication.	<p>REFERENCE ID</p> <p>Experian is unable to verify your identity using the remote proofing service.</p> <p>Please write down the reference number provided above and phone Experian's support center at (855)339-7880 to complete identity proofing over the phone.</p>	Contact Experian Verifications Support Services at the support center number provided in the error message; give the Customer Service Representative the Reference ID received in the error message and continue the proofing process via a phone process with Customer Service.	Not applicable
You have entered Canada as your country of residence.	<p>Experian is unable to verify the identity of individuals who reside in Canada.</p> <p>Because you live in Canada, you will be required to complete an in-person identity verification process. Please contact the QualityNet Help Desk or your Security Administrator for more information.</p>	Contact your Security Administrator to complete the proofing process.	Complete the proofing process with the user in question, using the In-Person Proofing application within the Secure QualityNet Portal (Section 5.4.4.2).

Issue	On-Screen Message	User Action	Security Administrator Action
Identity questions cannot be generated for you	<p>REFERENCE ID</p> <p>Experian is unable to generate Identity Challenge Questions to verify your identity using the remote proofing service.</p> <p>Please write down the reference number provided above and phone Experian's support center at (855)339-7880 to complete identity proofing over the phone.</p>	<p>Contact Experian Verification Support Service at the support center number provided in the error message; give the Customer Service Representative the reference ID received in the error message and continue the proofing process via a phone process with Customer Service.</p>	Not applicable
	<p>Experian has indicated that you did not complete the phone proofing session with them successfully. To complete proofing, you will be required to complete an in-person identity verification process. Please contact the QualityNet Help Desk or your Security Administrator for more information.</p>	<p>Contact your Security Administrator to complete the proofing process.</p>	<p>Complete the proofing process with the user in question, using the In-Person Proofing application within Secure QualityNet Portal (Section 5.4.4.2) .</p>

Issue	On-Screen Message	User Action	Security Administrator Action
Depending on the error encountered, the associated error message will be displayed along with text that provides a description of the error	There was a problem with your entries on the previous page. To correct the errors and resubmit, click Previous.	Click the PREVIOUS button. Do not use the back button on the browser.	Not applicable

5.3 Logging In to Secure QualityNet Portal

Note: To log in to the Secure QualityNet Portal, you must have a QualityNet user ID and password provisioned by your Security Administrator, and you must complete the New User Enrollment Process that includes identity proofing and multifactor credential enrollment. Please turn to Section 5.2 if you still need to prove your identity and enroll your credential.

To log in:

1. Open your choice of Internet Browser (such as Internet Explorer).
2. Enter the [QualityNet](https://www.qualitynet.org/) web site address into your internet browser's web site address field: <https://www.qualitynet.org/>.
3. The QualityNet Home page appears, with a LOGIN link at the upper-right corner of the page (see Figure 5-10).

Figure 5-10. QualityNet Home Page-LOGIN button



4. Click **LOGIN**. The Destination Page appears (see Figure 5-11).

Figure 5-11. QualityNet Destination Page

Choose Your QualityNet Destination

QualityNet systems and applications are in the process of being consolidated. During this time of transition, please select your primary quality program to reach the right log in screen for your QualityNet portal.

Select your primary quality program:

- End Stage Renal Disease Quality Reporting Program
- Ambulatory Surgical Center Quality Reporting Program
- PPS-Exempt Cancer Hospital Quality Reporting Program
- Inpatient Hospital Quality Reporting Program
- Inpatient Psychiatric Quality Reporting Program
- Outpatient Hospital Quality Reporting Program
- Physicians Quality Reporting System / eRx
- Quality Improvement Organizations

Help
Need to register for a QualityNet account?

- The Destination page provides links to all QualityNet systems and applications. The ASCQR Program link leads to the Secure QualityNet Portal login page, shown in Figure 5-12.

Figure 5-12. QualityNet Login Page

CMS.gov | QualityNet
Centers for Medicare & Medicaid Services

Log In to QualityNet *Required Field

Please enter your CMS User ID and password, followed by your Symantec VIP Security Code, then click Submit.

*User ID

*Password

*Security Code

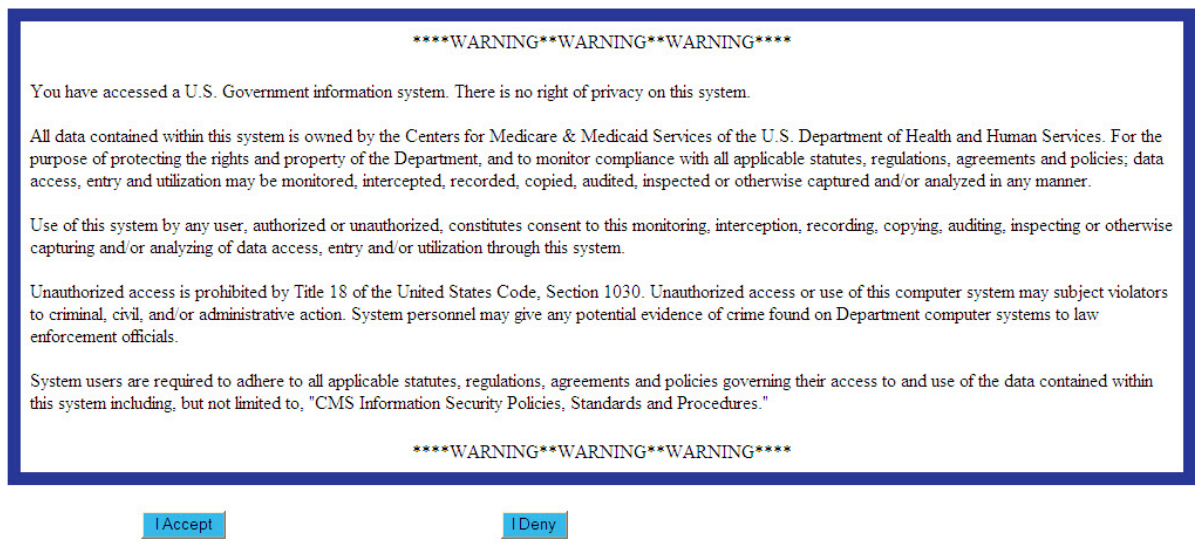
Help
Start/Complete New User Enrollment
Forgot your password?
Trouble with your Security Code?
Need to register for a QualityNet account?

CMS.gov | QualityNet
A federal government website managed by the Centers for Medicare & Medicaid Services
7500 Security Boulevard, Baltimore, MD 21244

- Type your User ID, Password, and Security Code (accessible via the Verisign web site or mobile phone application) and click **SUBMIT**.

The following Warning page appears, advising you that you have accessed a U.S. Government system. Click **I Accept** to continue. Click **I Deny** if you choose not to accept the displayed terms and conditions (see Figure 5-13).

Figure 5-13. CMS Warning Page



You arrive on the Secure QualityNet Portal Landing/Home Page, as shown in Figure 5-14.

Figure 5-14. Secure QualityNet Portal Landing/Home Page



Upon a successful login, users can access the landing page.

5.3.1 Security Error Messages and Required User Action

The following table displays security error messages along with their accompanying user actions:

Table 5-2. Security Error Messages and Required User Action

Issue	On-Screen Message	User Action	Security Administrator Action
Unable to sign in to My QualityNet	JavaScript is Required to Access QualityNet. To enable JavaScript, follow these instructions: (displayed instructions)	Follow the displayed instructions to enable JavaScript	Not applicable
Unable to sign in to My QualityNet	This site requires the ability to open pop-up windows for communication. Please disable your pop-up blocker and reload this page	Click OK to close the message. Enable pop-ups for qualitynet.org and retry signing in	Not applicable
Unable to sign in to My QualityNet and answer the new security questions or create new password	Please contact your organization's QualityNet Security Administrator to request a temporary password	Contact your organization's QualityNet Security Administrator (SA)	Access Edit Users and complete Reset Password for Selected User
Unable to sign in to My QualityNet	User ID or Password is incorrect. Check for accuracy and re-enter your User ID and Password	Re-enter your User ID and Password	Not applicable

Issue	On-Screen Message	User Action	Security Administrator Action
Unable to sign in to My QualityNet (has previously signed-in successfully to the new QualityNet)	Your account has been temporarily locked because multiple attempts to sign in were unsuccessful. Click the 'Forgot your Password?' link to continue	Access and complete Forgot My Password, located on the Sign-In page for My QualityNet	Not applicable
Unable to successfully use the "Forgot My Password" feature	Your account has been locked. Please contact your organization's QualityNet Security Administrator to unlock your account	Contact your organization's QualityNet Security Administrator	Access Edit Users and complete Reset Password for Selected User
Unable to sign in to My QualityNet	Your account is in pending status. It must be approved by your Security Administrator before you will be allowed to sign in	Complete registration paperwork. Contact your organization's QualityNet Security Administrator with questions on the pending status	Send completed registration paperwork to the QualityNet Help Desk if not already done. If the account is pended for other reasons, access Approve User and approve the account.
Unable to sign in to My QualityNet	Your account has been locked due to invalid user status. Contact the QualityNet Help Desk at 1-(866)-288-8912 for assistance	Contact your organization's QualityNet Security Administrator	SA contacts the QualityNet Help Desk (Potential security issue or deactivated account after > 120 days of non-use)

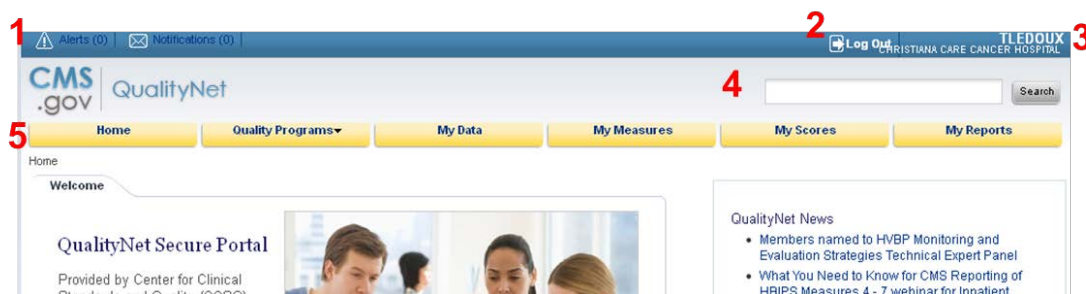
Issue	On-Screen Message	User Action	Security Administrator Action
Unable to sign in to My QualityNet	Account for user: “name” is not activated. Please contact your QualityNet Security Administrator	Contact your organization’s QualityNet Security Administrator	SA contacts the QualityNet Help Desk
Unable to sign in to My QualityNet	Your account could not be accessed because it contains multiple token records. Contact the QualityNet Help Desk at 1-(866)-288-8912 for assistance	Contact your organization’s QualityNet Security Administrator	SA contacts the QualityNet Help Desk

5.4 Navigating the Secure QualityNet Portal

The Secure QualityNet Portal Landing/Home Page has the following functionality:

5.4.1 Header

Figure 5-15. Header Section of the Secure QualityNet Portal Landing/Home Page



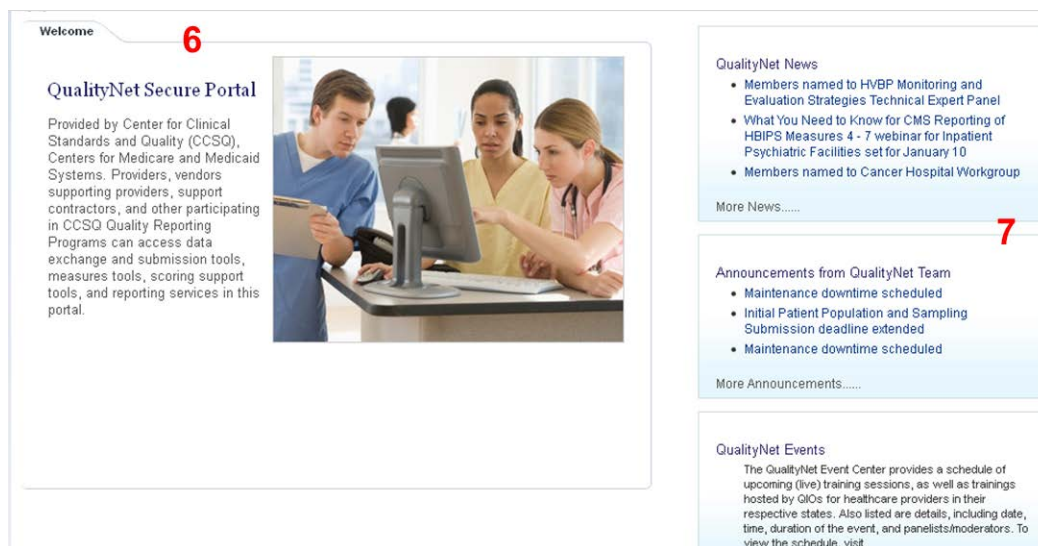
1. **Alerts and Notifications** are noted in the header ribbon—these are messages from applications to which a user has access. For example, a user might see a notification that a report s/he ran is ready to view, or an alert that s/he is approaching the deadline to confirm participation in a Quality Reporting program.
2. The **Log Out** link/button enables you to exit the Portal.
3. The **User’s Name and Organization** information confirms who is logged in for this particular portal session.

4. The **Search** feature enables you to search for information available on the QualityNet.org information website, such as Specification Manuals.
5. The **Global Navigation Menu** enables you to access specific sections of the portal offering reporting, measures, data, scoring, and Quality Reporting program functionality. **Important:** There is no File Exchange capability within the portal. Security Administrators are able to access the QualityNet System File Exchange applications and can securely exchange files for users if this capability is required.

5.4.2 Content Window

The Content window contains the following information:

Figure 5-16. Content Window



1. The **Welcome** area presents information for users who are new to the portal.
2. **News, announcements, and events** from the QualityNet team appear on the right side of the page. A link to QualityNet training events (live and recorded WebEx events) also appears here.

5.4.3 Footer

Figure 5-17: Footer



1. The **QualityNet Home** button takes users back to the portal's landing page from any location.
2. **QualityNet Helpful Links** list the standard footer links including QualityNet contact information, the About QualityNet statement, the QualityNet Accessibility Statement, QualityNet Privacy Policy, and QualityNet Terms of Use, all of which open in a separate browser tab when clicked.
3. **QualityNet Help** links to QualityNet help documents, including a link to this user guide and other QualityNet training materials. The **FAQs** link opens a new browser tab that leads to the CMS Q&A tool for Quality Reporting Program questions and answers provided by Quality Reporting support contractors.
4. **CMS Sites** provides links to the QualityNet.org information web site and the www.cms.gov web site.
5. The **Adobe Acrobat Reader** link provides a direct path to download Adobe's Acrobat Reader application.

5.4.4 Managing Security in the Secure QualityNet Portal

All Secure QualityNet Portal users are able to add and remove multifactor credentials.

In addition, Security Administrators are able to perform in-person proofing of user identity. Other security tasks that Security Administrators may need to do, such as manage users (create, update, or delete their accounts) or help users reset passwords, must be done in the QualityNet System. See the details below.

5.4.4.1 Managing Multifactor Credentials

1. Navigate to the **Quality Programs** tab and click **Hospital Quality Reporting Programs**.
2. The **My Tasks** page appears. Click **Manage Multifactor Credential**. The **Add/Remove Credential** screen appears.

To add a credential, proceed to step 3. To remove a credential, proceed to step 4.

3. To add a credential:

Have the new Symantec VIP application open and running.

Enter the static (blue) credential ID, then enter a fresh security code and click **ADD CREDENTIAL**.

A confirmation appears, stating that your user ID is now linked to the new credential. You can link up to five credentials to a single user ID.

4. To remove a credential:

Enter the credential ID of the Symantec VIP application that you want to unlink from your user ID.

Enter a fresh security code and click **REMOVE CREDENTIAL**.

A confirmation appears, stating that this credential is no longer linked to your user ID.

Note: if you lose a credential (if your phone is stolen, for example), please call the QualityNet Help Desk to report the lost credential. You cannot remove a credential unless you can access the VIP application and record both the credential ID and a valid security code.

5.4.4.2 In-Person Proofing

Important: In order to complete this procedure, the individual who requires in-person proofing must be physically present in the room with the Security Administrator.

Security Administrators who perform in-person proofing of users who could not complete the online proofing process will use the In-Person Proofing application to record the user's identity credentials. The application also records the Security Administrator's proofing decision (approves, rejects, or cancels).

1. Navigate to the **Quality Programs** tab and click **Hospital Quality Reporting Programs**.
2. The **My Tasks** page appears. Click **In-Person Proofing**. The following screen appears:

Figure 5-18. In Person Proofing Screen-Account ID Entry

The screenshot displays the 'In Person Proofing' interface. At the top, there is a navigation bar with tabs: Home, Quality Programs (selected), My Data, My Measures, My Scores, and My Reports. Below the navigation bar, the breadcrumb trail reads: Quality Programs > Hospital Reporting Quality System > Manage Security > In-Person Proofing. The main content area is divided into two sections. On the left, under the heading 'Instruction', there is a text box containing instructions: 'Please review and select the type of identification used for proofing the individual below and take appropriate action. If there are issues with the identification materials provided (i.e., an expired license or passport), you may choose to cancel this request and complete at the appropriate time. This is a choice to use instead of reject to give the user the ability to return with appropriate and correct identification materials.' On the right, under the heading 'In Person Proofing', there is a form with a label '* Account ID' and a text input field. To the right of the input field is a blue 'Search' button. Above the input field, there are two lines of text: '* Required field, if approved' and '** Required field, if rejected'.

3. Enter the user ID for the individual who needs to prove his/her identity to you and click **Search**. The following screen appears:

Figure 5-19. In Person Proofing Screen – Verification of ID Type

The screenshot displays the 'In Person Proofing' interface. On the left, an 'Instructions' box explains the process and includes the Experian logo and a 'Verified Secure Site' badge. The main section, titled 'In Person Proofing', contains a search bar for 'Account ID' with a 'SEARCH' button. Below this, there are dropdown menus for 'Photo Identification', 'Address Confirmation', and 'Date of Birth Confirmation'. A checkbox for 'I affirm that the individual has appeared in person...' is present. At the bottom, there is a 'Reason for Rejection' dropdown, a 'Comments' text area, and three buttons: 'CANCEL', 'REJECT', and 'APPROVE'.

4. You are asked to record the authenticity of and type of ID used to confirm the user's identity. Choose the correct documents the user presented to you for each documentation type.
5. Place a checkmark in the Confirmation checkbox.
6. If the user brings incorrect documentation, do not **REJECT** the request, instead **CANCEL** it. This allows the request to be opened again when the user can produce the right documentation.
7. Click the button that confirms your decision (**Approve**, **Cancel**, or **Reject**). If you reject the user, you must explain why in the **Comments** field provided.

5.4.4.3 Creating, Updating, and Removing Users

See Section 7.4 for detailed instructions on creating, updating, and removing users. Security Administrators must log into MyQualityNet (IQR or OQR) to access the Security applications to manage users.

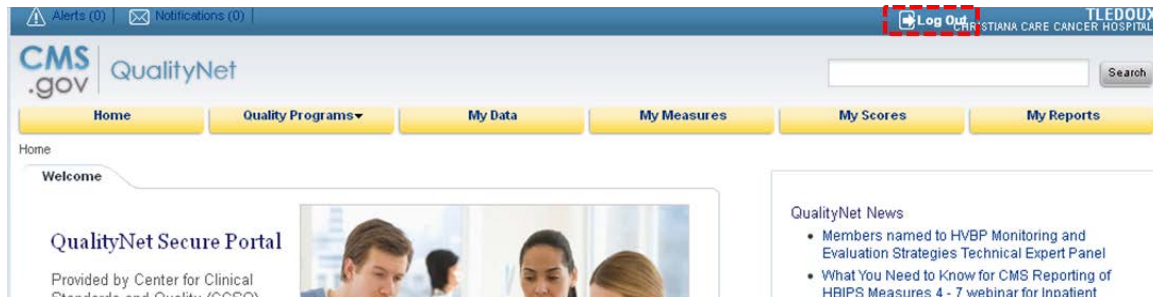
5.4.4.4 Assisting Users with Password Resets

See Section 7.4.2 for detailed instructions on resetting passwords. Security Administrators must log into My QualityNet (IQR or OQR) to access the Security applications to manage users.

5.4.5 Logging Out of Secure QualityNet Portal

The **Log Out** link is located on the Portal screen's blue ribbon, in the upper- right corner (see Figure 5-20).

Figure 5-20. Log Out Link Location



Click **Log Out** to exit the portal. A dialog box appears, asking you to confirm that you want to exit. When you click **Yes**, you will return to <https://www.qualitynet.org> and your portal session will be terminated.