

**SUPPORTING STATEMENT  
FOR THE PAPERWORK REDUCTION ACT SUBMISSION  
QualityNet Identity Management System (QIMS) Account Form  
(CMS-10267)**

A. Background

The Office of Clinical Standards and Quality (OCSQ) is replacing two legacy applications that collect information for the CMS-2728 End Stage Renal Disease Medical Evidence Report Medicare Entitlement and/or Patient Registration (OMB No. 0938-0046) and the CMS-2746 ESRD Death Notification (OMB No. 0938-0448). The new system, replacing these two legacy applications, is known as the “Consolidated Renal Operations in a Web Enabled Network (CROWNWeb).” CROWNWeb is the system that is mandated for the Final Rule published April 15, 2008, with the title “Medicare and Medicaid Programs Conditions for Coverage for End-Stage Renal Disease Facilities.” Due to the sensitivity of the data available in CROWNWeb, CMS must ensure that only authorized dialysis facility and ESRD Network Organization personnel have access to CROWNWeb data and that only data pertaining to their own patients is available to facility personnel. The CMS Chief Information Officer (CIO) has mandated that a multifactor authentication system be used in the creation of CROWNWeb accounts. The QualityNet Identity Management System (QIMS) will be that system used in the creating and maintaining of CROWNWeb user accounts.

QIMS will use form CMS-10267 which is a currently approved collection due to expire in Mary 2011. Due to the need to incorporate the multifactor registration, the form is being slightly modified. Part A (page 1 and 2) of the form will collect data for user registration and Part B (page 3) will collect CROWNWeb roles and scope.

B. Justification

1. Need and Legal Basis

The need and legal basis information provided by the CMS Information Security Officer (ISSO) is listed below. Since the QIMS account form is for the collection of personally identifiable information and the assignment of CROWNWeb system privileges, the web pages referenced below govern User Identification (need for, creation of, care of, handling of, preservation, authentication, storage, association, and authorization).

[http://www.cms.hhs.gov/InformationSecurity/12\\_Laws\\_Regs.asp](http://www.cms.hhs.gov/InformationSecurity/12_Laws_Regs.asp)  
<http://csrc.nist.gov/publications/PubsFIPS.html> (particularly FIPS 198, 199 AND 201-1)  
<http://csrc.nist.gov/publications/PubsSPs.html> (particular SP 800-53 Rev 2)  
<http://csrc.nist.gov/publications/PubsByLR.html> (SP 800-63 V1.0.2)

2. Information Users

The QualityNet Identity Management System (QIMS) account registration form must be completed by any new persons needing access to CROWNWeb. The 8,561 existing accounts owners will not have to reregister for new user accounts. The CROWNWeb user community is composed of CMS employees, ESRD Network Organization staff and dialysis facilities staff. The CROWNWeb system is the system used as the collection point of data necessary for entitlement of ESRD patients to Medicare benefits and Federal Government monitoring and assessing of quality and type of care provided to renal patients. The data collected in QIMS will provide the necessary security measures for creating and maintaining active CROWNWeb user accounts and collection of audit trail information required by the CMS Information Security Officers (ISSO). The total active QIMS accounts for CROWNWeb are expected to reach 16,000.

### 3. Use of Information Technology

The QIMS system will allow the creation and maintenance of active CROWNWeb user accounts to be improved greatly because the system allows the security officials governing these user accounts to be closer to their public. There is also a separation of duty to ensure security measures are met. CMS approves ESRD networks and network's approve facilities that they monitor. An approved facility and network manager must approve the applicant's request by signing their access form, the applicant's identity must also be verified and anyone requesting the role of a QIMS security official (SO) must also have their form notarized by a Notary Public. The QIMS system has been enhanced from the original QualityNet Identity Provisioning System (QIPS) to remove the data entry burden from the SO by allowing the applicant to complete their form on-line and enhanced to include second factor authentication as mandated by the CMS Chief Information Officer (CIO). Because this process is automated and handled in a web based system, the automation of this process has made it quicker. Also, account violations will be able to be identified and dealt with quicker, thus improving system security. Annual recertification processes and additional security features required by the CMS ISSO have also been incorporated.

- Since the digital signatures are not available in the QIMS system, the form must be completed and signed by the applicant, signed/approved by their manager, vetted by the SO and notarized (SO account forms only need notarization). The form must be kept on file by the Identity Management Service team once the account is activated.

### 4. Duplication of Similar Information

Since the QIMS account form not only collects applicant information but roles and access specific to the CROWNWeb system, there is no other form in place or system available to collect this information. Also, the user community of the CROWNWeb application, specifically the ESRD networks and dialysis facilities are specific to CROWNWeb so their personal information is not available in other CMS identity management systems.

### 5. Small Businesses

A small business would be described as a provider that is not a member of a chain organization and/or has a small dialysis patient population. These providers are legislatively required to maintain the same patient information and to report on this information in the same manner as all other providers of renal services. The ESRD networks will enter the accounts for smaller facilities that do not have the staff size to handle the separation of duties or the data entry burden. Also, limited and approved CMS contractor staff has access rights to assist in the Security Official's data entry burden should assistance be requested and authorization be provided by the ESRD Networks or dialysis facilities.

#### 6. Less Frequent Collection

Due to the sensitivity of the data within CROWNWeb, the QIMS Account form must be collected in order to ensure that only authorized dialysis facility and ESRD Network Organization personnel have access to CROWNWeb data and that only data pertaining to their own patients is available to facility personnel.

#### 7. Special Circumstances

- The recertification process is only performed annually. As QIMS is expanded to support other applications/systems, the same user ID can obtain access to additional applications/systems provided that the appropriate approvals have been granted.
- There is no written response necessary in fewer than 30 days. The form, when completed, approved, vetted and notarized (only SO account forms require notarization) creates the user account.
- Only the original/signed copy of the QIMS form is required and kept by one entity.
- The identity management team has the responsibility of activating the user account.
- The form is required to be retained for 7 years.
- The form has no connection to a statistical survey.
- There are no requirements for statistical data classification.
- Since the data collected on the QIMS form contains personally identifiable information, confidentiality rules apply. We are following all the regulations mandated by the CMS Information System Security Officer (ISSO) and the CMS Chief Information Officer (CIO).
- No trade secrets or confidential information is involved in this process.

#### 8. Federal Register Notice/Outside Consultation

The 60-day Federal Register notice published on July 12, 2010.

The QIMS account form is required for identity and security management of individuals accessing the "Consolidated Renal Operations in a Web Enabled Network (CROWNWeb) system". CROWNWeb is the system that is mandated for the Final Rule published April 15, 2008, with the title "Medicare and Medicaid Programs Conditions for Coverage for End-

Stage Renal Disease Facilities.”

9. Payment/Gifts to Respondents

No payments or gifts are made to respondents.

10. Confidentiality

A confidentiality statement is provided on the QIMS account form as it related to the Privacy Act regulations.

11. Sensitive Questions

Personally identifiable information is requested on the QIMS account form. The information collected on the QIMS account form includes (asterisk denotes required fields):

Type of Request

- \*Type of Account Creation
- \*Date Requested
- \*QIMS User ID for change/disable/enable

Personnel Information

- Prefix
- \*First Name
- Middle Initial
- \*Last Name
- Suffix
- \*Personal Address
- \*Birthdate
- Cell Phone
- \*Business Phone & Extension
- \*Business E-mail Address or Personal E-mail Address
- \*Identification Used
- \*ID Number
- \*Issued By
- \*Expiration Date

Business Information

- \*Business Name
- \*Job Title
- Fax Number
- \*Business Address
- \*Approving Manager’s Name
- \*Manager’s Email Address
- \*Manager’s Job Title

- o \*Manager's Phone Number
- Signatures/Dates
- o Applicant Signature and Date
  - o Manager's Signature and Date
  - o Security Official's Signature and Date
  - o Notary's Signature and Date
- 2<sup>nd</sup> Factor/Application Access
- o Application(s) to be accessed Checkbox
  - o 2<sup>nd</sup> Factor Credential Checkbox
  - o 2<sup>nd</sup> Factor Contact
- CROWNWeb Access
- o \*System Access Required for the Applicant's Job Role

12. Burden Estimates (Total Hours & Wages and Postage Fees)

As of May 12, 2010, a total of 8,561 QIMS/CROWNWeb user accounts exist, of which 5,938 are Security Officer (SO) Accounts. In the next year, CROWNWeb will be rolled out nationally and there is an expected growth of an additional 7,439 accounts (total 16,000 accounts) that first year. The existing accounts will be grandfathered in so new account creation is not required. Also, since all SO accounts have been created, it is anticipated that all new accounts will be mainly general users; therefore, the notarization burden will be minimal. Because of the number of new accounts that will be created the first year, the burden estimate is broken down into two parts – year 1 and subsequent year(s). A figure of 1,600 (10% of 16,000 total) is used for the subsequent years to account for personnel changes; however, the total CROWNWeb user population is expected to remain at 16,000.

Estimated Hourly Wage: \$36.82 is the hourly rate for RN staff as obtained from the Bureau of Labor statistics web site (<http://stats.bls.gov>) on May 12, 2010. (\$76,570 divided by 2080 hours = \$36.82)

Average time to complete account registration process (breakdown below): 30 minutes

- o 10 minutes to complete, print and sign form
- o 5 minutes to obtain management approval signature
- o 5 minutes for QIMS Security Officer to verify and sign form
- o 5 minutes to get form notarized (only required for Security Officer Account forms)
- o 5 minutes to fax form to Identity Management Service team

**First Year: Estimated registration costs = \$136,951.99**

- (7,439 CROWNWeb users x \$36.82) x.5)

**Subsequent Years: Estimated registration costs = \$29,456**

- (1,600 CROWNWeb users x \$36.82) x.5)
- Note – 1,600 is 10% of total expected CROWNWeb Users (16,000)

Training - Annual Security Awareness Power Point Training: 60 minutes (1 hour)

**First Year: \$589,120 (16,000 total users x \$36.82)**

**Subsequent Years: \$589,120 (16,000 total users x \$36.82)**

Annual Mailing cost: Individual account forms can be mailed using first class postage (\$0.44); otherwise, if more than 1 form is mailed together there is a security requirement in place that the forms must be mailed USPS Certified/Return Receipt at an approximate cost of \$5.55 (www.usps.com). Due to the feedback from the pilot that went live November 2008, it is expected that the mailings will be individual mailings and not bulk mailings. The Security Officials (SO) found that the bulk mailing deliveries took longer and were inconvenient because of the travel required to the post office.

**First Year: Estimated mailing costs = \$3,273.16 (7,439 forms x .44)**

**Subsequent Years: Estimated mailing costs = \$704 (1,600 forms x .44)**

- Note – 1,600 is 10% of total expected CROWNWeb Users (16,000)

Year 1 Burden =

- New Accounts: 7,439
- Registration Process (7,439): \$136,951.99
- Training (16,000 total users): \$589,120
- Mailing Costs (7,439 individual forms): \$3,273.16
- Total Cost: **\$729,345.15**

Subsequent Year(s) Burden =

- New Accounts: 1,600
- Registration Process (1,600): \$29,456
- Training (16,000 total users): \$589,120
- Mailing Costs (1,600 individual forms): \$704
- Total Cost: **\$619,280**

### 13. Capital Costs

No capital costs are expected since the data entry collection system is a web based system. QIMS account applicants, managers, security officers, and help desk staff only need a computer that has internet access.

### 14. Cost to the Federal Government

The expected annual cost to the Federal Government to cover the expense of the help desk facility and the identity management service team to activate and maintain 16,000 QIMS account forms and to provide CMS requested audit reporting will cost approximately \$500,000. These services will be contracted out.

15. Changes to Burden

The cost of the first year is expected to be much higher than the subsequent years because it includes the creation of an additional 7,439 user accounts. The yearly account creation for subsequent years is expected to be 1,600 forms (10%) due to personnel changes. Since the total CROWNWeb user population is expected to remain at 16,000, the maintenance cost to the Federal Government is to remain approximately at \$500,000.

16. Publication and Tabulation Dates

The information collected on the QIMS Account Form (Part B) is used solely for the creation and maintenance of CROWNWeb user accounts.

17. Expiration Date

CMS would like an exemption from displaying the expiration date as these forms are used on a continuing basis. To include an expiration date would result in having to discard a potentially large number of forms.

18. Certification Statement

There are no exceptions to the certification statement.