DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Office of Clinical Standards and Quality
Information Systems Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

QualityNet
Security Point of Contact
Procedures

Version 2.5

March
2019

Prepared by:
Ventech Solutions

Document Tracking/Updates

Date	Version	Description	Page, Section(s) Affected
11/2010	0.1	Initial document creation.	Entire Document
11/2010	0.2	First copy revised and additional sections added.	Entire Document
01/12/2015	0.3	Update for current SOW structures	Entire Document
02/01/2016	2.0	Updated entire SPOC onboarding process	Entire Document
02/29/2016	2.1	Updated SPOC distribution list names	Page 9
03/11/2016	2.2	Performed draft review	Entire Document
03/15/2016	2.3	Completed updates based on CMS feedback	Entire Document
04/11/2016	2.4	Updated Submitter/Certifier fields in Appointment Form	Appendix B
03/1/2019	2.5	Performed draft review and updated Appointment Form	Entire Document

TABLE OF CONTENTS

INTRODUCTION

The Centers for Medicare & Medicaid Services (CMS), Center for Clinical Standards and Quality (CCSQ), Information Systems Group (ISG) is responsible for implementing and administering an information security program to protect its Healthcare Quality Information System's (HCQIS) infrastructure also known as QualityNet (QNet) and its information resources, in compliance with applicable public laws, Federal regulations, and Executive Orders including the Federal Information Security Management Act of 2002 (FISMA); the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, dated November 28, 2000; and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

These procedures establish uniform guidelines and security best practices for protecting and controlling Information Technology (IT) resources, directly or indirectly related to QNet activities.

PURPOSE & SCOPE

This document serves to outline processes and procedures associated with the selection and appointment of a Security Point of Contact (SPOC), the removal of a SPOC from an organization, the roles and responsibilities of a SPOC, SPOC training, and locations of reference materials available to the SPOC. To ensure compliance with federal laws and QNet procedures, SPOCs should review and become familiar with all material referenced in APPENDIX A. This document does not replace common sense or overrule any existing Federal, State, or Local laws.

RESPONSIBILITIES

CMS Contractors with access to HCQIS systems including the QNet infrastructure are responsible for properly protecting, safeguarding, and disposing of all information used, gathered, or developed as a result of work under the contract. The Contractor shall also protect all Government data, equipment, etc. by treating the necessary information as sensitive.

The SPOC ensures personnel at each of the Contractor's respective location(s) are compliant with security requirements set forth by the QUALITYNET SYSTEM SECURITY POLICY. The SPOC works directly with the CMS ISSOs and/or the QNet infrastructure support security team on all related security deliverables, events, and/or tasks. The SPOC is the central point of contact for all individuals at the local organization regarding security matters. Responsibilities include, but are not limited to:

- Understanding CMS security requirements and policies
- Serving as the primary POC for security incidents at his/her organization/site
- Reporting and handling of security incidents that occur within the organization/site

- Coordinating the destruction of sensitive information in accordance with CMS policy
- Ensuring the integrity of security processes and documentation
- Assisting CMS ISSOs with managing security locally
- Managing and maintaining all Security Awareness Training (SAT) for the contract
- Managing and assuring appropriate FISMA level requirements are being met at the organization

ORGANIZATIONAL SPOC APPOINTMENT

When an organization has been awarded a QNet contract, it is the Chief Executive Officer's (CEO) responsibility, or the highest-ranking organizational representative's (i.e. Program Director) responsibility to assign a SPOC and one Secondary SPOC. The primary SPOC will be responsible for all locations and users within the parent contractor's organization. The secondary SPOC will assume responsibility in the absence of the primary SPOC. A SPOC should be someone with a good understanding of the best security practices, while also possessing the capability to provide sufficient detail during an investigation of a security incident. An individual may be the designated SPOC across multiple contracts that support the HCQIS infrastructure; however, the designating and removal process must remain separate for each contract and deliverable submission. If the above responsibilities are not fulfilled by the Primary and Secondary SPOCs, the SPOC Escalation POC will be required to perform the SPOC responsibilities listed above. The SPOC Escalation POC will be contacted if/when SPOCs are unresponsive or when more severe incidents occur (e.g. Program Manager).

PREREQUISITES TO BECOME A SPOC

Access to various environments and assets play a key role when reporting and investigating security incidents and other events. All SPOCs will require the following accounts in order to perform their specific roles and duties:

- **Internal *.hcqis.org e-mail address** – the HCQIS e-mail address will be utilized for verification and contacts
- **QNet LDAP account** – only organizations with domain account users are required to have a SPOC
- **QNet File Exchange** – QNet SFT (aka Axway) will be utilized for secure exchange of artifacts during security incident handling.
- **ServiceNow access w/proper site code** – ServiceNow access is required for SPOC submission forms and monitoring security incident tickets.
    - Sites codes are established during initial infrastructure onboarding processes by the ServiceNow team. Site codes are predetermined and usually follow format of the contract or site names (ex. *QIO/QIN-xx, ESRD Network-xx, ADO xx*).
    - ServiceNow access may be acquired through the local organizations' Account Administrator (AA).

APPOINTING A NEW SPOC

The organization's highest-ranking official must complete the QUALITYNET SECURITY POINT OF CONTACT APPOINTMENT FORM, located in APPENDIX B, to propose a new SPOC. All required information must be entered into the form; the completed form must then be emailed to the QNet Help Desk with a request to create a ticket, to be assigned to the QNet Infrastructure Security Team.

Note: Any contract vehicle deliverables must continue to be submitted per the COR or statement of deliverables

CHANGING OR REMOVING A SPOC

Should a SPOC leave the organization, or no longer is tasked with performing the SPOC's duties; the QNet Help Desk is to be notified immediately so that a ServiceNow ticket can be created. The ticket should be assigned to the QNet Infrastructure Security Team. A Security Analyst will remove the individual from the SPOC module in ServiceNow and the associated distribution list. All changes to the SPOC Escalation POC must also be submitted immediately to the QNet Help Desk.

Note: A single ticket can be created to update the current SPOC list for an organization.

INCIDENT RESPONSE PROCEDURES

As stated in the QUALITYNET INCIDENT RESPONSE PROCEDURES, SPOCs and local IT support are responsible for receiving any report of a suspected security breach, incident, or violation and ensuring that it is reported to the QNet Help Desk.

Due to the nature and privacy of the information which identifies a security incident, as well as the expediency with which responses must be handled, SPOCs must immediately call the QNet Help Desk and complete the QUALITYNET INCIDENT REPORT FORM, located in APPENDIX B, as part of their reporting suspected incidents procedures. The QUALITYNET INCIDENT REPORT FORM must be sent securely via encrypted email to **securityoperations@hcqis.org** or Secure File Transfer (SFT) to the **Ventech Security** organization.

For each incident on the contract, the SPOC is responsible to:

- Serve as the QNet component functional system's point of contact for security incidents and assist with the triage, response, and recovery phases.
- Prepare facility-level plans and procedures to address system security incidents, in accordance with this document, and the security system standard operating procedures.
- Contact the QNet Help Desk **immediately** to report security incidents, providing all possible supporting documentation in a secure format.
- Submit the QUALITYNET INCIDENT RESPONSE FORM within one (1) business hour of the

initial incident notification given to the QNet Help Desk.

- Respond to any and all inquiries within one (1) business day of the request.
- Capture and securely store all evidence and/or artifacts relating to the incident.
    - These are not to be destroyed until the investigation is completed and explicit written notification has been given by the QNet Infrastructure Security Team.
- File any appropriate police report with local law enforcement.
- Provide technical support and advice for incident handling, impact assessment, and technical system management, including actions to be taken if circumstances are not covered by standard operating procedures.
- Coordinate evaluation and categorization of security advisories and information.
- Refer information to the QNet Help Desk.
- Report incident status and resolution information to management in accordance with this document and the standard operating procedures.
- Assist in information gathering, forensics, and reporting activities.
- Provide ad hoc and periodic reports on security incidents and handling of advisories.

Security incidents should be resolved within one week of the initial notification to the QNet Help Desk. For additional information on Incident Response, please refer to the QUALITYNET INCIDENT RESPONSE PROCEDURES, and to the INCIDENT RESPONSE PROCESS FLOWCHART in APPENDIX C.

APPENDIX A: REFERENCES

POINT OF CONTACTS (POCS)

QNet Infrastructure Security Team – securityoperations@hcqis.org
CMS QNet Information System Security Officers (ISSOs) – cms_qnet_security@cms.hhs.gov

FEDERAL LAWS AND REGULATIONS

Federal Information Security Management Act of 2002 (FISMA) – http://csrc.nist.gov/groups/SMA/fisma/index.html

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf

NIST Special Publications 800 Series – http://csrc.nist.gov/publications/PubsSPs.html

CMS POLICIES & STANDARDS

Information Security & Privacy Library – https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Note: The latest versions of the Acceptable Risk Safeguards (ARS) & other security related documentation can be downloaded from the Information Security & Privacy Library

QNET POLICIES AND PROCEDURES

QIONET

QNet System Security Policy, QNet Incident Response Procedures, & SAT Training Information – https://qionet.sdps.org/training_resources/qnet_security.shtml

ESRD

Additional ESRD Network resources may be found here:

http://esrdnetworks.org/
http://esrdncc.org/

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Office of Clinical Standards and Quality
Information Systems Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

APPENDIX B: QUALITYNET SECURITY POINT OF CONTACT APPOINTMENT FORM

PROCESS/PROCEDURES FOR COMPLETING & SUBMITTING THIS FORM

1. Contact the QNet Help Desk to open a ServiceNow ticket, and provide the completed SPOC Appointment Form to be entered as an attachment. Ensure that all of the following information is placed into the ServiceNow ticket:
    - **Site/Region ID (if applicable):** *Network xx, QIN-x, BFCC-Area/Region x, etc.*
    - **Organization Name:** *XYZ Healthcare*
    - **Contract:** *BFCC-QIO, QIN-QIO, ESRD Network, ADO, Program Support, Infrastructure, etc.*
    - **Name**
    - **HCQIS E-mail Address**
    - **Phone Number**
    - **Primary or Alternate Designation**
2. The QNet Help Desk will create the ServiceNow ticket & assign it to the **QNet Infrastructure Security Team**
3. The **QNet Infrastructure Security Team** will verify that the form is completed accurately with all required data fields. Upon verification, a security team member will add the SPOC into the ServiceNow SPOC Module under the respective organization.
    - **Note:** New organizations that have not previously been added to ServiceNow will be routed to the ServiceNow Team to have a site code created.
4. Once the SPOC is added to the ServiceNow module, the security team will add the SPOC to the respected supporting program email distribution group. The current SPOC distribution list includes:
    - **QIO-SPOC** – *BFCC, QIN, QIO-NCC, VQIRC, etc.*
    - **ESRD-SPOC** – *ESRD Networks, ESRD NCC, etc.*
    - **HCQIS-Support-SPOC** – *Infrastructure, ADO, PMBR, etc.*
    - **Quality-Reporting-SPOC** – *Hospitals, Physicians, & other QNET reporting programs*
    - **HCQIS-Program-SPOC** – *All other supported programs*
5. Once all tasks are complete, the SPOC will receive notification and the ticket will be closed. The SPOC will immediately be placed on all future security communications from CMS and the QNet Infrastructure Security Team.

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Office of Clinical Standards and Quality
Information Systems Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

QualityNet
Security Point of Contact (SPOC)
Appointment Form

Site/Region Identification:	
Organization Name:	
Submitter's Name:	
Submitter's Title:	
Submitter's Phone:	

I appoint the following individuals to serve as this organization's QualityNet Security Point of Contact(s) (SPOCs). This appointment complies with the requirements of the contract SOW and the HCQIS/QNet processes.

I certify that this appointment is in compliance with the CMS Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR), Appendix B, Security Control AC-5, and Separation of Duties.

I acknowledge that I am required to submit a new memo of appointment whenever there is change to any of the data contained herein. I understand that the new memo must be submitted within five calendar days of that change being effective.

Please select the appropriate distribution list for the organization, as it pertains to the requested SPOC appointment *(select one)*:

- ☐ QIO-SPOC (*BFCC, QIN, QIO-NCC, VQIRC, etc.)*
- ☐ ESRD-SPOC (*ESRD Networks, ESRD NCC, etc.)*
- ☐ HCQIS-Support-SPOC (*Infrastructure, ADO, PMBR, etc.)*
- ☐ Quality-Reporting-SPOC (*Hospitals, Physicians, & other QNET reporting programs)*
- ☐ HCQIS-Program-SPOC (*All other supported programs)*

Primary SPOC:	
HCQIS Email Address:	
Office Phone:	
Mobile/Alternate Phone:	
Office Address:	

Secondary SPOC:	
HCQIS Email Address:	
Office Phone:	
Mobile/Alternate Phone:	
Office Address:	

SPOC Escalation POC:	
HCQIS Email Address:	
Office Phone:	
Mobile/Alternate Phone:	
Office Address:	

Certified by:

Printed Name:		Signature:	
Title:		Date:	

NOTE: The "Certifier" cannot be the same individual as the Primary or Secondary SPOC appointees and must be one of the QualityNet contractor's highest-ranking organizational representatives (CEO, Program Director, etc.). The submitter may serve as the certifier, as long as the previous condition has been met. The certifier holds the responsibility and authority to assign the SPOC(s) for the organization and may also serve as the Escalation POC.

APPENDIX C: INCIDENT RESPONSE PROCESS FLOWCHART