Department of Health & Human Services
Centers for Medicare & Medicaid Services
Centers for Clinical Standards and Quality
Information Systems Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

QualityNet
System Security Policy

Version 8.0
May 2013

Revision/Change Record

Date	Version	Description	Page, Section Affected
July 23, 2008	5.0	Updated Versions of ARS, PISP, QIO and ESRD Manuals, and Enterprise Complex Patch Management Policy	All
September 11, 2008	5.0	Added Section on QualityNet Help Desk	4.9.
August 2009	6.0	Update	All
December 2010	6.1	Complete update	All
July 2011	7.0	Significant format and layout changes.	All
May 2013	8.0	- Significant format and layout changes - Email Matrix Appendix B added - Section changes - Media protection section scaled	All

Table of Contents

List of Tables

QualityNet System Security Policy

1. Introduction

The Centers for Medicare and Medicaid Services (CMS), Center for Clinical Standards and Quality (CCSQ), Information Systems Group (ISG) is responsible for implementing and administering information security guidance and an educational awareness program in support of QualityNet. This document establishes the QualityNet Information Security (IS) Program Policy, which aims to reduce the risk and minimize the effect of security incidents by establishing specific procedures under which QualityNet shall operate its information systems.

This policy contains multiple links to other security directives and publications that are pertinent to the implementation and operation of a successful Information Systems Security Program, such as the CMS Information Security Acceptable Risk Safeguards (ARS) and the CMS Policy for the Information Security Program (PISP). All QualityNet users must always adhere to the policies and procedures prescribed within these publications. **Failure to adhere to these policies and/or procedures will result in a security violation occurring on the QualityNet system.**

The QualityNet Information Security Program protects QualityNet information resources in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, the Privacy Act of 1974, the, the Federal Information Security Management Act of 2002 (FISMA), Appendix III to the Office of Management and Budget (OMB) Circular A-130, *Security of Federal Automated Information Resources*, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually identifiable data. Section 5 U.S.C. §552a (e) (10) of the Act is very clear; federal systems must *"...establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."*

The QualityNet System Security Policy provides the foundation for the QualityNet Information Security Program. This Policy includes a broad set of required security standards based upon NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, and NIST 800-63, *Electronic Authentication Guideline*, as well as the CMS Policy for the Information Security Program (PISP), and the CMS Information Security Acceptable Risk Safeguards (ARS). This document expands upon the security controls that must be implemented to protect the QualityNet Enterprise data and infrastructure. These requirements are equally applicable to all QualityNet users, contractors, business partners and stakeholders.

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

Table 1 - ARS Families

A primary responsibility of QualityNet security is to protect Privacy Act data and other sensitive information it collects, produces, stores, transmits and disseminates in the course of conducting its operations. This responsibility forms a covenant with its beneficiaries, personnel, and health care providers. This responsibility is extended to QualityNet contractors, State agencies acting as QualityNet agents, other government organizations, as well as any entity that has been authorized access to QualityNet information resources as a party to a Data Use Agreement (DUA) with CMS.

QualityNet System Owners/Managers have the responsibility to maintain efficient and effective operations of the QualityNet network systems. The confidentiality, integrity and availability of information transmitted via internet and e-mail systems is a joint responsibility of all QualityNet users. The responsibility for maintaining the QualityNet System Security Policy is delegated to the CCSQ/ISG Information System Security Officers (ISSOs). The security guidance within this policy is mandated for use within the QualityNet system and network infrastructure.

QualityNet users are bound by these Rules of Behavior, guidance, and policy at all times. Violations may result in loss of computer access, written reprimands, termination, fines and/or imprisonment.
(Prosecuting Computer Crimes)

2. Purpose

This document provides a comprehensive information security policy to be followed by QualityNet users who process, store, transmit, or receive QualityNet Medicare and Medicaid data of any sensitivity or classification.

The scope of this policy applies to the Health Care Quality Improvement System (HCQIS) located at the CMS Warrenton, VA Data Center (also known as the QualityNet Data Center); a national network of Quality Improvement Organizations (QIO) responsible for each U.S. state, territory, and the District of Columbia; 1 Clinical Data Abstraction Center (CDAC); the End Stage Renal Disease (ESRD) networks; multiple contractor support locations; and other authorized users who access HCQIS and QualityNet information systems.

The QualityNet Security Awareness section of this policy contains security awareness guidance for all QualityNet functional users and Security Point of Contact (SPOC).

The QualityNet Rules of Behavior, Computer and System Use, and Media Protection and Control provide guidance on acceptable usage of the QualityNet infrastructure, its e-mail and internet services, and security controls for the proper handling, control and/or disposition of digital and non-digital media containing sensitive information(e.g., Personally Identifiable Information (PII), Electronic Health Records (eHR), and Protected Health Information (PHI).

The QualityNet Security Roles & Responsibilities section of this policy outlines those duties related to the implementation of the QualityNet Information Security Program for various QualityNet entities.

It is important to note that this policy does not address either specific business process requirements or the full suite of internal controls that together ensure that business requirements are fulfilled.   It is the responsibility of the business owner of QualityNet systems, in collaboration with the system owner, to ensure that all business process-related internal controls are incorporated into QualityNet systems throughout the risk management process (i.e., via the CMS Expedited Life Cycle) and employed when appropriate and feasible. Business and system owners must document and certify the incorporated security/internal controls in the QualityNet IS Risk Assessment (RA) and QualityNet System Security Plan (SSP) for the system.

3. QualityNet Security Awareness

The Security Awareness Training (SAT) provides a basic overview of security best practice techniques and training to all QualityNet users and is performed annually. Additionally, as new users are introduced to QualityNet, they must complete the SAT prior to any QualityNet account activation or access.

Below lists the current process for completing this requirement:

- Select this link to launch the training:
  http://iase.disa.mil/eta/cyberchallenge/launchPage.htm
- Select "Launch New **CyberAwareness Challenge Federal Version**"
- Complete the online training as prescribed by the program.
- Type your name in the online display for the Certificate of Completion, which is provided at the successful conclusion of the training, and print a copy. (Note: Certificates with a name element prepared otherwise will not be accepted.)
- Sign the Certificate of Completion and provide the original to the local Security Point of Contact (SPOC) for record retention.

4. QualityNet Rules of Behavior

4.1 Introduction

QualityNet has established Rules of Behavior (RoB) as part of the comprehensive QualityNet Security Awareness Program. These rules are designed to promote security awareness for system maintainers, users, operators, and administrators of QualityNet systems. System administrators require an additional Rules of Behavior that document their access as privileged users to QualityNet. Rules of Behavior establish ethical and practical standards, recognizing that knowledgeable users are the foundation to a successful security program. These guidelines were established to hold users accountable for their actions with regard to the Confidentiality, Integrity, and Availability (CIA) of QualityNet information. The Rules of Behavior document and procedure can be found in the QIO and ESRD Infrastructure IT Administrator manuals as an additional appendix.

4.2 Purpose

This section provides guidelines for QualityNet users regarding their responsibilities to support and maintain information security for all QualityNet data. Users must be proactive by staying alert to threats and vulnerabilities, staying abreast of security policies and issues, and reporting any suspected security incident. Users are to act ethically, take initiative, and accept responsibility for safeguarding information resources. The QualityNet Rules of Behavior apply to all QualityNet users, to include those individuals who utilize any QualityNet resource, or are under contract with QualityNet to provide specific services.

4.3 General Rules and Guidelines

As trusted entities of QualityNet, users are the custodial agent of the data used on behalf of the beneficiary. QualityNet users are the first line of defense against security incidents involving data loss, corruption, compromise, and/or exposure.

As with any written guidance, this RoB will require updating periodically in order to deal with new security threats and concerns. Moreover, every possible contingency cannot be addressed; therefore, users are challenged to apply the stated principles, along with their best judgment and the highest ethical standards, to choose their actions wisely. Commensurate with that responsibility are consequences for non-compliance with the RoB. Depending on the severity of the violation, management discretion, and the due process of law, consequences can include the suspension of access privileges, reprimand, suspension, demotion, removal, and criminal and/or civil prosecution.

4.3.1 Physical and Environmental Responsibilities

- **Protect Sensitive Unclassified Information.** Disclosure and modification of QualityNet data that is not specifically authorized is prohibited. QualityNet data should not be used for unauthorized or illegal purposes, for private gain, or to misrepresent oneself or the Centers for Medicare & Medicaid Services (CMS), Health and Human Services (HHS) and the Federal Government. Copyright laws must not be violated when distributing or receiving information via public access systems.

- **Protect Your Equipment.** Mobile computing devices (i.e., laptops, portable storage, memory sticks, etc.) must never be left unsecured by way of appropriate locks or other safeguards to protect from theft. Practice good housekeeping at all times, including no smoking, drinking, or eating around your personal computer or workstation. Keep electrical appliances and magnets away from your computer and storage media.
- **Protect Your Area.** Recognize, politely challenge, and assist people who do not belong in the area to avoid potential security attacks, such as, "Shoulder Surfing" or "Social Engineering". Physical access to secured areas (e.g., data centers, wiring closets) must be limited to authorized personnel via appropriate authorization credentials (e.g., identification badges, proximity cards, smart cards). Authorization credentials (e.g., identification badges, proximity cards, smart cards) must be provided to visitors before authorizing access to areas where QualityNet information systems reside. Visitor access records to areas where QualityNet information systems reside should be maintained and reviewed on a monthly basis. Workstations must be set up so that the computer screen is not visible by individuals standing at a door or when first entering the room (i.e., "shoulder surfing"). If necessary, privacy filter screens may be utilized.
- **Protect Your Media.** Lock up all diskettes, software, removable media, and equipment that contain fixed media and sensitive data. Do not discard QualityNet Medicare and Medicaid sensitive information using the regular trash or established unsecured refuse removal. (Please refer to the QualityNet Media Protection and Decommission Procedures for the Guidelines for Destruction of Sensitive Information.)
- **Report All Security Violations and Suspicious Activity.** All suspected security violations should be reported to the QualityNet Help Desk through your Security Point of Contact (SPOC) as soon as possible. **Security incidents involving Personally Identifiable Information (PII) and/or Protected Health Information (PHI) must be reported to the local SPOC immediately upon discovery. Some examples of a PII/PHI Security Incidents can include but are not limited to, sending PII/PHI in visible clear text via email or sending a fax with PII/PHI to an unauthorized wrong recipient.** (Refer to the QualityNet Incident Response Procedures for further information)
- **Comply with Requirements.** Comply with all applicable Federal, QualityNet and CMS/HHS security policies and procedures.

4.3.2 Data Ownership

All data, reports, documentation, and material developed or provided by a government agency or healthcare provider using QualityNet shall remain the property of the U.S. Government. All reports, documentation and material developed in support of QualityNet shall be the property of the U.S. Government.

4.3.3 Privacy

Ensure the protection and privacy of sensitive information (i.e., PII/PHI) at all times. **Never leave sensitive information unattended or unprotected.** It must always be maintained in a properly secured container (e.g., locked file cabinets or other non-portable storage solutions) when it is not actively being utilized. The use of portable locked containers is acceptable for only the minimum time during which the data is being transported to a different location. Also, properly dispose of unneeded information/data by following the guidance provided in the QualityNet Media Protection and Decommission Procedures.

4.3.4 Information Security Incident Administration

A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations that support an information system. A security incident also includes the loss of data through theft or device misplacement, the loss or misplacement of non-digital media and the misrouting of mail. All of these have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction. The following are some examples of information security incidents:

- Loss or unauthorized disclosure of sensitive data, e.g., PII/PHI.
- Unauthorized alteration of data.
- Unauthorized use of user IDs and passwords.
- Introduction of malicious code or computer viruses into QualityNet information systems.
- Fraudulent activities.
- Network security breach, e.g., when a system has been compromised with a Rootkit, Key Logger, Virus or Worm.
- Loss or theft of computer equipment or media.
- Snooping –user attempting to access the internal network beyond their user privileges.
- Tailgating/Piggybacking – individual entering a secure location by following someone else through a door without having the proper access.

If you become aware of a potential security incident or problem, you **must** report it immediately to your supervisor and SPOC. Once the security problem occurs, an immediate, brief assessment must be undertaken by your SPOC and reported to the QualityNet Help Desk (Phone: 866-288-8912; e-mail: qnetsupport@sdps.org). If the assessment determines that an incident either has taken place or is suspected of having taken place, then a number of initial steps can be followed in order to contain any damage and to minimize the risk to the QualityNet IT and network infrastructure. These steps are further outlined in the QualityNet Incident Response Procedures.

The QualityNet Help Desk is the primary point of contact for information security issues regarding circumvention of information security policies, procedures, controls, or safeguards. The SPOC will be required to coordinate component reports on suspected information security incidents or violations and provide that feedback to the QualityNet Security Team and the QualityNet Help Desk.

All QualityNet Security Points of Contact have the responsibility to ensure that all suspected security intrusions, incidents, or violations are reported to the QualityNet Help Desk. Component supervisors must also ensure that their employees and contractors know their security responsibilities and incident reporting procedures.

5. QualityNet Computer and System Use

5.1 Introduction

QualityNet information systems process data on a daily basis that can be considered sensitive, and if improperly disclosed, may result in harmful malicious activity which can compromise the overall security architecture of the QualityNet infrastructure. Disclosure of some data processed by QualityNet information systems also carries the potential to be in violation of the Health Insurance Portability and Accountability Act of 1996(HIPAA), the Federal Information Security Management Act of 2002 (FISMA), and/or the Privacy Act of 1974.

Strong technical safeguards must be established and exercised by all QualityNet personnel to ensure the Confidentiality, Integrity, and Availability (CIA) of QualityNet information systems, and sensitive QualityNet data. Users must be aware that taking personal responsibility for the security of their workstation, and the data it contains, is an essential part of their job function.

5.2 Purpose

The purpose of this section is to define the appropriate use of all QualityNet information systems that store, process, and/or transmit QualityNet data. The rules and regulations set forth in this section are in place to provide system users, maintainers, operators, and administrators with comprehensive technical guidelines to assist in reaching the goal of the QualityNet Security Awareness Program. Users must also be aware that common sense and prudent judgment must be applied in accordance to all guidelines provided in this section to prevent potential violations, incidents, and breaches from occurring.

5.3 General Rules and Guidelines

5.3.1 Technical Responsibilities

- **Protect Your Workstation.** Always log out or lock your workstation while it is unattended. A fifteen minute password locking screensaver is required for all workstations and cannot be reconfigured by QualityNet users.
- **Protect Your Passwords.** Use only permitted passwords. Change passwords frequently according to existing password policies. Use meaningless character strings, safeguard and do not share your password with anyone. Protect passwords, information, equipment, systems, networks, and communications pathways to which you have access.
- **Standard SDPS Workstation Image**. Do not modify or change workstation configurations or settings without QualityNet Support Engineer direction. This includes, but is not limited to, desktop backgrounds and Windows desktop schemes. Do not reconfigure equipment, software, or hinder computers by operating system passwords.

- **Protect Against Viruses.** Never bring unauthorized or non-business related personal software to work. Beware of borrowed or unsolicited software; these may contain a computer virus designed to capture, alter, or destroy data. Only QualityNet approved hardware and software shall be used on QualityNet workstations. Non-QualityNet hardware such as personally owned or corporate issued thumb drives are prohibited at all times. Minimize the threat of viruses by write protecting diskettes, perform virus checking against any "foreign" data source, and never circumvent the antivirus safeguards on the system.
- **Protect Your Files.** Establish and periodically review access privileges for each sensitive file. Inspect your data to ensure that someone has not tampered with it. Notify your SPOC if access to sensitive information resources has been granted beyond what is required to perform your duties.
- **Protect Against Disaster.** Save your files to a network drive, not your local hard drive (C) or My Documents. The network engineers back up network data and files at frequent intervals. Sensitive information should always be saved on the network, never on portable media or hard drives. Please refer to your QualityNet Network Administrator or SPOC for more information or assistance.

5.3.2 Proper use of QualityNet or Government Information Systems

All use of QualityNet owned or leased computer systems and equipment must be for officially authorized purposes only. All systems and equipment are to be used only by authorized personnel or organizations. Users must exercise common sense and prudent judgment when using systems and/or equipment for personal use.

- Users may access QualityNet systems and data only to the extent that they have been granted authorization.
- Users must not attempt to unlawfully access systems or network resources for which they have not been granted access.

5.3.3 Misuse of QualityNet or Government Information Systems

Use of government equipment for personal business or non-work related activities (e.g., computer games) is strictly prohibited, except as specifically provided in the Personal Use – internet section of this document. The use of government computers for any type of non-official activity violates QualityNet Rules of Behavior and exposes a user to serious disciplinary action. Note that there is no distinction between stand-alone and on-line computer systems. In addition, keeping personal records, playing computer games, or loading unauthorized software onto government computers may be cause for severe disciplinary action. This includes, but is not limited to; accessing, downloading or executing unauthorized programs. Misuse of government property, including programs and data, may be punishable by loss of user privileges, termination, fines, imprisonment, or all of the above.

5.3.3.1 Explicit Material

QualityNet information systems **shall not** be used to send sexually explicit or sexually oriented material via e-mail. Harassing, abusive, intimidating, discriminatory, or other offensive e-mail is also strictly **prohibited**. HHS/CMS/QualityNet maintains a “zero tolerance” policy for any abuse of this type of activity and any reported violations will be fully investigated. QualityNet users found to be in violation of this policy will be subject to immediate termination of their QualityNet user account privileges, report of the violation to the CMS Regional Office Project Officer overseeing their contract and CMS Contracts Office, and possible legal action. If you receive a message containing defamatory, obscene, offensive, or harassing information, you **must** immediately report this finding to your supervisor and SPOC. The SPOC will call the QualityNet Help Desk to initiate the investigation. Chain-type messages and executable graphics files should be deleted immediately. Anyone engaging in the transmission of inappropriate e-mail may be subject to disciplinary action.

Because a wide variety of materials may be considered offensive by colleagues, customers, or suppliers, it is a violation of QualityNet security guidance to store or redistribute any document or graphic file that is not directly related to the user’s job or the QualityNet business activities. The display of any kind of sexually explicit image or document on any QualityNet functional component system is a violation of the QualityNet security guidance and CMS policy on sexual harassment. In addition, sexually explicit material may not be viewed, archived, stored, distributed, edited, or recorded using QualityNet network or computing resources.

QualityNet uses independently supplied software and data to identify inappropriate or sexually explicit internet sites. QualityNet may block access from within our networks to all such sites. ***If a user finds that they have accidentally connected to a site that contains sexually explicit or offensive material, the user must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program and report the site information to the QualityNet Help Desk (phone: 866-288-8912; e-mail: qnetsupport@sdps.org) so it can be blocked.***

5.3.4 Personal and Corporate Owned Information Systems

All non-QualityNet information systems are restricted from any official U.S. Government business involving the processing, storage, or transmission of QualityNet information unless authorized by a CMS QNet Information System Security Officer (ISSO) in writing. This includes, but is not limited to your corporate-supplied workstation, unauthorized external storage devices, and personal computer.

5.3.5 Removal of Equipment and Off-Site Computing

Authorization must be obtained prior to the removal of any QualityNet equipment from an office or building. Local Network Administrators should maintain a check-out log for laptops and other portable computing devices issued or managed by QualityNet and owned by the U.S. Government. An audit review of the logs should be performed annually to maintain an accurate inventory of QualityNet equipment. QualityNet issued equipment should never be taken out of country.

Users who wish to access government computer resources from off-site locations shall provide a secure and protected environment for the government data, government-owned and furnished computing resources. The user must ensure the integrity of the data created, accessed, or modified through the use of an approved VPN solution. The employee shall also adhere to the letter and spirit of all applicable government laws, regulations, contracts, licenses, policies, standards, guidelines, business controls, security rules, and other expectations. Work performance from an off-site location will be monitored and audited producing an audit trail of events and activities that will be automatically reported and reviewed by the QualityNet Security staff. For specific procedures involved in off-site computing, see your QualityNet Network Administrator or SPOC for information specific to your office/location.

5.3.6 Printer and Fax Machine Administration and Guidance

QualityNet allows fax machines to transmit sensitive information provided the following safeguards are utilized to mitigate the risks of unauthorized disclosure.

The safeguards listed below must be followed explicitly:

- The fax cover sheet **must** contain the following disclaimer:

"*The attached information is CONFIDENTIAL and is intended only for the use of the addressee(s) identified above. If the reader of this message is not the intended recipient(s) or the employee or agency responsible for delivering the message to the intended recipient(s), please note that any dissemination, distribution, or copying of the communication is strictly prohibited. Anyone who receives this communication in error should notify us immediately by telephone and return the original message to us at the address above via U.S. Mail. Thank you*."

- Do not put individually identifiable and/or sensitive information on the fax cover sheet.
- Before sending the fax, confirm with the intended recipient that the telephone number for the fax machine is correct. Also confirm that an authorized individual is available to retrieve the document from the fax machine.
- Remove the original document. Wait for the fax machine to print the transmission confirmation. Once transmission is confirmed, contact the receiving party to verify that the fax was received.
- If you are receiving a fax with individually identifiable and/or sensitive information, confirm the expected delivery time with the sender and remove the individually identifiable and/or sensitive information from the fax machine as soon as it arrives.

Printers and fax machines must be located in a secure location where operation can be observed and where sensitive printed or faxed material can be adequately controlled. Documents containing Personally Identifiable Information (PII) and/or Protected Health Information (PHI) must **immediately** be cleared from shared printers.

Paper jams in the fax machine or printer containing privacy or sensitive data must be **immediately** removed and properly disposed of according to the policy. Please refer to the QualityNet Media Protection and Decommission Procedures for the guidelines for Destruction of Media.

5.3.7 Guidance for Mailing PII/PHI

When needed, PII and PHI can be sent via mail, but extra precautionary measures should be exercised when mailing this information as it is outside the direct control of QualityNet. The following actions must be taken when mailing PII/PHI:

- The intended recipient must be contacted to verify their full mailing address prior to shipment. PRS or any other application that stores this type of information should never be used as the sole resource for verifying this information.
- An inventory sheet should be included within the package providing a page count and details of what is included.
- Tamper evident packaging, and if possible, cryptography is to be utilized.
- Packages must have tracking with a receipt from the commercial carrier.

5.3.8 Username and Password Rules

- Every QualityNet user must have a unique username and password for any QualityNet information system for which they have access to.
- Every computer system must have a password assigned.
- Sharing of usernames and passwords is prohibited.
- Passwords must be mixed case, alphanumeric, and at least 8 characters long.
- Safeguard your password. Commit it to memory; do not post it; do not keep it in an obvious place or an unsecured area.
- Do not use an obvious password. Avoid anything resembling your name, hobbies, address, phone number, Social Security Number (SSN), or other personal attributes; do not use a word that can be found in the dictionary.
- Passwords must be changed every 60 days.
- Six unique passwords must be used prior to reusing a password.
- Passwords **must** adhere to the QualityNet & CMS ARS security standards.

5.3.9 Software Administration and Guidance

QualityNet users are not allowed to install or modify software on any QualityNet government owned or leased computer unless approved by the QualityNet Network Administrator or a CMS authorized IT Support Contractor acting on behalf of CMS or a CMS official. Approval must be received for each installation or service and coordinated via the QualityNet Help Desk (Phone: 866-288-8912; e-mail: qnetsupport@sdps.org). This approval is necessary to ensure compatibility of software and security of data files as well as licensing agreements.

Users who make, acquire, or use unauthorized or unlicensed copies of computer software, or use software that is not for official business, shall be disciplined appropriately. Such discipline may include loss of user privileges and/or termination. QualityNet does not condone the illegal duplication of software or any activity that would violate a licensing agreement.

QualityNet licenses the use of computer software from a variety of external vendors. QualityNet does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it. With regard to software use on local area networks or on multiple machines, QualityNet users shall use the software only in accordance with the licensing agreement(s). QualityNet users who learn of any misuse of software or related documentation within their organization shall notify their supervisor, System Administrator or Security Point of Contact (SPOC).

Dispose of unneeded software by returning it to your local System/Network Administrator to be reformatted for reuse or to be destroyed according to policy. Please refer to the QualityNet Media Protection and Decommission Procedures for the guidelines for Destruction of Media.

5.3.10 Wireless Restriction

The installation of wireless access points (WAP) to any QualityNet information system is strictly prohibited unless explicitly authorized, in writing, by the CMS CISO or his/her designated representative. Wireless technologies can include, but are not limited to, Bluetooth, 802.11x, satellite, packet radio (UHF/VHF), and microwave.

5.4 QualityNet E-mail Use

5.4.1 Introduction

This section provides the QualityNet user community policy information pertaining to the appropriate use of QualityNet e-mail and sets forth to establish procedures to ensure appropriate measures are taken to prevent unauthorized use. This e-mail guidance requires users keep abreast of QualityNet security policies and issues, remain vigilant in alerts of threats and vulnerabilities, and report all violations of this security guidance. Violations must be reported by contacting the QualityNet Help Desk through your Security Point of Contact. It is the responsibility of QualityNet System Maintainers/Managers to publish this guidance; as well as, maintain efficient and technical operation of e-mail to provide integrity and confidentiality for data transmission.

All authorized users of the QualityNet e-mail services are reminded this service is provided for government use only in support of the QualityNet mission. E-mail and communications are considered to be government property and are subject to the statutes, regulations, and policies governing proper use of these services; as well as, those regulations and policies pertaining to the confidentiality and disclosure of Federal government information. This includes similar services provided such as system Instant Messaging (IM) services or MS LYNC.

QualityNet e-mail resources shall not be used to violate laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of any QualityNet resource for illegal activity is grounds for disciplinary action and is strictly prohibited. All violations are subject to prosecution under Prosecuting Computer Crimes**.**

5.4.2 Data Transmission

Electronic mail (e-mail) is defined as an office communications tool whereby electronic messages are prepared, sent, and retrieved on personal computers.

It is not permissible to use the QualityNet e-mail resources for transmission of QualityNet Privacy Act protected and/or other sensitive QualityNet information.

QualityNet users should exercise good judgment and common sense when distributing messages. *Confidential information should never be disseminated via e-mail.* This may include, but is not limited to, the transmission of PII, PHI, infrastructure related data, QualityNet clinical, survey, project data, and/or financial information. Like any other written materials, all QualityNet functional component-related messages should be carefully guarded and protected. QualityNet users must also abide by copyright laws, ethics rules, and other applicable QualityNet regulations, policies, and laws. Contact your supervisor or SPOC for clarification and guidance on this directive.

As stated in the aforementioned paragraph, sensitive data cannot be sent via e-mail at any time. However, approved encryption mechanisms that meet the FIPS 140-2, *Security Requirements for Cryptographic Modules*, can be used to encrypt e-mail attachments which can then be sent via e-mail. If sufficient cryptography is not available, any data that may fall into the category of sensitive data must be conveyed via fax, phone, a secured network drive, or QualityNet File Exchange. QualityNet users can use the *Sensitive Data as Email Matrix* located in Appendix B as guidance for determining an appropriate method of transmission for specific data types.

When sending test data, all data must clearly represent dummy/false information as to not be confused with live data. An example of this would include renaming a patient as “Test Patient 1” or listing their Social Security Number as “123-45-6789”. Data that is not clearly represented as test data is to be treated as live data.

Please refer to the CMS Policy for the Information Security Program (PISP) and CMS Information Security Acceptable Risk Safeguards (ARS) for further guidance on approved methods for PII/PHI transmission and storage.

5.4.3 Content Filtering and Monitoring

E-mail filtering products are designed to help an organization enforce its e-mail policies. QualityNet has implemented an e-mail filtering solution to assist with this need. Comprehensive spam and e-mail filtering software allows QualityNet to proactively monitor and manage inbound and outbound communications. If necessary, the spam and e-mail filtering software will block unauthorized inbound and outbound communications. QualityNet provides a multi-level approach to e-mail filtering that allows spam management, virus protection, and the handling of confidential information.

As mandated by the U.S. Department of Health and Human Services (HHS), this QualityNet e-mail security guidance requires that attachments to e-mail with the following extensions are stripped and discarded because of possible virus convolution.

.hta	.pif	.shs	.shb	.sct	.vb	.vbs	.vbe	.wsc	.wsf	.wsh	.scr

Additionally, within the QualityNet infrastructure the QualityNet enterprise e-mail anti-virus server will block the following types of files:

- .exe, including encrypted files
- .bat
- Password-protected files

Users should be aware of attachments and should not accept any that are suspicious or from unknown parties. Avoid opening any e-mail from unknown parties, especially those containing attachments. If you do not recognize the e-mail, good practice is to immediately delete the suspected e-mail and ensure its removal from the system.

QualityNet administrators may access and monitor e-mail usage at any time for any reason without notice. QualityNet managers may request reports that will allow the review of e-mail activity and the analysis of the usage patterns. QualityNet managers may choose to publicize this information to ensure QualityNet internet resources are devoted to maintaining the highest levels of security and productivity. This reporting capability will be statistical in nature. Except for the above purposes, no other attempts will be made to publicly identify an individual user or their usage habits.

5.4.4 Personal Use

QualityNet e-mail service is intended for business use only. QualityNet e-mail users must exercise common sense, prudent judgment, and propriety in the use of this resource. Users who misuse resources in this way will have e-mail privileges withdrawn and possibly be subject to disciplinary action. Repeated e-mail violations will be reported to the CMS Regional Office Project Officer overseeing their contract.

Users shall identify themselves clearly and accurately when sending or forwarding e-mail over the internet. Anonymous or pseudonymous posting is forbidden. All e-mail must be manually reviewed prior to forwarding to other addresses. **Automatic forwarding of e-mail is prohibited.** This includes not only e-mail messages but all other e-mail artifacts such as meeting requests, tasks, and calendar reminders.

The use of QualityNet e-mail resources to conduct any activities already prohibited by Federal, HHS, CMS, or other QualityNet policies (such as private fund raising, political activities, etc.) is prohibited.

Any type of mass e-mailing by QualityNet functional component employees that does not pertain to governmental business is forbidden.

Sharing of QualityNet e-mail accounts is forbidden. Each QualityNet functional component employee should maintain his or her own e-mail address. Usernames and passwords are used for authentication purposes and help maintain individual accountability for e-mail resource usage. Any employee who obtains an ID and password for use of e-mail resources from QualityNet must keep that password confidential. QualityNet security policy prohibits the sharing of user IDs or passwords obtained for access to e-mail.

5.5 QualityNet Internet Use

5.5.1 Introduction

This section provides the QualityNet user community with guidelines pertaining to the appropriate use of the Internet on QualityNet owned information systems. Users are reminded it is forbidden to reveal sensitive QualityNet Medicare information or any other material covered by existing QualityNet privacy policies and procedures on the internet. The Privacy Act of 1974, 5 U.S.C. § 552A, protects personal privacy from invasion by Federal agencies and levies civil and criminal penalties for violations of the provisions of the Act. In addition, users releasing such privacy or sensitive information, whether or not the release is inadvertent, may be subject to the penalties provided in existing QualityNet policies and procedures.

Title 42 of the US Code of Federal Regulations (42 CFR) Part 480 delineates the authority and responsibility of the QIO to disclose information and their responsibility to protect it from unauthorized disclosure. Please refer to Chapter 10 of the QIO Manual for further information.

5.5.2 Content Filtering and Monitoring

Web filtering products are designed to help an organization enforce their internet acceptable use security policies. QualityNet has implemented a web-filtering software solution that enables proactive monitoring, management and, when appropriate, blocking access of inappropriate web sites. QualityNet will block sites based off of categories or content that does not adhere to security, infrastructure, and/or business rules.

Category	Examples
Adult Content	Child Pornography, Explicit Art, Obscene/Tasteless, Pornography/Adult Content, R Rated, X Rated.
Bandwidth	Internet Radio, Peer-to-peer/File Sharing, VoIP, Web Based Storage.
Custom Categories	Social Networks.
Entertainment	Gambling, Gaming.
Illegal/Questionable	Criminal Skills, Dubious/Unsavory, Hate & Discrimination, Illegal Drugs, Terrorist/Militant/Extremist.
Internet Communication	Chat, Instant Messaging.
Internet Productivity	Adware.
Internet/Intranet Misc.	Domain Landing, Invalid Web Pages.
Security	Hacking, Malicious Code/Virus, Phishing, Spyware.

Table 2 – Blocked Web Sites

Allowed Content:

CMS may allow direct URL access for websites in blocked categories. Legitimate business use must be submitted to CMS prior to exception approval.

Other blocked sites such as Webinars may be allowed for business use only. These sites are allowed only if there is not “Third Party” software to install. Any software requiring installation must be approved in advance by the QualityNet Admin and CMS QNET ISSO. If approved, no PII/PHI or any other sensitive information is to be displayed during a session.

QualityNet internet security systems incorporate the ability to record World Wide Web (WWW) site visits generated from the QualityNet network for each QualityNet user. QualityNet security administration reserves the right to monitor QualityNet internet traffic at any time. ***QualityNet users do not have an entitlement to privacy with regard to internet usage.***

QualityNet managers have the ability to generate reports that will allow for the review of activity and the analysis of the usage patterns. QualityNet managers may choose to publicize this information to ensure QualityNet internet resources are devoted to maintaining the highest levels of security and productivity.

5.5.3 Personal Use

QualityNet users are permitted the use of QualityNet internet facilities for non-business research or browsing during the organization’s defined mealtime or break periods, or outside of normal work hours, provided that all other usage policies are adhered to and the usage does not violate Federal, HHS, CMS, or other QualityNet security policies. QualityNet internet users must exercise common sense, prudent judgment, and propriety in the use of this resource. Users who misuse QualityNet resources will have their internet privileges withdrawn and may be subject to disciplinary action.

Users with internet access must take particular care to understand the copyright, trademark, libel, slander, and public speech control laws of all countries in which QualityNet maintains a business presence so their activity on the internet does not inadvertently violate any laws.

The use of QualityNet internet resources to conduct any activities already prohibited by Federal, HHS, CMS, or other QualityNet policies (such as private fund raising, political activities, etc.) is prohibited.

QualityNet has installed an internet firewall to assure the safety and security of the QualityNet networks. Any employee who attempts to disable, defeat, or circumvent any QualityNet security facility may be subject to disciplinary action.

With approval from the Engineering Review Board (ERB), the SPOC or Security Administrator may download approved software with direct defined business use and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license and for the intended purpose justified as described in the approved ERB request.

Prohibited Activities at any time:

Users **cannot** use QualityNet internet facilities to download or participate in:

- Entertainment software
- Game programs
- Play games against opponents over the internet
- Social Networking (MySpace or equivalent websites unless authorized by CMS)
- Internet Radio and Music Streaming services

Only authorized or approved QualityNet internet services provided by CMS or appropriate business related websites are permissible for use during normal working hours. CMS and QualityNet reserve the right to limit the use or block access to any website deemed inappropriate for use.

Users **cannot** upload any software licensed to QualityNet or data owned or licensed by QualityNet or the U.S Government without the express authorization of CMS.

Peer-to-Peer (P2P) file sharing software is prohibited at all times on QualityNet internet and network resources.

- **It is illegal.** Both the Copyright Act of 1976, and the more recent Digital Millennium Copyright Act of 1998, prohibit the distribution or sharing of copyrighted works without the explicit permission of the copyright holder.
- **It is dangerous.** P2P software currently available for file sharing may bypass your computer's operating system security and open your entire computer, along with your sensitive personal information, to anyone on the internet. This activity could potentially provide a conduit from your computer to the QualityNet network and compromise our network security. P2P programs such as µTorrent, Limewire, Kazaa, mIRC and others may affect your computer's performance and can cause system crashes or loss of your valuable data.
- **It degrades overall network performance.** The nature of these programs is to share your files with as many computers as possible. The resulting volume of network traffic can degrade and/or disable the performance of the entire network.

Unique usernames and passwords establish individual accountability for internet resource usage. Usernames and passwords function as the authentication mechanism by which a user is identified and granted access to network resources. All QualityNet users **must** keep their password confidential. QualityNet security policy prohibits users from sharing usernames or passwords at any time for any purpose.

5.5.4 Social Media

CMS Social Media guidelines identify the appropriate use of social media for CMS business and provide examples of how QualityNet personnel are to use social media in the workplace. All QualityNet employees should familiarize themselves with these guidelines, and be aware of the legitimate business use of social media.

Though some social media is blocked under the Social Media Policy, CMS does allow access to some social media sites (e.g., Facebook, YouTube, Twitter, Foursquare, SquibD, Pinterest, LiveJournal, etc.) as deemed appropriate. QualityNet users may access these social media sites in the workplace for work related purposes only. Work related purposes can be defined as informational, educational and/or training tools that provide employees with the ability to perform specific job tasks or functions. As with other aspects of the Internet, authorized use of social media sites must support CMS' mission and operations.

Social media can be used to support CMS in a number of ways. Below are a few examples of how social media can be used for CMS business:

- Accessing or obtaining information outside of CMS:
    - Accessing government content housed on social software websites. For example, Congressional testimony is available on YouTube and CDC updates on H1N1 are available through Twitter.
    - Accessing known external networking sites (YouTube, Facebook, LinkedIn, etc.) for information on "best practices" in recruitment, communication, and performance management.
    - Accessing training, professional materials and research, and information resources.
    - Accessing professional communities-of-practice for regular exchanges on topical issues.

- Sharing information outside of CMS:
    - Sharing public information with beneficiaries, press, caregivers and other key audiences on a variety of QIO/ESRD programs.
    - Making use of a wide variety of training, research and resource materials available on social networking sites.
    - Sharing information on "best practices" in recruitment, communication and performance management.
    - Posting recruitment and marketing videos and materials for access by prospective candidates.
    - Publishing information regarding planned recruitment events.

5.5.4.1 Social Media Monitoring

The QualityNet community is reminded that the use of social software in the workplace or on CMS-issued equipment is subject to comprehensive auditing, monitoring and tracking. Either during working or non-working hours (e.g., while at home), QualityNet personnel must not use social media websites and CMS equipment and/or resources to transmit information or knowingly connect to sites for unlawful or prohibited purposes that may violate HHS, CMS and/or other QualityNet policies.

QualityNet users **<u>must not</u>:**

- Use the words "CMS" or "HHS" to identify groups they create on these services, and if they do so, employees should include a disclaimer[1] stating that the statements expressed therein do not necessarily reflect the views of CMS, HHS or the United States Government;

[1] A standard disclaimer is the following: "The views expressed here do not necessarily represent the views or opinions of CMS or the Federal government."

- Violate any harassment or discrimination policies (such as CMS' Equal Employment "Zero Tolerance" policy) or violate any CMS, HHS, or government-wide policies;
- Disclose potentially confidential CMS/HHS information or information that may be protected by the Privacy Act or other statutory authority;
- Make false statements, or reckless statements with disregard for the truth, about CMS or its employees;
- Use the CMS/HHS logo;
- Transmit, or attempt to access, photos that are sexually explicit, sexually oriented (e.g. lewd/indecent) or pornographic, or contain profane/abusive comments.

Additional information regarding the appropriate use of social media can be found here:

http://intranet.cms.gov/Component/OOM/MPSG/Documents/policyonsocialsoftware.docx

Please notify your internal point of contact if you have any questions. He or she may contact the QualityNet Help Desk if additional information and/or assistance is needed.

6. QualityNet Media Protection and Control

6.1 Introduction

This section defines the policy for the destruction of sensitive PII/PHI Medicare information and establishes a minimum set of security controls that will apply for all QualityNet users. Once sensitive QualityNet data is no longer needed, all QualityNet sensitive information must be securely destroyed by an approved method. Users need to understand that taking personal responsibility for the handling, storage, and destruction of sensitive information is an essential part of their job.

<u>**Users must understand that as trusted entities of QualityNet, they are the custodial agents of data used on behalf of beneficiaries. QualityNet users are critical components against a potential disclosure of beneficiary information. Users must ensure that the data/medium identified to be destroyed, be done so in such a manner, that the data will not be recoverable.**</u>

For further detailed information related to QualityNet Media Protection, please refer to the QualityNet Media Protection and Decommission Procedures.

6.2 Purpose

The purpose of this section is to establish uniform guidelines for the proper identification, handling, and disposal of computer and hardcopy media. The disposal procedure(s) used will depend upon the type and intended disposition of the media. Electronic media may be scheduled for removal from service for a variety of reasons. Adequately disposing of electronic media will reduce security risk.

6.3 General Rules and Guidelines

The following guidance for the destruction of PII/PHI Medicare sensitive information applies to <u>**all**</u> QualityNet users, users under contract to QualityNet, and Care Providers supplying QualityNet services or using QualityNet information resources.

Release of Computer Storage Media – Computer storage media that has been used to record sensitive PII/PHI Medicare information must not leave the controlled channels until it has been degaussed/ zeroized prior to recycling for reuse or destroyed by the approved QualityNet method.

Sensitive Information Destruction/Concealment Before Servicing Done – Before computer magnetic storage media is sent to a vendor for trade-in, servicing, or disposal, all PII/PHI Medicare sensitive information must be destroyed or concealed by the approved QualityNet method.

Areas Containing Sensitive Information Must Have Cross-Cut (Confetti) Type Shredders or Secure Storage Bins Clearly Marked and Identified for Destruction –

The staff working in these areas must be trained and be informed which materials need to be shredded or how the sensitive materials stored in the secure storage bins must be prepared for destruction.

In Lieu of a Shredder, the Use of a Bonded, Secure Document Destruction Service is Acceptable – When the QualityNet Functional Component office is utilizing a bonded removal/destruction service, a log must be maintained to document the chain of custody for the material to be destroyed. A file containing a copy of the invoices submitted by the destruction service will suffice in lieu of a log. The purpose of a record or log is to maintain an audit trail of the life-cycle for the destruction of the sensitive hard copy information.

Use of Secure Containers to Hold Sensitive Information to Be Destroyed – All sensitive information no longer being used or no longer needed—no matter what form it takes (e.g., disks, tapes, hard drives, CDs, DVDs, hardcopy, printouts, etc.) shall be placed in designated, specially designed secure storage bins, that can be appropriately secured, until such time as authorized personnel or a bonded destruction service picks it up for destruction. The sensitive information must have controlled or limited access to ensure that the material is protected until pickup or destruction occurs.

Persons Authorized to Destroy Sensitive Medicare Information – To ensure the destruction of sensitive information is performed correctly, this service must be carried out by assigned QualityNet Functional Component personnel or a bonded destruction service. A log must be maintained to track the history of all destroyed sensitive information. Bonded destruction service companies must keep a log and provide certificates of destruction of all QualityNet information destroyed. If the bonded destruction service company does not keep a log of all QualityNet information destroyed, the SPOC must keep a log of the QualityNet information destroyed. A file containing a copy of the invoices submitted by the destruction service will suffice in lieu of a log. The purpose of a record or log is to maintain an audit trail of the life-cycle for the destruction of the sensitive hard copy information.

Destruction of Materials Used in Handling Sensitive Information – All materials used in the handling of sensitive information, which could be analyzed to deduce sensitive information, must be destroyed in a manner similar to that required for sensitive information. This security guidance covers typewriter ribbons, carbon papers, mimeograph stencil masters, photographic negatives, thermal fax transfer films, aborted computer hardcopy output, unacceptable photocopies, etc.

7. QualityNet Security Roles and Responsibilities

The following entities have responsibilities related to the implementation of the QualityNet Information Security Program.

7.1 QualityNet Business Owners/System Maintainers/Managers

QualityNet Business and System Maintainers / Managers shall assess the risk to the information and information systems over which they have responsibility. They shall also ensure, through system certification, that each information system is developed, implemented, and operated according to the requirements of this policy.

7.2 QualityNet Information System Security Officer (ISSO) and Chief Information System Security Officer (CISSO)

The QualityNet CISSO (Chief Information System Security Officer) shall oversee the implementation and management of the QualityNet IS program. The CISSO will also act as lead ISSO (Information System Security Officer) within the QualityNet IS program. The ISSO (Information System Security Officer) shall coordinate the technical certification of Risk Assessments (RAs) and System Security Plans (SSPs) and serves as the primary point of contact for all information security issues such as contingency planning and incident response and security related policy. The ISSO shall also ensure that QualityNet adheres to all applicable federal laws, regulations, policies, and procedures.

7.3 QualityNet Security Analysts/Engineers

QualityNet Security Analysts/Engineers shall assist the ISSO with the implementation of the QualityNet IS program. They are involved in planning, coordinating and implementing security policies and procedures covering the QualityNet enterprise environment. Specific duties include conducting risk assessments, developing and updating security and contingency plans as well as disaster or emergency recovery procedures for networking infrastructure and application systems.

7.4 QualityNet System Engineers/Administrators

QualityNet System Engineers/Administrators shall be responsible for verifying that system security requirements of their systems are being met; establishing and communicating the security safeguards required for protecting systems based on the sensitivity levels of the information; ensuring that the security controls implemented are functioning as intended; and periodically reviewing and verifying that all users of the system are authorized and are using the required systems security safeguards, in compliance with QualityNet IS Program. System Engineers/Administrators shall also be responsible for the planning and implementation of ongoing maintenance of information systems, including updates, upgrades and patches in accordance with the ILC and this policy.

7.5 QualityNet Database Administrators

QualityNet Database Administrators shall be responsible for verifying that system security requirements of their systems are being met; establishing and communicating the security safeguards required for protecting systems based on the sensitivity levels of the information; ensuring that the security controls implemented are functioning as intended; and periodically reviewing and verifying that all users of the system are authorized and are using the required systems security safeguards, in compliance with QualityNet IS Program. System / Database Administrators shall also be responsible for the planning and implementation of on-going maintenance of information systems, including updates, upgrades and patches in accordance with the ILC and this policy.

7.6 QualityNet System Maintainers/Developers

System Maintainers/Developers shall be responsible for developing and implementing the security requirements throughout the ILC as System Owners/System Maintainers/Managers define the requirements of the information system. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for System Maintainers/Developers), or operational practices (e.g., awareness and training). The System Maintainer/Manager shall also be responsible for the planning and implementation for the on-going maintenance of the information system, including updates, upgrades and patches in accordance with the ILC and this policy.

7.7 QIO Security Points of Contact (SPOC)/Information System Security Officers (ISSO)

QIO Security Points of Contact (SPOC)/Information System Security Officers (ISSO) shall be responsible for ensuring the protection of QualityNet information (data) and information systems within each of their respective facilities by complying with the requirements maintained in this policy. The SPOC shall be responsible for receiving any report of suspected security intrusions, incidents, events, violations, or breaches and ensuring that it is reported to the QualityNet Helpdesk.

7.8 QualityNet Users

QualityNet users shall be responsible for ensuring the protection of QualityNet information (data) and information systems by complying with the requirements maintained in this policy. As trusted entities of QualityNet, users shall assume the responsibility for being custodial agents of beneficiary data. In addition, QualityNet users shall be required to complete yearly security awareness training.

7.9 QualityNet Help Desk

The QualityNet Help Desk (phone: 866-288-8912; e-mail: qnetsupport@sdps.org) shall serve as the first point of contact for reported operational problems and security incidents.

Upon notification of a security incident, the QualityNet Help Desk shall immediately notify appropriate QualityNet Security personnel who will categorize and manage security incidents to closure.

Appendix A – References

Federal Laws and Regulations

Privacy Act of 1974 - http://www.justice.gov/opcl/privstat.htm

OMB Circular A130, Appendix III - http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii

e-GOV Act of 2002 - http://www.archives.gov/about/laws/egov-act-section-207.html

FISMA - http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Electronic Freedom of Information Act of 1996 (E-FOIA) – http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm

Department of Justice (DOJ) Freedom of Information Act (FOIA) - http://www.usdoj.gov/04foia/index.html

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

Clinger-Cohen Act - http://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf

Homeland Security Presidential Directive 12 - http://www.dhs.gov/homeland-security-presidential-directive-12

Homeland Security Presidential Directive 7 - http://www.dhs.gov/homeland-security-presidential-directive-7

OMB Memoranda - http://www.whitehouse.gov/omb/memoranda_default

NIST Special Publications (800 Series) - http://csrc.nist.gov/publications/PubsSPs.html

CMS Policy and Standards

CMS Policy for Information Security - http://www.cms.hhs.gov/InformationSecurity/Downloads/IS_Policy.pdf

CMS Policy for the Information Security Program (PISP) - http://www.cms.hhs.gov/InformationSecurity/Downloads/PISP.pdf

CMS Information Security Acceptable Risk Safeguards (ARS) - http://www.cms.hhs.gov/InformationSecurity/Downloads/ARS.pdf

CMS Information Security (IS) Certification & Accreditation (C&A) Program Procedures - http://www.cms.hhs.gov/informationsecurity/downloads/CA_procedure.pdf

CMS System Security Plan (SSP) Procedure -
http://www.cms.gov/informationsecurity/downloads/SSP_Procedure.pdf

CMS Information Security Risk Assessment (IS RA) Procedure -
http://www.cms.gov/informationsecurity/downloads/IS_RA_Procedure.pdf

CMS IS Incident Handling and Breach Analysis/Notification Procedure –
http://www.cms.gov/informationsecurity/downloads/Incident_Handling_Procedure.pdf

QualityNet Policy and Procedures

QualityNet Incident Response Procedures -
https://qionet.sdps.org/training_resources/qnet_security.shtml

QualityNet Media Protection and Decommission Procedures -
https://qionet.sdps.org/training_resources/qnet_security.shtml

QIO Infrastructure Operations and Support Manual –
http://qionet.sdps.org/ (secure login required)

QIO Infrastructure IT Administrator Manual –
http://qionet.sdps.org/ (secure login required)

ESRD Infrastructure Support Manual - http://esrdncc.org/index/information-for-esrd-networks

ESRD Infrastructure IT Administrator Manual - http://esrdncc.org/index/information-for-esrd-networks

Appendix B – The Sensitive Data as Email Matrix

Transmission of Specific Data Types via Email in Clear Text

System/Information	Example	Internal Email*	External Email*
Single QualityNet User password, encrypted file password; Limiting factors: (1) Except for the password itself, the body of the email is **blank**. (2) Only **a single** password per email. Email **format MUST** be **plain-text**, not HTML or Rich-text.	All	Yes, with limiting factors	Yes, with limiting factors
IP Address (all formats except one, see next item below)	123.123.123.123	Yes	**No**
IP Address (restricted to a single format, as shown, i.e., first and second octet must be masked)	XXX.XXX.123.123	Yes	Yes
Single Server Names, Database Names, Computer Names, Host Names, Asset Tag Number (**NOTE:** Single name only, names are not Internet DNS resolvable, no network or logical system diagrams, no additional details about the host – purpose, location, etc.)	PdXxYy01	Yes	Yes
Multiple server names, database names, host names, Asset Tag Numbers without regard to quantity or type (i.e., names are Internet DNS resolvable or names are not Internet DNS resolvable)		Yes	No
Private/Internal/Intranet URL that is non-routable via the Internet	QIONet.sdps.org	Yes	Yes
Taxpayer Identification Number (TIN) (includes EIN and SSN)	All formats	No	No
Date of Birth (all formats)	01/01/2001	No	No

Table 3 - Sensitive Data as Email Matrix

*Must adhere to these definitions:

- Internal Email is defined as email that originates from and delivers to only addressing schemes ending in esrd.net or sdps.org.
- External Email includes all email not included within the definition of Internal Email.