QualityNet/SDPS
HIPAA Compliance Summary

Transaction and Code Set Rule
Compliance date = October 16, 2003
SDPS accepts the mandated Code Sets (ICD-9, CPT, HCPCS, etc…) as required, however the ANSI transactions are not utilized as this system is not involved in the claim payment process.

National Identifiers
Employer Identifier – effective date = July 30, 2004
Not applicable

Provider Identifier – effective date = May 23, 2005, compliance date = May 23, 2007
In progress of modifying applications to facilitate the collection of NPI and updating systems to retain and crosswalk the providers' identifiers. Contractors are working side by side with CMS to ensure timely compliance.

Privacy Rule
Compliance date = April 14, 2003
The QualityNet/SDPS system stores/processes the data submitted by the providers to the QIO program. Data from the QualityNet/SDPS system is only released according to Chapter 10 – Confidentiality and Disclosure of the Quality Improvement Organization Manual (Rev. 15, 06-30-06).

Security Rule
Compliance date = April 20, 2005
The 3 major requirement sections that comprise the rule, Administrative Safeguards, Physical Safeguards and Technical Safeguards are addressed and implemented as follows:

Administrative

Security Management Process

- SDPS/QualityNet utilizes the CMS Risk Assessment methodology and has performed Risk Assessments on all existing systems, as well as all new systems. Any vulnerabilities that are identified are either mitigated to a low risk level or the risk is accepted in writing by the Business Owner/Manager. Risk Assessments are performed when there is a major change to an existing system or a security violation.

- Information System Activity Review – The QualityNet Support Engineer Auditing and Monitoring Policy Version 1.0, September 1, 2005 defines types of system activity to be monitored.

Assigned Security Responsibility – An Information Systems Security Officer (ISSO) has been assigned to the QualityNet/SDPS system. For QualityNet the ISSO is Michael Blake and as interim is Jason Goldwater; both are CMS employees.

Workforce Security

- Authorization and/or Supervision – The system access options in the QualityNet system employ the least privilege philosophy. Users are granted access to only what they need to do their jobs.
- Workforce Clearance Procedure – CMS has implemented background check procedures based on the HSPD-12.
- Termination Procedures – Upon termination or transfer of a user, system and physical access is revoked. The QualityNet Support Engineer Auditing and Monitoring Policy Version 1.0, September 1, 2005 is followed and periodic auditing is performed to ensure the termination procedures are being followed.

Information Access Management

- Isolating Healthcare Clearinghouse function – Not Applicable, the QualityNet/SDPS systems do not function as Healthcare Clearinghouses.
- Access Authorization, Access Establishment and Modification - QualityNet Identification and Authentication Policy, Version 1.0, June 1, 2006 cover such items as Account Management, Least Privilege, and Identifier Management.

Security Awareness and Training Plan – QualityNet Security Policy Handbook training is required prior to being granted a password to the QualityNet/SDPS System. This training is performed, tested, and tracked via the QualityNet eLearning Center which is an Internet based Learning Management System (LMS). In addition to the initial training, this policy handbook is updated, at minimum, annually and training is required annually.

- Security Reminders - Periodic reminders are provided via monthly newsletters and posters that cover different security issues.
- Protection from Malicious Software – Virus, Spyware and Adware protection is located on all servers and workstations and definitions are updated daily.
- Log-In Monitoring – Log in monitoring is specific to mainframes and QualityNet/SDPS does not run on a mainframe.
- Password Management – Passwords are required to be changed upon initial login and policy requires the passwords to be a minimum of 8 bytes, combination of letters and numbers/special characters, changed every 60 days, 6 unique prior to reusing a password.

Security Incident Procedures

- Response and Reporting – The QualityNet Security Incident Policy and Procedures Version 2.0 dated July 26, 2006 was released on August 2, 2006.

Contingency Plans

- Data Backup Plan – Data Back up plans are in place and weekly back ups are taken off site to a local climate controlled storage facility and monthly back ups are taken to a climate controlled storage facility 100 miles away from the main location.
- Disaster Recovery Plan & Emergency Mode of Operation Plan & Applications and Data Criticality Analysis – Quality Net Contingency Plan (General Support System) and The Health Care Quality Improvement Systems (HCQIS) Contingency Plan for the SDPS, QIES and CROWN major applications are in place. All QIOs have also submitted their plans which are reviewed by CMS.
- Testing and Revision Procedure - Table top tests are performed annually to test the effectiveness of the plans, and adjustments are made based on results. Real life tests have been also performed due to the hurricanes.
- Periodic Technical and Non-technical Security Evaluation – Annual penetration testing is performed by an outside entity reviews against requirements are performed as required. Reviews include but are not limited to: The HHS Minimum Security Configuration Requirements, based on NIST 800-53, Federal Information System Management Act (FISMA) Requirements, NIST – DISA STIGS, Checklists and NSA Guides.

Business Associate Contracts and Other Arrangements. – Providers do not need Business Associate Agreements with QIOs to release data to them, as the QIOs are Health Oversight Agencies. Data from the QualityNet/SDPS system is only released according to Chapter 10 – Confidentiality and Disclosure of the Quality Improvement Organization Manual (Rev. 15, 06-30-06).

Physical

Facility Access Controls

- Contingency Operations - Quality Net Contingency Plan (General Support System) and The Health Care Quality Improvement Systems (HCQIS) Contingency Plan for the SDPS, QIES and CROWN major applications are in place. All QIOs have also submitted their plans which are reviewed by CMS.
- Facility Security Plan & Maintenance Records – Physical and Environmental Protection Policy, V1.0 – due for publication October 2006. The QIO Security Audit Checklist is utilized to validate appropriate controls are in place at the QIOs.
- Access Control and Validation Procedures – QualityNet Identification and Authentication Policy, Version 1.0, June 1, 2006 covers such items as Account Management, Least Privilege, and Identifier Management.

Workstation Use

- *Policy and Procedures for Workstation Use* – The CMS QualityNet Rules of Behavior are documented in the CMS QualityNet System Security Policy Handbook, Version 3.0, April 24, 2006. Also includes policies on e-mail and Internet usage.

Workstation Security

- *Implement Physical Safeguards for Workstations* - Physical and Environmental Protection Policy, V1.0 – due for publication October 2006. The QIO Security Audit Checklist is utilized to validate appropriate controls are in place at the QIOs.

Device and Media Controls

- Disposal, Media Re-Use and Accountability – Guidelines for disposal and reuse of hardware are included in the QualityNet Enterprise Hardware Decommission Policies and Procedures. V1.0 July 15, 2005. Disposal of paper and media is addressed in the CMS QualityNet System Security Policy Handbook, Version 3.0, April 24, 2006.
- Data Back up and Storage – Requirements include daily and weekly back ups, and are in section 4.4 of the QIO Infrastructure Operations and Support Manual, V3.0, April 28, 2006

Technical Safeguards

Access Control

- Unique User Identification – Unique User Ids are required in this system and guidance on how to set up a new user is located on page 58 in the QIO Infrastructure IT Administrator Manual, V2.0, September 1, 2005.
- Emergency Access Procedure – If necessary, administrators are granted the access necessary to provide emergency access.
- Automatic Logoff – All workstations are configured to auto lock after 10 minutes of non-use. Users are required to lock their workstations when leaving their desk.
- Encryption and Decryption – Encryption of passwords files is in place. Encryption of data is in placed based on results from the respective risk assessment.

Audit Controls – The QualityNet Support Engineer Auditing and Monitoring Policy Version 1.0, September 1, 2005 defines types of system activity to be monitored.

Integrity

- Mechanism to Authenticate Electronic Protected Health Information - QualityNet Identification and Authentication Policy, Version 1.0, June 1, 2006 covers such items as Account Management, Least Privilege, and Identifier Management.

Person or Entity Authentication - QualityNet Identification and Authentication Policy, Version 1.0, June 1, 2006 covers such items as Account Management, Least Privilege, and Identifier Management.

Transmission Security

- Integrity Controls - Virtual Private Network (VPN) Registration and Account Maintenance Procedures , Version 1.0, July 14, 2006
- Encryption – Encryption requirements are evaluated in each risk assessment of a system and a determination is made as to whether or not encryption applies and if so, how it should apply.

Multiple reviews of the system have occurred.

- FISMA audit by OIG
- Minimum Security Configuration Requirement review – based on the NIST SP 800-53.
- JANUS Penetration testing