Office of the Administrator
Centers for Medicare & Medicaid Services

CMS Policy for
Information Security

April 12, 2006

Document Number: CMS-OA-POL-SEC01

TABLE OF CONTENTS

1. PURPOSE

CMS' information and information systems are fundamental to our daily operations and future success. We shall implement procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed on our systems, and to ensure that the systems and information are available to authorized persons when required.

2. BACKGROUND

As the agency charged with administering the Medicare, Medicaid, and State Children's Health Insurance Programs, CMS collects, generates and stores financial, health care, and other sensitive information. Most of this information relates to the health care provided to the nation's Medicare and Medicaid beneficiaries, and as such has access restrictions as required under legislative and regulatory directives. CMS must protect and ensure the security of its information and information systems.

The objective of our information security policy is to safeguard the confidentiality, integrity and availability of our information and systems. These terms are defined as follows:

- *Confidentiality* is ensuring that information and processing capability are protected from unauthorized disclosure or use.

- *Integrity* is ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably.

- *Availability* is ensuring that information systems, including stored information and processing capability, are always available to authorized users when needed.

To accomplish the objectives of the CMS Policy for Information Security, CMS has established an Enterprise-wide Information Security Program based on four pillars:

- Security Policies and Procedures – to assure that security policies, standards, guidelines and procedures are developed and remain current and consistent with CMS's business and information system environments.

- Training & Awareness – to increase staff awareness of the importance of security, to empower appropriate staff with the skills needed to conduct CMS information security management activities and to correct unsafe computing practices found in audits.

- Security Architecture – to assure that the information security environment continues to meet business needs and to address new and emerging threats by identifying risks and by providing adequate security protection through the testing, implementation, and improvement of new and existing security technologies and processes.

- Certification and Accreditation – to assure that security risks are identified, appropriate protections are in-place, and security responsibilities are assigned, prior to authorizing system(s) for operation, as well as periodic assurance thereafter.

3. SCOPE

This CMS Policy for Information Security applies to all management, users, system owners/managers, system maintainers, system developers, operators and administrators, including contractors and third parties, of CMS information systems, facilities, communications networks and information. This policy applies to all information collected or maintained by or on behalf of CMS and all information systems used or operated by CMS, by a CMS contractor, or any organization on behalf of CMS.

4. POLICY

All CMS information shall be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction -- whether accidental or intentional – in order to maintain confidentiality, integrity, and availability. The security controls to provide this protection shall be risk-based and business-driven with implementation achieved through a defense-in-depth security structure. Access to all CMS information shall be limited based on a least-privilege approach and a need-to-know basis. Authorized user access shall be limited to only information necessary for the performance of required tasks.

Information security is a responsibility shared by senior agency officials, all CMS managers and staff, Business and System Owners, IT professionals, and all other users of CMS information and information systems. CMS shall implement an Information Security Program that provides policies, standards, procedures, and guidance to ensure the protection of our information and information systems. CMS shall develop and maintain a virtual *Information Security Handbook* to communicate with and to assist senior agency officials and Business and System Owners on specific information security issues, such as management, operational and technical safeguards as well as on information security policies, standards, procedures and guidance.

5. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this policy:

5.A. CMS Administrator

The CMS Administrator has the overall responsibility for the implementation of an agency-wide Information Security Program as required by laws and regulation and as directed by the Department of Health and Human Services (DHHS) for ensuring compliance with all government-wide legal and policy requirements. This includes providing information security protections commensurate with the risk and magnitude of the harm resulting from access, use

disclosure, disruption, modification, or destruction of CMS information or information systems; complying with the requirements of Federal Information Security Act (FISMA) of 2002; ensuring that information security management processes are integrated with the CMS strategic and operational planning process; ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control; delegating to the Chief Information Officer (CIO) the authority to ensure compliance with the FISMA requirements; ensuring that CMS has trained personnel sufficient to assist CMS in FISMA compliance; and ensuring that the CIO, in coordination with senior agency officials, reports annually on the effectiveness of the CMS information security program.

5. B. Director, Office of Information Services (OIS) and Chief Information Officer (CIO)

The CMS CIO is responsible for the implementation and administration of the CMS Information Security Program. The CIO, with input from senior agency officials, and Business and System Owners, develops and implements additional policies, standards, guidelines and procedures that fully comply with this policy and FISMA, as well as DHHS and government-wide security directives. FISMA requirements include: periodic assessments or risk; certification and accreditation of all systems including annual security testing and security self assessments; development and testing of contingency plans; providing security and awareness training to all employees and specialized (role-based) training to those with significant security responsibilities. The CIO shall publish and maintain these policies, standards and guidelines in the virtual C*MS Information Security Handbook*.

The CIO shall designate a Chief Information Security Officer (CISO) to carry out the CIO's information security responsibilities; develop and maintain the CMS-wide information security program, develop and maintain information security policies, procedures and control techniques to address all applicable requirements; train and oversee personnel with significant responsibilities for information security; and assist senior agency officials as well as Business and System Owners in understanding their security responsibilities. The CIO is the CMS Designated Approving Authority (DAA) for all CMS information systems.

5. C. Chief Information Security Officer (CISO)

The CMS CISO shall carry out the CIO's responsibilities under FISMA, have information security duties as his/her primary duty, shall possess professional qualifications to administer the information security functions and shall head an office with the mission and resources to assist in achieving and maintaining organizational compliance with the CMS information security policies, standards and procedures.

5. D. Business Owners/Partners and System Owners/Managers

Business and System Owners must periodically assess the risk and magnitude of harm to the information and systems over which they have control that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of CMS information or information systems that support the operations and assets of the agency; develop operational

policies and procedures that: are based on the risk assessments, cost-effectively reduce information security risks to an acceptable level, ensure that information security is addressed throughout the life cycle of the information systems under their control, and ensure compliance with CMS information security policies, standards and procedures. Also, for systems within their control Business and System Owners must provide subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate; provide annual information, system specific, security awareness training to inform personnel including contractors and other users of information systems under their control of CMS' information security requirements; periodically test and evaluate, including self-assessments, the effectiveness of the information security policies, procedures and practices with a frequency depending on risk, but no less than annually; plan implement, evaluate and document remedial action to address any deficiencies in the implementation of the CMS information security policies, standards and procedures; maintain current certification for all systems including updating system security plans and risk assessments, develop processes for detecting, reporting and responding to security incidents for systems within their control; develop and test annually contingency plans to ensure the continuity of operations for CMS information systems; and appoint an Information System Security Officer for each system.

5. E. Users

Users have the responsibility to ensure the protection of CMS' information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction by complying with the information security requirements maintained in this policy and in the virtual *CMS Information Security Handbook.*

6. APPLICABLE LAWS/GUIDANCE

The following laws and guidance and any officially designated successors are applicable to this policy:

- E-Government Act of 2002;
- Federal Information Security Management Act (FISMA) of 2002,
- Health Insurance Portability and Accountability Act (HIPAA), 1996;
- The Privacy Act of 1974;
- Office of Management and Budget (OMB) Circular No. A-123 Management Responsibility for Internal Control
- OMB Circular No. A-127, Financial Management Systems;
- OMB Circular A-130, Management of Federal Information Resources;
- HHS-IRM-2004-0002, Information Security Program Policy, December 15, 2004
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series, including but not limited to:
    - NIST SP 800-12 – *An Introduction to Computer Security – The NIST Handbook,*
    - NIST SP 800-18 – *Guidelines for Developing Security Plans,*
    - NIST SP 800-26 – *Security Self-Assessment Guide for Information Technology Systems,*

- NIST SP 800-34 – *Contingency Planning Guide for Information Technology Systems*, and
- NIST SP 800-37 – *Guide for the Security Certification and Accreditation of Federal Information Systems.*

7. EFFECTIVE DATES

This policy supersedes the policy dated September 10, 2003, and becomes effective on the date that CMS' Administrator signs it and remains in effect until officially superseded or cancelled by the Administrator.

8. INFORMATION AND ASSISTANCE

Please contact Bethany Delude, Director, Division of Security Policy and Assessments, within the System Security Group, OIS, at 410-786-5841 (e-mail: Bethany.Delude@cms.hhs.gov) for further information on this policy.

9. APPROVED

/s/ 04/12/06

Mark McClellan, M.D., Ph.D.
Administrator, CMS

Date of Issuance

10. GLOSSARY

Accreditation – authorization by the CMS CIO, or his/her designate, to place an IT system into operation.

Certification – the technical and non-technical evaluation of an IT system – by the system owner or by an independent certifying agent - that produces the necessary information required by the authorizing official to make a credible, risk-based decision on whether to place an IT system into operation.

11. ATTACHMENTS

There are no attachments to this policy.