Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS POLICY FOR THE ACCEPTABLE USE OF CMS DESKTOP/LAPTOP AND OTHER IT RESOURCES

December 8, 2008

Document Number: CMS-CIO-POL-INF04-02

TABLE OF CONTENTS

Nature of Changes

Version INF04-02: This is a revision to the December 2005 issuance of the *CMS Policy for Acceptable Use of CMS Desktop/Laptop and Other IT Resources*, in response to CMS modifying this policy to expand the Operational Policy section to support the CMS 2009 Desktop Refresh. Modifications can be found in the following sections:

1. Section 2, Background:
    a. Changed date of issuance for the HHS Information Resource Management (IRM) Policy for Personal Use of Information Resources to February 17, 2006.
    b. Changed virus-infected to malicious software which is a broader category for prevention.

2. Section 4, Operational Policy – Rewrote section adding subsections for the following:
    - 4.1. Prohibited Use of CMS IT Resources;
    - 4.2. Internet and Email Usage;
    - 4.3. Personal Use of CMS IT Resources;
    - 4.4. Unacceptable and Unlicensed Software Usage; and
    - 4.5. Monitoring of CMS IT Resource Usage.

3. Section 5, Roles and Responsibilities:
    a. 5.2. – Changed name of responsible organization under roles and responsibilities to Office of Information Services (OIS) / Enterprise Data Center Group (EDCG).
    b. 5.3. – Changed name of responsible organization under roles and responsibilities to Office of Information Services (OIS) / Enterprise Architecture and Strategy Group (EASG).
    c. 5.3. – Restructured subsection into two bullets that describes the responsibilities of the OIS/EASG for the following activities:
        - Training all CMS employees, contractors, and other users of CMS IT resources on personal use policies, to include inappropriate use; and
        - In compliance with the Federal Information Security Management Act (FISMA) of 2002; P.L. 107-347, E-Government Act of 2002 includes the FISMA: providing appropriate training to CMS employees involved in the operation or use of computer systems containing sensitive information to enhance employees' awareness of the threats and vulnerabilities of computer systems and to encourage the use of improved security practices.
    d. 5.4. – IT Infrastructure Implementation Agent or Contractor:
        - Added responsibility for testing approved software for integration into the standard CMS desktop/laptop build image; and
        - Added responsibility for implementing security controls to prevent and detect improper file sharing.

4. Section 6, Applicable Laws/Guidance:
    a. Added Privacy Act of 1974 (5 U.S.C. Section 552a, As Amended).

b. Added Federal Information Security Management Act of 2002.
c. Added Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Revised November 30, 2000.
d. Updated the date of the HHS-IRM-2004-0001 from November 23, 2004 to February 17, 2006.
e. Updated the date of Article 35 from June 9, 2004 to November 16, 2007.
f. Removed hyperlinks from applicable laws/guidance documents.

5. Section 7, Effective Dates – Added sentence indicating that this policy supersedes the previous version that was signed by the CIO on August 8, 2005.

6. Section 8, Information and Assistance – Updated the Director contact organization to the Enterprise Architecture and Strategy Group (EASG).

7. Section 9, Approved – Updated to reflect the current Chief Information Officer, Julie C. Boughn.

8. General – Reformatted document to reflect current CMS policy format.

1. PURPOSE

This document establishes a policy for acceptable and non-acceptable use of desktop/laptop and other information technology (IT) resources that are owned, leased, or controlled by the Centers for Medicare and Medicaid Services (CMS).

2. BACKGROUND

On February 17, 2006, the Department of Health and Human Services (HHS) issued the HHS Information Resources Management (IRM) Policy for Personal Use of Information Resources, which limits acceptable personal use of HHS-owned IT resources by all Departmental Operating Divisions, including the Office of the Secretary, and organizations conducting business for and on behalf of the Department through contractual relationships when using HHS IT resources. The HHS policy includes teleworking, travel, and other off-site locations, as well as all of the office locations of the Department.

The HHS-issued personal use policy builds upon previous IT resource use policies established by the Office of Management and Budget (OMB) and the President of the United States by Executive Order. The OMB Personal Use Policies and "File Sharing" Technology memorandum dated September 8, 2004, detailed specific actions that agencies must take to ensure the appropriate use of certain technologies used for file sharing across networks. Likewise, Presidential Executive Order 13103 dated September 30, 1998 established US Government policy regarding Computer Software Piracy.

As an operating division of HHS, CMS has adopted the policy and restrictions set forth by the HHS IRM policy, as well as the predecessor OMB policy and Executive Order 13103. In addition to these Government policies, CMS has established its own additional restrictions regarding acceptable and non-acceptable use of desktop/laptop and other IT resources by CMS employees, contractor personnel, interns, and other non-government personnel.

CMS has established a standard desktop/laptop computer software configuration that greatly reduces operations and maintenance costs and enhances the security of the CMS IT infrastructure by preventing the possible downloading of malicious software. In addition, this standard software configuration establishes parameters based on government and private industry standards for allowing software other than CMS-approved software to reside on CMS desktop computers and laptops.

3. SCOPE

This policy applies to the use of all CMS IT resources (e.g., desktop computers, laptops, printers, disk space storage, software, telecommunications equipment, networks, Internet, E-mail, etc.) and supporting infrastructure that is owned, leased, or controlled by CMS and used by its employees, contractors, interns, or other personnel at the Central, Regional, and Satellite office locations.

4. OPERATIONAL POLICY

4.1. Prohibited Use of CMS IT Resources

The following uses of CMS IT resources are strictly prohibited at any time by any CMS employee, contractor, or other user, unless otherwise indicated:

- Activities that are in violation of law, Government-wide rule or regulation or that are otherwise inappropriate for the workplace. This includes, but is not limited to, the following:
    - Intentional creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually-oriented materials;
    - Intentional creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal activities; and
    - Intentional creation, downloading, viewing, storage, copying, or transmission of materials related to hate speech, or that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation;
- Activities that would compromise the security of any Government host computer. This includes, but is not limited to, avoiding CMS-established security procedures and inappropriate sharing or disclosure of a person's digital authentication (log-in identification and passwords);
- Posting CMS or personal information to external newsgroups, bulletin boards, or other public forums without authority, including information that is at odds with Department and Agency missions or positions. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee or representative, unless appropriate CMS approval has been obtained;
- Establishing personal, commercial, and/or non-profit organizational web pages on CMS owned, leased, or controlled machines;
- Intentional and unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information. This includes computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked, or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data;
- Creation or use of unauthorized list servers or the distribution of unauthorized newsletters;
- Distribution of anonymous E-mail messages;
- E-mail communications to groups of employees that require CMS approval prior to distribution and have not received such approval (e.g., retirement announcements, Union notices or announcements, charitable solicitations);
- Creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter;

- Downloading and/or installing software from the Internet or other electronic sources that is freeware/shareware or non-approved software. This includes, but is not limited to, games, virus software, port scanners, vulnerability scanners, password crackers, anti-virus software, firewalls, and web browsers;
- Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (such as consulting for pay, sales or administration of business transactions, sale of goods or services);
- Engaging in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;
- Use of Peer-to-Peer software without CMS CIO approval;
- The addition of personal IT resources to existing CMS IT resources without the appropriate management authorization, including the installation of modems on CMS data lines and reconfiguration of systems;
- Use of CMS systems as a staging ground or platform to gain unauthorized access to other systems;
- Use of streaming audio and video from the Internet, unless authorized for use to accomplish CMS business; and
- Online-gaming activities.

4.2. Internet and E-Mail Usage

Internet and E-mail etiquette, customs and courtesies shall be followed by all CMS employees, contractors, and other users of CMS IT resources.

CMS Internet and E-mail resources are the property of the Agency. Any use of CMS Internet and E-mail resources is made with the understanding that such use is not secure, private or anonymous. CMS employees using CMS' Internet and E-mail resources are subject to having their activities monitored by system or security personnel without any further specific notice.

When CMS employees access the Internet using Internet addresses and domain names registered to CMS, they may be perceived by others to represent the Agency. Thus, CMS employees shall not use the Internet for any purpose, which would reflect negatively on CMS or its employees.

Official video and voice files may not be downloaded from the Internet, except when they will be used to serve an approved CMS function.

4.3. Personal Use of CMS IT Resources

CMS employees have no inherent right to employ CMS IT resources for non-government purposes, and are only granted the privilege of such use when the following conditions are met:

- Personal use involves minimal additional expense to the Agency;
- Personal use is performed on the employee's non-work time (i.e., weekends, before and after working hours or during lunch periods) and does not result in loss of employee productivity or interference with official duties;
- Personal use does not overburden (i.e., cause congestion, delay, or disruption of service to) any CMS IT resources;
- Personal use does not interfere with the mission or operations of CMS; and
- Personal use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch or the Master Labor Agreement between CMS and the American Federation of Government Employees (AFGE).

Use of CMS IT resources to accomplish work-related responsibilities will always have priority over personal use of such resources.

4.4. Unacceptable and Unlicensed Software Usage

CMS employees, contractors, and other users of CMS IT resources shall not install on any CMS computer or file server any software that lacks appropriate license. The only software authorized for use on CMS' desktop/laptop computers is that which has been purchased through the normal CMS requisition procedures or software that has been developed, evaluated, and documented in-house. Software personally-owned by a CMS employee, contractor, or other users of CMS IT resources is also prohibited from installation on CMS desktop/laptop computers or file servers, even if the person has a software license that allows the software to be installed on more than one computer at a time.

All software installed on CMS owned, leased, or controlled desktop/laptop computers that is not custom developed in-house, must have a license certificate or documented "proof of purchase" of the license. A "proof of purchase" for a license can consist of any of the following:

- Approved purchase record;
- Certified receipt or invoice;
- Validated HHS Form 393 (Purchase/Service/Stock Requisition Form);
- CMS credit card invoice;
- Vendor proof of license purchase certificate;
- Vendor end-user authorization form for volume licensing;
- Vendor-provided notice of software purchase; and
- End-user license agreement.

4.5. Monitoring of CMS IT Resource Usage

Periodically, CMS staff or contractors will be monitoring the computers and networks to ensure that no illegal software or unacceptable use of IT resources is occurring within the Agency. Unauthorized or inappropriate use of CMS IT resources by an employee, contractor, or other user could result in the loss of use or limitations on the use of such resources, disciplinary or adverse actions, criminal penalties, and/or financial liability for the cost of inappropriate use or any other action deemed appropriate by the Agency.

5. ROLES AND RESPONSIBILITIES

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

5.1. CMS Employees, Contractors, and Other Users of CMS IT Resources

CMS employees, contractors, and other users of CMS IT resources are responsible for the following activities:

- Adhering to the policy statements set forth in Section 4 of this policy document;
- Adhering to additional CMS operational policies that augment this policy (see Associated Resources Section below);
- Seeking guidance from CMS management when in doubt about the implementation of this policy; and
- Identifying and removing any illegal and unacceptable software from any desktop and/or laptop computer owned, leased, or controlled by CMS in accordance with the appropriate procedures (see Associated Resources Section below).

5.2. Office of Information Services (OIS)/Enterprise Data Center Group (EDCG)

OIS/EDCG is responsible for the following activities:

- Providing oversight and auditing of the CMS-controlled desktop/laptop and other IT resources;
- Developing and implementing operational procedures to ensure compliance with this policy (see Associated Resources Section below);
- Approving new desktop/laptop software for implementation and use;
- Establishing waiver procedures and signature files for any and all approved Peer-to-Peer software purchases and implementations that allow individual users of the Internet to connect to each other and trade files; and
- Overseeing CMS' IT Infrastructure Implementation Agent or Contractor's execution of their role in fulfilling this policy.

5.3. Office of Information Services (OIS)/Enterprise Architecture and Strategy Group (EASG)

OIS/EASG is responsible for the following activities:

- Training all CMS employees, contractors, and other users of CMS IT resources on personal use policies, to include inappropriate use; and
- In compliance with the Federal Information Security Management Act (FISMA) of 2002; P.L. 107-347, E-Government Act of 2002 includes the FISMA: providing appropriate training to CMS employees involved in the operation or use of computer systems containing sensitive information to enhance employees' awareness of the threats and vulnerabilities of computer systems and to encourage the use of improved security practices.

5.4. IT Infrastructure Implementation Agent or Contractor

CMS' IT Infrastructure Implementation Agent or Contractor is responsible for the following activities:

- Developing and implementing procedures to cover the installation, configuration, and auditing techniques used to ensure that CMS employees, contractors, and other CMS IT resource users adhere to this policy; and
- Testing approved software for integration into the standard CMS desktop/laptop build image;
- Implementing security controls to prevent and detect improper file sharing; and
- Installing, maintaining, and auditing the desktop/laptop computers and networks owned, leased, or controlled by CMS to ensure only legal and acceptable use of such resources.

6. APPLICABLE LAWS/GUIDANCE

The following laws and guidance are applicable to this policy:

- Privacy Act of 1974 (5 U.S.C. Section 552a, As Amended);
- Federal Information Security Management Act of 2002;
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Revised November 30, 2000;
- Department of Health and Human Services (HHS) Information Resources Management (IRM) Policy for Personal Use of Information Technology Resources, HHS-IRM-2004-0001, February 17, 2006;
- Office of Management and Budget (OMB) Memorandum M-04-26, Personal Use Policies and 'File Sharing' Technology, September 8, 2004;
- Standards of Ethical Conduct for Employees of the Executive Branch, United States Office of Government Ethics, September 30, 1999;

- Executive Order 13103, Computer Software Piracy, September 30, 1998, published in the NARA Federal Register, Vol. 63, No. 192, October 5, 1998; and
- Master Labor Agreement between the Centers for Medicare & Medicaid Services (CMS) and the American Federation of Government Employees, Article 35, November 16, 2007.

7. EFFECTIVE DATES

This policy becomes effective on the date that CMS' Chief Information Officer (CIO) signs it and remains in effect until officially superseded or cancelled by the CIO. This policy supersedes the previous version that was signed by the CIO on August 8, 2005.

8. INFORMATION AND ASSISTANCE

Contact the Director of the Enterprise Architecture and Strategy Group (EASG) within the Office of Information Services (OIS) for further information regarding this policy.

9. APPROVED

Julie C. Boughn
CMS Chief Information Officer and
Director, Office of Information Services

Date of Issuance

10. ASSOCIATED RESOURCES

This policy is augmented by the:

- CMS Operational Policy for Analog Line Request & Usage
- CMS Operational Policy for Disk Space Storage Management
- Procedure: Identifying and Removing Inappropriate Software
- Procedure: Identifying and Removing Unlicensed Software