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

CMS POLICY FOR WIRELESS CLIENT ACCESS

January 7, 2009

Document Number: CMS-CIO-POL-INF12-01

TABLE OF CONTENTS

1. PURPOSE

This document establishes a policy for the administration (i.e., access, configuration, management, and monitoring) of Wireless client devices using IEEE 802.11a/b/g/n protocols to access the Centers for Medicare & Medicaid Services (CMS). Other types of wireless access are not addressed in this policy.

2. BACKGROUND

CMS operates and maintains a complex computer networking infrastructure. Employees are provided with laptop computers to access this infrastructure. These laptops support IEEE 802.11 wireless connectivity which can be used to access CMS resources, by employees on travel, at contractor sites, at alternate duty stations, and at home. CMS also procures the services of contractors to administer its systems, develop and test applications, and perform other business related services. Many of these contractors use company owned wireless enabled laptops to perform these business functions.

CMS has established an Internet accessible VPN architecture which allows remote users to securely access the CMS data center infrastructure from devices attached to the Internet. This VPN architecture, used in conjunction with enforced laptop configuration standards, network protection tools, and network access controls, can be used by laptops to securely access CMS resources. This policy establishes parameters for the security of wireless access based on acceptable government and private industry standards.

The proper configuration of wireless client devices is essential for the overall security defense against unauthorized access and intrusions by preventing network attacks and penetration attempts. The review of client configuration, security, and audit logs provides CMS with a means of ensuring that a secure connection exists between the client and CMS network. Using client based and network security measures to augment wireless client configuration provides a critical second layer of defense in a wireless environment.

3. SCOPE

This policy applies to all client devices using IEEE 802.11a,b,g,n protocols, controlled and operated by CMS or its designated Agent(s) or Contractor(s) for access to the CMS Central and Regional Office infrastructure (e.g., CMS Single Site facility, Lord Baltimore Bldg, 7111 Building, and other offsite facilities), or its Enterprise Data Centers. This policy does not apply to wireless devices that do not use 802.11 type protocols; examples of such devices are Blackberries or other Personal Digital Assistants. The configuration of wireless Access Points (AP) is not covered by this policy.

This policy does not supersede any other applicable law or higher level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

4. OPERATIONAL POLICY

4.1. Wireless Client Support

CMS wireless client devices shall be accessible for configuration, management, and monitoring by CMS in accordance with established CMS Network Access Control Procedures.

4.2. Wireless Client Configuration

Wireless client laptops shall be configured in accordance with CMS Information Security policy, standards, and procedures, and at a minimum shall address the following:

- All wireless client devices accessing CMS resources shall comply with the Federal Desktop Core Configuration (FDCC);
- All wireless client devices shall be configured with anti-virus, and have current anti-virus signature files;
- All wireless client devices shall have current operating system security patches applied;
- All wireless client devices shall use host based firewall software to protect the client;
- All wireless client devices shall encrypt all data at rest on the device, using FIPS 140-2 approved encryption algorithms;
- All wireless client devices shall use the CMS VPN when accessing CMS resources;
- All wireless client devices shall be secured when not in use;
- All wireless client devices shall use two-factor authentication (e.g., User ID/password and smart card);
- Smart cards or other devices used for second factor authentication shall be kept separate from the wireless client device when not in use;
- User password complexity and frequency of change shall comply with CMS Information Security Acceptable Risk Safeguards (ARS);
- All wireless client devices shall be validated for compliance prior to being allowed to access CMS resources;
- The link between the wireless client device and the Access Point (AP) shall use encryption to the greatest extent possible. It is understood that some APs do not employ encryption; if there is a choice, then the most secure one shall be selected;
- All wireless client devices shall only use Infrastructure mode, i.e., connections to APs. Ad Hoc mode shall not be used; and
- All users of wireless client devices shall sign an agreement to adhere to appropriate CMS laptop usage standards and procedures.

4.3. Wireless Client Management & Monitoring

CMS owned laptops will be managed in accordance with standard CMS laptop management procedures. Contractor owned wireless client devices shall be managed by contractor procedures, and must meet government standards, subject to review by CMS. At a minimum, the contractors shall ensure that all devices have current operating system patch levels, current firewall software configured to CMS standards, an operating anti-virus/anti-spyware system with current anti-virus/anti-spyware signature files, and a configuration that meets OMB-7-11 guidelines as implemented by CMS.

All wireless client device logs shall be reviewed in accordance with established CMS Log Review Procedures.

All wireless client device security policies shall be reviewed and updated annually Ad hoc reviews may be necessitated by a security event, such as implementation of major enterprise computing environment modifications and any occurrence of a major information security incident.

5. ROLES AND RESPONSIBILITIES

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

5.1. Office of Information Systems (OIS)/Enterprise Data Center Group (EDCG)/Division of Operations Management (DOM) Security Personnel

The OIS/EDCG/DOM Security Personnel are responsible for the following activities:

- Providing oversight and auditing of wireless client devices;
- Providing CMS standards, procedures, and guidelines for configuration, implementation, maintenance, technical support, management, and monitoring of wireless client devices in accordance with National Institute of Standards and Technology (NIST) and National Security Agency (NSA) guidelines;
- Ensuring all wireless client device issues are addressed in an appropriate and timely manner; and
- Ensuring that controls are in place to validate all remote devices each time they attempt connection to CMS infrastructure.

5.2. CMS CITIC Contractor/EDC Contractor

CMS CITIC Contractor/EDC Contractor is responsible for the following activities:

- Providing a secure Master System Image (MSI) and appropriate security measures to provide maximum protection for CMS wireless laptops connecting to CMS infrastructure through the Internet;
- Providing appropriate network access control and network protection services to effectively check configuration of CMS or CMS contractor wireless laptops connecting to the CMS infrastructure; and
- As part of the procedures for allowing CMS contractors to remotely connect to the CMS infrastructure, include procedures for contractors to properly safeguard their laptops during wireless operations.

5.3. CMS Contractor(s)

Contractors are responsible for the following activities:

- Adhering to CMS policies, standards, and procedures for configuration and operation of devices connecting remotely to CMS infrastructure;
- Providing implementation, maintenance, technical support, management, and monitoring of contractor owned wireless client devices;
- Implementing changes (e.g., platform upgrades, device upgrades, and patches) to wireless client devices in a timely manner in accordance with the CMS Policy for the Information Security Program (PISP) and the Information Security Acceptable Risk Safeguards (ARS); and
- Reviewing and approving wireless client device audit logs, procedures, and policy changes.

5.3. CMS Employees

CMS employees are responsible for:

- Adhering to CMS policy, standards, and procedures regarding remote connectivity to CMS;
- Operating the wireless client devices in a secure manner;
- Connecting only to trusted Access Points, such as those provided by business partners or hotels at which the employees are staying;
- Reporting suspected security incidents to the CMS IT Service Desk; and
- Signing a laptop usage agreement prior to operating their Laptop from a remote location.

5.4. Contractor Employees

Contractor employees are responsible for:

- Adhering to CMS policy, standards, and procedures regarding remote connectivity to CMS;
- Maintaining secure wireless client device configurations;
- Operating the wireless client devices in a secure manner;

- Connecting only to trusted Access Points, such as those provided by business partners or hotels at which the contractor employees are staying;
- Reporting suspected security incidents to their management and to the CMS IT Service Desk; and
- Sign a CMS remote access usage agreement.

6. APPLICABLE LAWS/GUIDANCE

The following laws and/or guidance are applicable to this operational policy:

- OMB Memorandum 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- NIST FIPS 140-2, Security Requirements for Cryptographic Modules, NIST FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors;
- NIST SP 800-48, "Wireless Network Security for IEEE 802.11a.b.g and Bluetooth";
- NIST SP 800-61, "Computer Security Incident Handling Guide";
- HHS IRM Policy for IT Security for Remote Access;
- HHS Encryption Standard for Mobile Devices and Portable Media;
- HHS Rules of Behavior;
- Department of Health and Human Services (DHHS) Network and Telecommunications Security Policy;
- CMS Policy for Information Security (IS);
- CMS Policy for the Information Security Program; and
- CMS Information Security (IS) Acceptable Risk Safeguards (ARS).

7. EFFECTIVE DATES

This operational policy becomes effective on the date that CMS' CIO signs it and remains in effect until officially superseded or cancelled by the CIO.

8. INFORMATION AND ASSISTANCE

Contact the Director of the Enterprise Data Center Group (EDCG) within the Office of Information Services (OIS) for further information regarding this operational policy.

9. APPROVED

/s/ 12/30/2008

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

Date of Issuance

10. ATTACHMENTS

None.

GLOSSARY

Firewall
A firewall is a hardware or software device that is configured to permit, deny, or proxy data through the network via different levels of trust.

Wireless Client Devices
Client devices in wireless networks, also referred to as stations (STA), serve as wireless endpoint devices. They enable end users to gain access and utilize resources provided by wireless networks. Common examples are laptop computers and wireless print devices.

Access Points
An Access Point (AP) logically connects client devices to one another and provides access to a distribution system (DS), which can be an organization's enterprise wired network, or a public access point for Internet access. Wireless APs provide a mobile capability by allowing users to freely move within an AP's coverage area while maintaining connectivity between the client device and the AP.

Infrastructure Mode
In this mode, an Access Point connects Wireless Client Devices to each other, or to a distribution system. All client traffic flows through the AP; there is no direct client to client traffic.

Ad Hoc Mode
This mode does not use Access Points. Only Wireless Client Devices are involved in the communication.

IEEE 802.11a/b/g/n
A set of physical layer standards that are used to provide Wireless LAN connectivity for a variety of devices. The various letter suffixes define different radio frequencies and link rates.