DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-15-25
Baltimore, Maryland 21244-1850

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

OFFICE OF INFORMATION SERVICES

CIO DIRECTIVE 07-03

DATE: August 13, 2007

TO: CMS Centers and Office Directors
Consortia Administrators

FROM: Julie Boughn, CMS Chief Information Officer (CIO) &
Director, Office of Information Services

SUBJECT: Mandatory Encryption on all Removable Storage Devices -- ACTION

Background

Throughout the Federal government, measures are being taken to properly safeguard sensitive information, which includes Personally Identifiable Information (PII) that can be used to distinguish or trace an individual's identity. Recent news reports of lost or stolen government laptops containing unencrypted sensitive information demonstrate the potential risks and costs that can be incurred when unencrypted sensitive information is compromised. Adding to these concerns are the risks associated with removable storage devices such as external hard drives and flash/thumb drives that can store enormous amounts of data.

In an effort to properly safeguard the government's information assets while using information technology, the Office of Management and Budget (OMB) issued Memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, which requires all government agencies to implement appropriate safeguards for the protection of sensitive information. OMB M-06-16 recommends that all departments and agencies "encrypt all data on mobile computers/devices which carry data unless the data is determined to be non-sensitive." In Section 4.E.9 of the *CMS Policy for Privacy Act Implementation & Breach Notification* issued July 23, 2007, CMS requires that "All PII that is remotely stored must be encrypted in accordance with NIST Special Publication 800-53 security controls."

In response, CMS has implemented encryption software (i.e., *PointSec for PC*) on all Agency laptops. CMS has also implemented additional encryption software (i.e., *PointSec Media Encryption*, or PME) on all Agency workstations (desktop PCs and laptops) to enable staff to encrypt PII on removable storage devices and recordable media (e.g., CDs, DVDs, floppies), as well as PII that is sent via email.

Purpose

The purpose of this directive is to implement additional requirements regarding the safeguarding of sensitive information on removable storage devices and recordable media in accordance with Section 4.1.20 of the draft *CMS Policy for the Information Security Program*, Version 2.0, dated June 26, 2007.

Only CMS-issued removable storage devices may be used at CMS. No personally-owned or contractor-owned equipment is to be connected to a CMS device, unless explicitly authorized in writing by the CIO or the CIO's designated representative.

Currently, the PME software is configured to provide CMS staff with the option to encrypt files being saved to removable storage devices and/or recordable media. OIS will be modifying the PME software to force encryption on all files copied to a removable storage device that is connected to a CMS workstation. This change to the PME software will ensure all new files copied to a removable storage device get encrypted; however, all existing files on these devices will need to be manually encrypted.

CMS Business Component Leadership is expected to maintain an inventory of all removable storage devices that their business component has acquired and ensure that they can locate all devices in the inventory at any time. When a device is no longer wanted, needed, or used, a service request should be submitted through the CMS IT Service Desk to have the device decommissioned.

Timeframe

Please survey your business component and document all CMS-issued removable storage devices that are used by CMS staff, including staff located at satellite offices, using the attached "CMS Removable Storage Devices" spreadsheet template. Please submit your completed inventory spreadsheet to Doug Cincotta at doug.cincotta@cms.hhs.gov no later than **August 24, 2007**.

Upon receipt of your component's inventory spreadsheet, OIS will be scheduling time for a technician to assist your staff with encrypting all information stored on these devices.

CMS Business Component Leadership will be asked to periodically review and update their component's inventory on at least a quarterly basis. During the reviews, the location of all removable storage devices in the inventory must be confirmed.

Beginning **August 31, 2007**, the PME software will be forcing encryption on all files copied to a removable storage device that is connected to a CMS workstation, regardless of its contents.

If you have any questions or require additional information, please contact Bridget Berardino, Director, Division of Customer Liaison & Support Services, at bridget.berardino@cms.hhs.gov or 410-786-8308.

Thank you in advance for your prompt attention to this request.

Attachment
“CMS Removable Storage Devices” spreadsheet template