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

OFFICE OF INFORMATION SERVICES

CIO DIRECTIVE 07-04

DATE: August 21, 2007

TO: CMS Centers and Office Directors
Consortia Administrators

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

SUBJECT: CMS Information Security Incident Handling and Breach Analysis/Notification Procedure--ACTION

CMS has updated its Information Security Incident Handling Procedure to conform to guidance released by the Office of Management and Budget (OMB) and the Department of Health and Human Services (HHS). The updated procedure (see Attachment A) is applicable to all business conducted by CMS employees and contracted personnel. The procedure applies to contracts, agreements, and memorandums of understanding in which it is incorporated either directly or indirectly by reference. The procedure extends to all CMS business functions and processes. Examples include, but are not limited to, Medicare Contractors, Program Safeguard Contractors, Shared Systems, Quality Improvement Organizations, Quality Improvement Contractors, Medicare Advantage Contractors, Prescription Drug Plans, Medicare Call Centers, Enterprise Data Centers, Medicare Data Centers, and organizations conducting CMS-sponsored research.

CMS is an active participant in the HHS SecureOne program. Accordingly, this document adopts definitions, incident categories, reporting timeframes, and reporting templates provided by HHS SecureOne. The use of common terminology, timeframes, and reports will facilitate communication, reporting, and incident management.

Critical to the success of the *CMS Information Security Incident Handling and Breach Analysis/Notification Procedure* is the role of the CMS IT Service Desk and the Lockheed Martin Computer Security Incident Response Team (CSIRT). The CMS IT Service Desk is the focal point for all incident reporting. All system users and owners of CMS business functions and processes are to report incidents to the IT Service Desk according to the procedures described in Attachment A. Incidents are to be reported by telephone or e-mail to the CMS IT Service Desk utilizing the incident categories, reporting time criteria, and formats set forth in the procedure.

Please note that the CMS report template is changing with the release of this procedure in order to maintain alignment with HHS directives. There is one report template for incidents involving personally identifiable information (PII) and another for non-PII incidents. The CMS IT Service Desk will immediately transfer incidents to the CSIRT for further development according to the procedures set forth in the CMS *Information Security Incident Handling and Breach Analysis/Notification Procedure.*

Business Owners of the major CMS business functions, processes, and systems are key to the handling of CMS security incidents. Business Owners direct the day-to-day handling of all incidents under guidance from my office and the Center for Beneficiary Choices (for incidents involving PII).

Please ensure your familiarity with the attached procedures and the widest possible distribution of the updated procedure within each of your components, support contractors, and business partners.

Questions regarding the procedure, like the actual incidents, should be directed to the IT Service Desk by telephone at 410-786-2580 or by e-mail at cms_it_service_desk@cms.hhs.gov.

Attachment A -
CMS Information Security Incident Handling and Breach Analysis/Notification Procedure, Version 2.0, August 16, 2007