



Office of Information Services

JUN 12 2007

TO: CMS Center and Office Directors

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

SUBJECT: CIO Directive 07-01 —Transporting Sensitive Information: Encryption Requirements
for Data Leaving CMS Data Centers

As CMS is a trusted custodian of individual health care data, we must protect its most valuable assets, its information and its information systems. At CMS, we believe that putting the government's credibility at risk is not acceptable.

Effective immediately, and until further notice, no data including personally-identifiable information is to be transported from a CMS data center unless it has been encrypted. The encryption requirement may only be waived through written concurrence from the business owner of the data followed by a "wet" signature from the CIO, Deputy CIO, or the Chief Technology Officer.

The only exception to this requirement is for tapes destined for off-site storage or for the purpose of data center transitions, and that data must be shipped using proper precautions (i.e., locked in sturdy containers).

This Directive is in accordance with:

- CMS Policy for the Information Security Program (PISP) 4.10.5, **Media Transport**
"Physical, administrative, and technical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) to authorized personnel based on the sensitivity of the CMS information," and
- CMS Information Security Acceptable Risk Safeguards (ARS)
 - 1 – All sensitive information stored on digital media are protected during transport outside of controlled areas by using cryptography and tamper proof packaging and (a) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (b) if shipped, trackable with receipt by commercial carrier. If the use of cryptography is not technically feasible or the sensitive information is stored on non-digital media, written management approval (one level below the CIO) must be

obtained prior to transport and the information must be (a) hand carried using securable container via authorized personnel, or (b) if shipped, by United States Postal Service (USPS) Certified Mail with return receipt in tamper-proof packaging. Correspondence pertaining to a single individual may be mailed through regular USPS mail, but should contain the minimal amount of sensitive information in order to reduce the risk of unauthorized disclosure.

- o 2 – Activities associated with the transport of sensitive information system media are documented.
- o 3 - For systems designated as having "high" sensitivity – Employ an identified custodian at all times to transport information system media

If you have any questions or require additional information, please contact Cyndy Anderson Director, Division of IT Policies, Procedures and Audits, at Cynthia.Anderson@cms.hhs.gov or 410-786-5841.