

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C4-23-07
Baltimore, Maryland 21244-1850



CENTER FOR BENEFICIARY CHOICES

DATE: June 9, 2006

TO: All Medicare Advantage Organizations, Prescription Drug Plans, 1876 Cost Plans, 1833 Health Care Prepayment Plans, and Demonstration Projects

FROM: Abby L. Block, Director /s/

SUBJECT: Privacy and Security of Beneficiary Information

The Centers for Medicare & Medicaid Services (CMS) wants to remind all Medicare Managed Care Organizations (MCOs) and Prescription Drug Plan (PDP) Sponsors of their contractual obligation to abide by all Federal and State laws regarding confidentiality and disclosure of medical records, and other personally identifiable health information (see Article X of the Medicare Advantage Coordinated Care Plan Contract and Article IV of the Prescription Drug Plan Sponsor Contract and Article IV of the Addendum to the Medicare Managed Care Contract). As a requirement of participation in the Medicare program, compliance with the Health Insurance Portability and Accountability Act (HIPAA) is mandatory.

We further remind organizations of the necessity of effectively securing all beneficiary information, whether in paper or electronic format. This includes ensuring that data files are not saved on public or private computers when accessing corporate e-mail through the Internet, ensuring staff are properly trained to safeguard information, and ensuring electronic systems are properly programmed for beneficiary mailings. All organizations should either perform an internal risk assessment or engage an industry-recognized security expert to conduct an external risk assessment of the organization to identify and address security vulnerabilities. Weaknesses or gaps in your security program should be quick remedied. Organizations should annually train staff on responsibilities and consequences of failing to secure sensitive beneficiary information. Compliance with the HIPAA Security and Privacy rules must be documented and kept current in response to environmental or operational changes affecting the security of the electronic protected health information. In addition, plans should notify CMS immediately upon discovery of any security breach compromising beneficiary personally identifiable information.

CMS considers breaches of beneficiary security and privacy evidence of an organization's significant non-compliance with the Medicare contracts. Failure to adhere to CMS contract terms could lead to contract termination and/or the imposition of civil monetary penalties and/or intermediate sanctions.