DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop S2-26-12
Baltimore, Maryland 21244-1850

Center for Medicaid and State Operations

SMDL #06-022

September 20, 2006

Dear State Medicaid Director:

The Centers for Medicare & Medicaid Services (CMS), Center for Medicaid and State Operations, wants to remind State Medicaid systems and program staff of their obligation to abide by all Federal and State laws regarding the security and privacy of medical data and records, and of all protected health information.

The Code of Federal Regulations (at 45 CFR 95.621) provides that State agencies are responsible for the security of all automated data processing systems involved in the administration of Department of Health and Human Services' programs, and includes the establishment of a security plan that outlines how software and data security will be maintained. This section further requires that State agencies conduct a review and evaluation of physical and data security operating procedures and personnel practices on a biennial basis.

Additionally, State agencies are required by part 11 of the State Medicaid Manual to be in compliance with the security and privacy standards contained in Pub. L. 104–191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and adopted in 45 CFR Part 164, Subparts C and E, as follows: The security standards require that measures be taken to secure protected heath information that is transmitted or stored in electronic format. The privacy standards apply to protected health information that may be in electronic, oral, and paper form.

Further, State agencies are bound by the requirements in section 1902(a)(7) of the Social Security Act (the Act), as further interpreted in Federal regulations at 42 CFR 431.300 to 307. These provisions require that use or disclosure of information concerning applicants and recipients is permitted only when directly connected to administration of the State plan.

All organizations should perform either an internal risk assessment, or engage an industry recognized security expert, to conduct an external risk assessment of the organization in order to identify and address security vulnerabilities. Weaknesses or gaps in your security program should be quickly remedied. Organizations should train staff on their responsibilities, and on the consequences of failing to secure sensitive beneficiary information, as often as is required by the security requirements outlined in this letter.

The CMS considers breaches of beneficiary security and privacy to be very serious matters. Therefore, State agencies which are found to be out of compliance with the privacy or security requirements outlined in this memorandum can expect suspension or denial of Federal financial

participation for their information systems, and may be subject to other penalties under Federal and State laws and regulations.

Under the HIPAA standards, States must also require, through business associate agreements, that fiscal agent contractors and other entities that perform claims processing, third party, or other payment or reimbursement services on their behalf protect the privacy and security of protected health information. In so doing, States should ensure that their business associates update their procedures as necessitated by environmental or operational changes affecting security and privacy. In addition, these entities must also be compliant with the requirements of section 1902 (a)(7) of the Act.

As required by HIPAA rules, it is critical that each State include in all contracts a documented process to report breaches in privacy or security that compromise protected health information. The notification of a breach should immediately be reported by the contractor to State staff following the event. In addition to the above HIPAA requirements, the State, in turn, should immediately report a breach, whether discovered by its own staff or reported by a contractor, to the Director of the Division of State Systems at CMS.

In addition, all new contracts between the State and a vendor, who is responsible for handling applicant or beneficiary data, should include a section that addresses the protection of these data and identifies specific remedies to be levied against the contractor should a negligent breach occur. It is further recommended that the State examine current contract vehicles for sections addressing the safeguarding of applicant and beneficiary data, and consider amending the contracts if provisions for specific remedies do not currently exist.

Security and privacy breaches should be reported to:

Attention: Richard H. Friedman, Director
Centers for Medicare & Medicaid Systems
Center for Medicaid and State Operations
Finance, Systems and Budget Group
Division of State Systems
Room S3-13-15
7500 Security Blvd.
Baltimore, MD 21244-1850
Phone: (410) 786-4451
Fax: (410) 786-0370
E-mail: Richard.Friedman@cms.hhs.gov

I appreciate your commitment to protecting the security and privacy of our beneficiaries' health care data and personally identifiable health information.

Sincerely,

/s/

Dennis G. Smith
Director

cc:
CMS Regional Administrators

CMS Associate Regional Administrators
for Medicaid and State Operations

Martha Roherty
Director, Health Policy Unit
American Public Human Services Association

Joy Wilson
Director, Health Committee
National Conference of State Legislatures

Matt Salo
Director of Health Legislation
National Governors Association

Jacalyn Bryan Carden
Director of Policy and Programs
Association of State and Territorial Health Officials

Christie Raniszewski Herrera
Director, Health and Human Services Task Force
American Legislative Exchange Council

Lynne Flynn
Director for Health Policy
Council of State Governments