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

August 20, 2010

Dear State Medicaid Director:

This letter provides operational guidance addressing two of five findings from the Department of Health and Human Services Office of the Inspector General (OIG) audits of the Fiscal Year (FY) 2006 and FY 2007 Medicaid Payment Error Rate Measurement program (PERM). Those two audit findings from OIG address: (1) information security requirements; and (2) re-pricing claims. A third finding from the FY 2006 and FY 2007 audits, relating to reconciliation of State universe data to CMS' financial report, was addressed through revised data submission instructions and universe quality control protocols for the FY 2009 PERM measurement (75 FR 48816). This reconciliation process is also addressed in the PERM final regulation (75 FR 48816).

Information Security Requirements

Under PERM, States submit documentation that contains protected health information (PHI), which includes individually identifiable health information (IIHI), for purposes of medical reviews and data processing reviews on paid claims. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Centers for Medicare and Medicaid Services (CMS), its contractors, and States are all responsible for ensuring the security of electronic PHI (ePHI) and PHI that they maintain, transmit, disclose, or dispose. Information security requirements must safeguard against the potential breach of ePHI and PHI. CMS requires States, its contractors, and other business associates to adhere to Federal standards for the adequate encryption of PHI prior to transmission and that any passwords are sent securely and separately from the transmitted data, regardless of the method of transmission.

Under HIPAA, covered entities must ensure the secure transfer of ePHI and/or PHI contained in any data transmissions. To meet this requirement, we recommend all State data transfers containing ePHI and/or PHI be encrypted with software that is compliant with the Federal Information Processing Standards (FIPS) 140-2[1], and validated by the National Institute of Standards and Technology (NIST) module[2]. The software should also have key management,

[1] FIPS 140-2 can be found at: http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[2] NIST module can be found at: http://www.csrc.nist.gov/groups/STM/cmvp/index.html

which allows the State's system administrator to have the authority to unlock all encrypted files from the State's system. This method prevents the necessity of sharing the password with others

at the State if the State person sending the data to the contractor is unavailable to provide the key.

In the event of a breach of ePHI, PHI, or IIHI, CMS requires States, its contractors, and other business associates to adhere to the breach notification rules as mandated under the Health Information Technology for Economic and Clinical Health Act (HITECH), part of the American Recovery and Reinvestment Act (ARRA) of 2009[3].

Re-pricing of Claims

During medical reviews, claims are reviewed for accuracy of payment. As required under 42 CFR § 431.970(a)(6), States are obliged to report re-pricing information on claims that were determined during the review to have been improperly paid. In the past, the CMS Review Contractor (RC) has asked States to re-price claims determined during the review period that have been improperly paid, in order to verify the accuracy of the improper payment. However, if a State inadvertently re-prices claims incorrectly, it can affect the accuracy of the measurement. Therefore, CMS is asking States to verify the accuracy of the repriced claims.

States have the opportunity to re-price claims. When a State re-prices a claim, the State must provide documentation verifying the accuracy of the re-pricing, such as rate schedules or screen shots. If the documentation is not provided, the full amount of the claim will be found in error.

We appreciate your work with us regarding this response to the OIG recommendations and in ensuring the accuracy of PERM measurement. We look forward to continuing to work with you on this program.

Sincerely,

/s/

Deborah A. Taylor
Acting Director
Office of Financial Management

Jackie Garner
Consortia Administrator
Consortium for Medicaid and Children's Health Operations

[3] The HIPAA Breach Notification Rule, released by OCR/HHS , applies to HIPAA covered entities. This Rule may be accessed at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html. The Health Breach Notification Rule, released by the FTC, applies to non-HIPAA covered entities. This Rule may be access at: http//ftc.gov/healthbreach/.

cc:

CMS Regional Administrators

CMS Associate Regional Administrators
Division of Medicaid and Children's Health

Ann C. Kohler
NASMD Executive Director
American Public Human Services Association

Joy Wilson
Director, Health Committee
National Conference of State Legislatures

Matt Salo
Director of Health Legislation
National Governors Association

Debra Miller
Director for Health Policy
Council of State Governments

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

Barbara W. Levine
Chief, Government Relations and Legal Affairs
Association of State and Territorial Health Officials