



EXECUTIVE SUMMARY

We reviewed selected security controls and system edits for the New Jersey Medicaid Management Information System. The system adjudicates Medicaid claims submitted by health care providers. The system processed approximately \$8 billion in payments during calendar year 2007. Our review of system edits concluded that the division is not effectively monitoring certain paid claims and that change control over edit dispositions needs improvement. In addition, our review over logical security concluded that the division needs to implement formal, written security policies and procedures, and should better restrict and monitor access to confidential information.

AUDIT HIGHLIGHTS

- The division is not effectively monitoring paid claims marked for subsequent review. An analysis of data revealed that 735,000 non-pharmacy claims totaling \$157 million with at least one pay and report edit code attached to them were paid during the period June 11, 2007 to October 31, 2007. These pay and report edits were established to mark riskier claims for subsequent review; however, monitoring is not occurring on a systematic basis.
- Personally identifiable provider and recipient information is available to most NJMMIS users. Inquiries to these confidential screens are not logged and there is no way to determine whether an employee is making inappropriate inquiries to the NJMMIS.
- Written security policies and procedures for the NJMMIS have not been implemented. Our testing noted several deficiencies, the most significant being our ability to access NJMMIS user accounts of individuals who never accessed the system by utilizing a well-known user password assigned by the help desk.
- The division should strengthen control over changes to edit dispositions since changes are made directly into production by Unisys employees.

AUDITEE RESPONSE

The division did not completely concur with our recommendations (Page 11).

For the complete audit report click [here](#).