New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

Department of Human Services
Division of Medical Assistance
and Health Services
New Jersey Medicaid Management
Information System

June 11, 2007 to January 11, 2008

Richard L. Fair
State Auditor
The Honorable Jon S. Corzine
Governor of New Jersey

The Honorable Richard J. Codey
President of the Senate

The Honorable Joseph J. Roberts, Jr.
Speaker of the General Assembly

Mr. Albert Porroni
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Department of Human Services, Division of Medical Assistance and Health Services, New Jersey Medicaid Management Information System for the period of June 11, 2007 to January 11, 2008. If you would like a personal briefing, please call me at (609) 292-3700.

Richard L. Fair
State Auditor
April 24, 2008
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Objectives</td>
<td>1</td>
</tr>
<tr>
<td>Methodology</td>
<td>2</td>
</tr>
<tr>
<td>Conclusions</td>
<td>2</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>Pay and Report Edits</td>
<td>3</td>
</tr>
<tr>
<td>Edit Change Control</td>
<td>4</td>
</tr>
<tr>
<td>Security</td>
<td>7</td>
</tr>
<tr>
<td>Personally Identifiable Information</td>
<td>9</td>
</tr>
<tr>
<td>Auditee Response</td>
<td>11</td>
</tr>
</tbody>
</table>
Department of Human Services  
Division of Medical Assistance and Health Services  
New Jersey Medicaid Management Information System

**Scope**

We have completed an audit of the Department of Human Services, Division of Medical Assistance and Health Services, New Jersey Medicaid Management Information System (NJMMIS) for the period June 11, 2007 to January 11, 2008. Our audit evaluated a limited number of general and application controls involved in the system. Our tests of general controls included user authentication and authorization to provide system security. Our tests of application controls included a review of system edits to determine how edit codes are added to the system, how dispositions of these edits are changed, and how edit results are monitored.

The NJMMIS was developed to meet Federal Medicaid Management Information System guidelines and the requirements of the New Jersey Department of Human Services, Division of Medical Assistance and Health Services. The system adjudicates health care claims which are submitted by health care providers such as hospitals, pharmacies, or physicians. These claims can be submitted electronically or on paper. Unisys Corporation was awarded the current contract as the state’s fiscal agent. The contract is scheduled to end on August 23, 2008. Unisys designed, developed, implemented, and operates the NJMMIS.

**Objectives**

The objective of the audit was to determine the adequacy of selected general and application controls. These controls included user authentication and authorization to provide system security, and system edits to ensure appropriate data input, processing, and output.

This audit was conducted pursuant to the State Auditor’s responsibilities as set forth in Article VII, Section 1, Paragraph 6 of the State
Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with Governmental Auditing Standards issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by Control Objectives for Information and Related Technology issued by the Information System and Control Foundation.

In preparation for testing, we studied legislation, industry and governmental standards for computer security and operation, and policies and guidelines of the agency. Provisions we considered significant were documented and compliance with those requirements was verified by interview of agency and Unisys personnel, observation and access of the system, and through other tests we considered necessary.

A nonstatistical sampling approach was used. Our tests of general controls were designed to provide conclusions about the adequacy of those controls in place for information security planning and management. Our tests of application controls were designed to provide conclusions about the adequacy of system edit controls and monitoring. Sample transactions were judgmentally selected for testing.

Conclusions

Our review disclosed that while an awareness of the need to establish and maintain appropriate controls over NJMMIS exists, the selected general and application controls for information security planning and management, and system edit controls and monitoring require improvement.
Edits

An "edit" is a condition, set by the state, applied to a claim that determines whether the claim is ultimately paid or denied. Processed claims can be denied, paid, pended, paid and reported, generate an Explanation of Benefits, or generate a Claim Correction Form based on the edit disposition associated with the claim. Transactional data entered for processing are subject to a variety of edits for accuracy, completeness, and validity. Inadequate edits would allow for invalid or incorrect data being processed by the system. As of September 9, 2007, there were 1,140 edits that were applicable to at least one claim type.

---

Pay and Report Edits

As of September 9, 2007, there were 107 edits that were set to a disposition of pay and report. The pay and report edit marks a paid claim fitting the edit criteria so that reports can be generated by NJMMIS users to monitor claims payment activity. There is a single listing of all pay and report items generated. The listing is not a useful monitoring tool. Though some ad-hoc reporting is done, there is no systematic monitoring process for pay and report edits and the adjudicated claims associated with them.

The NJMMIS Systems Development Methodology and Standards states, "The MMIS produces reports and metrics that allow us [Unisys] and the State to review production activity regarding scheduled daily, weekly, and monthly reports to relay job production information." It lists the single pay and report edit listing as a "regularly reviewed" report.
Analysis of NJMMIS activity revealed that 735,411 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 payments represent 4.3 percent of all non-pharmacy claims paid during the period and 5.6 percent of the total dollar amount of all non-pharmacy claims paid during the period. We realize these transactions can be subject to intermittent ad-hoc review. However, there is no centralized monitoring process that ensures these riskier claims are given sufficient attention on a regular and recurring basis.

**Recommendation**

We recommend that the division review each of the pay and report edits to determine if the disposition should be changed to pay without reporting, pend, or deny future claims. For edits that should remain pay and report, the division should establish a systematic reporting process with monitoring responsibility assigned to individual staff.

---

**Edit Change Control**

The division has established the Project Request Report (PRR) process, which outlines the documentation, approval, testing, and implementation requirements for changes to the NJMMIS. For emergency changes, a streamlined procedure called Production Fix Request (PFR) had been established. Certain changes to edits, like changes to the disposition of an edit, require no coding changes and can be made directly into the production Error Text File by the Unisys’ File Maintenance Unit. The state has documented alternate procedures for making these types of changes in the NJMMIS Systems Development Methodology and Standards publication. This procedure was revised effective June 1, 2007 by the state and Unisys to better reflect the process.
that was taking place. The new policy calls for all changes to edits to follow similar steps at first. Then, changes that are not considered emergencies are instructed to follow the established PRR process. Emergency or “fast track” changes follow a separate documented procedure, different from the previous PFR process.

A test of edit changes where the disposition was changed to a less restrictive disposition type was performed. These changes were critical because they allowed claims to pay with no restriction. We defined less restrictive as a change from a non-paying to paying disposition. There were 44 changes during the time period October 1, 2003 to September 1, 2007, two of which fell under the new policy for changes to edit dispositions that went into effect on June 1, 2007. Also, there were 91 edits turned off for at least one disposition type as of September 9, 2007, the date of our sample, of which 17 were tested. All of the sampled edits turned off were done so under the policy in effect prior to June 1, 2007.

Thirty-six changes that fell under the policy in effect as of June 1, 2007 and prior and both of the changes governed by the new policy were tested for various attributes required by the respective policy. For changes under the old policy, 15 of the 36 changes (42%) tested did not have the appropriate documentation. Of the 18 changes that required additional signatures, 11 (61%) did not have signatures. Finally, 17 of the 36 changes (47%) did not use the Error Test File Form, which was required by the policy, mostly for signature acquisition. Based on the date of the change compared to the date on the documentation, 15 of the 36 changes (42%) were done within one day, qualifying them as emergency changes. Of the two changes that fell under the new policy, one did not have the required approvals, one did not use an Error Text File Form, and both were without tracking numbers.
These results lead to the following conclusions. First, the lack of compliance with the existing policy shows that those policies were either not effective or not being utilized properly to handle emergency or fast track changes. Second, the existence of alternate procedures to the standard PFR process used for emergency changes enabled standard changes to get implemented without review and analysis typically required.

We also requested explanations from the division for the 17 edits that were turned off, as well as any pre-change analysis of the impact of the change and post-change monitoring that was performed. Ten of the changes were not explained, 12 did not have any evidence of pre-change analysis, and ten did not have any evidence of post-change monitoring. Although such analysis and monitoring is not required by division policy, it is considered best practice for change control procedures. No further audit work was done to determine if any of these edits should not have been turned off, and no claim is being made to that effect.

Change control procedures are developed to prevent the implementation of incorrect or unauthorized changes to a system. Failure to comply with established procedures, or the creation of alternate procedures for similar processes could result in the improper application of an edit and erroneous payment or denial of claims.

**Recommendation**

We recommend that the division eliminate any alternate procedures for changes to edits and use the established and well-structured Project Request Report (PRR) process for all changes to edits in the NJMMIS. If a change must be made on an emergency basis, the Production Fix Request (PFR) process already established and implemented for other emergency changes should be utilized. Since there is no coding change required in the cases mentioned above, the approval phase of the change should include
analysis of the effect of the change on claims processing, and a monitoring period should be set to review the actual effect of the change and take corrective action if necessary. In addition, to ensure approval by a person with proper authority over the change, a list of authorized approvers should be developed for each functional area.

Security

The division does not maintain appropriate formal information technology security policies and procedures for the NJMMIS. Such policies help ensure that employees at every level understand how to protect data and agree to fulfill their obligations to do so. Failure to maintain such policies and procedures led to the following conditions.

We requested and received a listing of users from the security table for the NJMMIS as of August 17, 2007. We noted there were 1,038 state users suspended in the three days leading up to our receipt of the file. We learned that although the Division of Medical Assistance and Health Services (DMAHS) Help Desk had been receiving quarterly reports from Unisys regarding the number of users that have not accessed the NJMMIS in 90 and 365 days, no action was taken by DMAHS because they thought Unisys was running a batch process to remove the users automatically. When this was realized, the division suspended the 1,038 users.

When a new user is created, the help desk assigns a temporary password to the user identification. When the new user accesses the application for the first time, the new user enters their user identification and temporary password. The user is then prompted to select a new password. If the new user does not access the application, the new user identification and default password can remain indefinitely.
We were able to gain access to the NJMMIS by utilizing a well-known temporary password for four of the 12 user identifications from the August 17, 2007 listing that had never accessed the system. A follow-up listing was then obtained on November 25, 2007. We again attempted to determine whether we could access the accounts of users who had never accessed the system by utilizing the same well-known default passwords. We were able to successfully gain access in 19 of 41 attempts.

In addition, an analysis of users that had not accessed the system in over 90 days but were not suspended was completed as of August 17, 2007. We noted 54 state users and 69 Unisys users that were not suspended. Upon further review, we noted 42 users had not accessed the system in more than 365 days, but were flagged only as not accessing the system in greater than 90 days. A follow-up review was completed of the security table as of November 25, 2007. Based on the results of the query, we noted 119 state users and eight Unisys users that had not accessed the NJMMIS in over 90 days but were not suspended.

**Recommendation**

We recommend the division develop and distribute security policies and procedures which would ensure:

- all users, regardless of their agency affiliation, that have been assigned a user identification but never logged on are suspended within a specified number of days;
- passwords assigned by the help desk for new users are different or not easily guessed for all users; and
- users that have not logged into the NJMMIS in a specified number of days are suspended and then terminated from the NJMMIS.

Page 8
Personally Identifiable Information

Personal information is available on both the Provider General Information Inquiry screen and the Medicaid Base Information Inquiry screen for recipients. Provider information available includes provider name, social security number and/or tax identification number, Drug Enforcement Agency number (used to prescribe narcotics), and birth date. Recipient information available is name, social security number, address and birth date. As of August 17, 2007 there were 899 current users representing 78 percent of total users with access to the provider inquiry screen, and 1,132 current users representing 98 percent of total users who have access to the recipient inquiry screen.

Inquiries to these highly critical screens are not logged. There is no way to determine whether an employee is making inappropriate inquiries to the NJMMIS, such as accessing personally identifiable information for fraudulent purposes. When presented with this issue, division staff seemed unaware that there was no monitoring of inquiry access. Unisys was aware that there was no monitoring of this access, and claimed the control was the knowledge that if management learned of an incident involving inappropriate inquiry, the employee would be terminated for improper use of data.

The provision of access to individuals should be implemented in a manner that reduces the possibility for disclosure of confidential information. This includes monitoring of that access.
Recommendation

We recommend that the division log access to this highly personal, sensitive information and forward the logs to supervisors for review and follow up. Such review and follow up can be done on a sample basis. While we realize the undertaking will take a substantial amount of time and effort, the sensitivity of the personally identifiable information certainly demands the attention.
April 22, 2008

Stephen M. Eells
Office of Legislative Services
Office of the State Auditor
125 South Warren Street
PO Box 067
Trenton, NJ 08625-0067

Dear Mr. Eells:

This is in response to your letter of April 3, 2008 to Commissioner Velez concerning the Office of Legislative Services (OLS) draft audit report entitled “Department of Human Services, Division of Medical Assistance and Health Services, New Jersey Medicaid Management Information System.” Your letter provides an opportunity to comment on the draft audit report.

Please be advised the Division of Medical Assistance and Health Services (DMAHS) believes the draft audit report requires significant revision. A review of the available information, within the limited time allotted, indicates the draft report contains potential errors, omissions and incomplete representations of this subject. It appears there may be confusion and misunderstanding of the operations of DMAHS related to the Medicaid Management Information System (MMIS).

The auditor’s findings and the Division’s responses are provided below:

FINDING 1-Pay and Report Edits:

As of September 9, 2007, there were 107 edits that were set to a disposition of pay and report. The pay and report edit marks a paid claim fitting the edit criteria so that reports can be generated by NJMMIS users to monitor claims payment activity. There is a single listing of all pay and report items generated. The listing is not a useful monitoring tool. Though some ad-hoc reporting is done, there is no systematic monitoring process for pay and report edits and the adjudicated claims associated with them.

The NJMMIS Systems Development Methodology and Standards states, “The MMIS produces reports and metrics that allow us [Unisys] and the State to review production activity regarding scheduled daily, weekly, and monthly reports to relay job production information.” It lists the single pay and report edit listing as a “regularly reviewed” report.
Analysis of NJMMS activity revealed that 735,411 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 payments represent 4.3 percent of all non-pharmacy claims paid during the period and 5.6 percent of the total dollar amount of all non-pharmacy claims paid during the period. We realize these transactions can be subject to intermittent ad-hoc review. However, there is no centralized monitoring process that ensures these riskier claims are given sufficient attention on a regular and recurring basis.

RECOMMENDATION:

We recommend that the division review each of the pay and report edits to determine if the disposition should be changed to pay without reporting, pend, or deny future claims. For edits that should remain pay and report, the division should establish a systematic reporting process with monitoring responsibility assigned to individual staff.

DMAHS RESPONSE:

We strongly disagree with the auditor's use of the term “riskier” to classify claims that have been paid and contain one or more “pay and report” (P&R) edits, especially when used in conjunction with 735,411 claims and $157 million claims payments. There is the real possibility that a person reviewing the audit findings will incorrectly assume that the $157 million in payments is at risk and that a large portion of those payments are inappropriate and potentially eligible for recovery. If it is the intent of the auditors to provide actual dollar amounts in their findings, then we feel that these dollar amounts need to be presented by edit code with corresponding edit descriptions and explanations so that a more clear assessment of risk for these payments can be made. We believe that the 735,411 and $157 million figures, as presented, can be very misleading.

There are many reasons why an edit within the NJMMS may have a disposition of P&R other than identifying the claim as requiring post payment review by the State. Three examples include Edit codes 0978, 0611, and 0915. For the five months of claims sampled by the auditors, the total number of claims paid containing at least one of these three edits is 447,081 claims or 61% of the total number of claims paid with one or more P&R edits. The total payments on claims containing at least one of these three edits are $73,036,018 or 47% of the dollars paid on non-pharmacy claims containing one or more edits.

The findings in the audit report offer no explanation as to why a particular P&R edit might be posted to the claim other than to suggest that the payment on that claim is “riskier” than the payment made on a claim with no pay and report edits. The documentation provided below for each of the three above mentioned P&R edits clearly documents that the classification of payment on more than 61% of these claims as “risky” is inappropriate.

Example Number One- Edit Code 0978 – POSSIBLE TPL/ACCIDENT INDICATOR OR TRAUMA DIAGNOSIS

This P&R edit is posted to an incoming claim if 1) the claim contains a diagnosis code that is considered trauma related or 2) the provider has indicated on the incoming claim that the service being billed is the result of an accident.
The NJMMIS includes the capability to produce and mail trauma notices to Medicaid beneficiaries if, based on the presence of certain diagnosis codes, there might be other non-traditional coverage that might pay for the cost for the service. Non-traditional coverage would include medical coverage that might be available through an auto insurance policy or a homeowner's policy. The design of the NJMMIS was to post Edit code 978 to any incoming claim if the diagnosis information on the claim might justify the issuance of a trauma mailer to the beneficiary. Other software would check for the presence of edit code 0978 to determine if a trauma mailer was to be produced.

For the period of time audited for P&R edits, Edit code 0978 was posted to a total of 301,995 paid claims and the final payment amount on these claims is $55,346,725. This constitutes 41% of the total number of non-pharmacy claims with at least one P&R edit and 35% of the total dollars paid.

Claims containing this edit were never intended to be manually reviewed for validity of payment.

Example Number Two - Edit Code 0611 - PAYMENT EXCEEDS BILLED CHARGES/PAID CHARGES

This edit is posted to a claim if the NJMMIS determines that the charge billed by the provider is less than the maximum Medicaid rate allowance. Since Medicaid pays the lower of the amount charged by the provider or the amount of the Medicaid rate, payments to the providers in this case will be based on the lower billed charges.

This edit was developed as part of the original NJMMIS and was initially established as an "Explanation of Benefits" edit that would be reported to providers on their weekly remittance advice. We originally initiated this edit because it would be uncommon that a provider would charge less for a service than Medicaid would pay. We believed that the probable explanation for the situation when this P&R edit posted was a billing error on the part of the provider. Posting this edit was a way to alert providers that they should check their claim for accuracy. We ultimately decided to discontinue returning this edit to the provider and changed the disposition of the edit from "Explanation of Benefits" to P&R.

It was never the intent that claims failing edit code 0611 would be reviewed following payment. Rather the edit was initially designed to notify the provider of possible billing errors. Our original payment to these providers would only change if s/he detected an error and resubmitted the claim.

For the period of time audited, edit code 0611 was posted to a total of 132,879 paid claims and the final payment amount on these claims was $12,737,858. This constitutes 18% of the total number of non-pharmacy claims with at least one pay and report edit and 8% of the total dollars paid.

Example Number Three - Edit Code 0915 - MULTIPLE LTC/HOSPICE CLAIMS PROCESSED SAME MONTH AND YEAR

This edit is applicable to both claims for long term care services and claims for hospice services. Medicaid regulations require that the patient make a contribution to the cost of his/her long term care or hospice care. The NJMMIS reduces the Medicaid payment made to these providers by the amount of the patient contribution. There are situations where more than one long term care or hospice care claim is paid for the same month for the same patient. Since the patient contribution
is applied to the first claim paid for the applicable month, it is important that any other relevant claims be marked to document that the patient contribution for the month has already been satisfied based by the previous payment of a claim for the same service month. The claim is marked through the posting of edit code 0915.

It was never the intent that claims failing edit code 0915 would be reviewed following payment. Rather the edit was designed to record the appropriate reason why the payment on the claim was not reduced by the patient contribution obligation.

For the period of time audited, edit 0915 was posted to a total of 12,207 paid claims and the final payment amount on these claims is $4,951,436. This constitutes 2% of the total number of non-pharmacy claims with at least one pay and report edit and the payments on these claims represents 3% of the total dollars paid.

Additionally, the auditor was advised that P&R edits are regularly developed and implemented to support the operations of units other than data system operations. The Division assigns the responsibility for the use and maintenance of these edits to individuals in the requesting unit. The application, use and maintenance of these pay and report edits is decentralized. The auditor was offered an opportunity to review all of the specific details of any or all P&R edits to determine if the edits are appropriately applied and utilized. While the auditor is correct to state there is no centralized monitoring process, the draft audit report does not accurately reflect the use of P&R edits by DMAHS.

We have initiated a review of the procedures for implementing, using and maintaining P&R edits. Part of this review is to determine which P&R edits are no longer relevant and should be turned off or modified. The review will also consider the continued staff need for these edits. With access to our Shared Data Warehouse and Decision Support System, the staff performing a review can utilize more options than simply a hard copy report. Each unit can easily design and run their own reports.

FINDING 2-Edit Change Control:

The division has established the Project Request Report (PRR) process, which outlines the documentation, approval, testing, and implementation requirements for changes to the NJMMIS. For emergency changes, a streamlined procedure called Production Fix Request (PFR) had been established. Certain changes to edits, like changes to the disposition of an edit, require no coding changes and can be made directly into the production Error Text File by the Unisys’ File Maintenance Unit. The state has documented alternate procedures for making these types of changes in the NJMMIS Systems Development Methodology and Standards publication. This procedure was revised effective June 1, 2007 by the state and Unisys to better reflect the process that was taking place. The new policy calls for all changes to edits to follow similar steps at first. Then, changes that are not considered emergencies are instructed to follow the established PRR process. Emergency or “fast track” changes follow a separate documented procedure, different from the previous PFR process.

A test of edit changes where the disposition was changed to a less restrictive disposition type was performed. These changes were critical because they allowed claims to pay with no restriction. We defined less restrictive as a change from a non-paying to paying disposition. There were 44
changes during the time period October 1, 2003 to September 1, 2007, two of which fell under the new policy for changes to edit dispositions that went into effect on June 1, 2007. Also, there were 91 edits turned off for at least one disposition type as of September 9, 2007, the date of our sample, of which 17 were tested. All of the sampled edits turned off were done so under the policy in effect prior to June 1, 2007.

Thirty-six changes that fell under the policy in effect as of June 1, 2007 and prior and both of the changes governed by the new policy were tested for various attributes required by the respective policy. For changes under the old policy, 15 of the 36 changes (42%) tested did not have the appropriate documentation. Of the 18 changes that required additional signatures, 11 (61%) did not have signatures. Finally, 17 of the 36 changes (47%) did not use the Error Test File Form, which was required by the policy, mostly for signature acquisition. Based on the date of the change compared to the date on the documentation, 15 of the 36 changes (42%) were done within one day, qualifying them as emergency changes. Of the two changes that fell under the new policy, one did not have the required approvals, one did not use an Error Text File Form, and both were without tracking numbers.

These results lead to the following conclusions. First, the lack of compliance with the existing policy shows that those policies were either not effective or not being utilized properly to handle emergency or fast track changes. Second, the existence of alternate procedures to the standard PFR process used for emergency changes enabled standard changes to get implemented without review and analysis typically required.

We also requested explanations from the division for the 17 edits that were turned off, as well as any pre-change analysis of the impact of the change and post-change monitoring that was performed. Ten of the changes were not explained, 12 did not have any evidence of pre-change analysis, and ten did not have any evidence of post-change monitoring. Although such analysis and monitoring is not required by division policy, it is considered best practice for change control procedures. No further audit work was done to determine if any of these edits should not have been turned off, and no claim is being made to that effect.

Change control procedures are developed to prevent the implementation of incorrect or unauthorized changes to a system. Failure to comply with established procedures, or the creation of alternate procedures for similar processes could result in the improper application of an edit and erroneous payment or denial of claims.

RECOMMENDATION:

We recommend that the division eliminate any alternate procedures for changes to edits and use the established and well-structured Project Request Report (PRR) process for all changes to edits in the NJMMS. If a change must be made on an emergency basis, the Production Fix Request (PFR) process already established and implemented for other emergency changes should be utilized. Since there is no coding change required in the cases mentioned above, the approval phase of the change should include analysis of the effect of the change on claims processing, and a monitoring period should be set to review the actual effect of the change and take corrective action if necessary. In addition, to ensure approval by a person with proper authority over the change, a list of authorized approvers should be developed for each functional area.
DMAHS RESPONSE:

The audit report should clarify that the edits discussed, did not affect the payment of claims before or after being turned off. The introduction of the findings regarding edits turned off without such an explanation may mislead the reader of the audit findings to arrive at a false conclusion. There are many reasons why an edit within the NJMMIS may have an edit disposition of “off”. In some cases, “off” is assigned to the edit at the time that the edit is created because the edit is inappropriate for the claim type/media code combination. In other cases, edits are turned off based on the implementation of changes that negate the ability to continue to perform the edit.

In an effort to illustrate various reasons why an edit would have a disposition of “off”, an explanation is provided below for six edits that have been “turned off”.

**Example Number One-Edit Code 0024 – POS Reversal Rejected – Resubmit Using FD-999 Form**

This edit is posted to an incoming pharmacy Point of Service (POS) transaction intended to reverse a previously submitted claim when the matching data submitted by the provider results in the matching of the reversal transaction to two or more previously paid claims. Since the system cannot determine which claim is to be reversed, an edit is posted to deny the POS reversal request and instruct the provider to submit his/her request using the hard copy FD-999 adjustment/void request form which will require the provider to identify the specific claim to be reversed (voided) by the unique Internal Control Number.

Since only POS (HIPAA electronic) transactions are subject to this edit, the edit is turned off for all other media types.

**Example Number Two-Edit Code 0144 – Type of Service Code Invalid**

The Type of Service Code is a field that was collected from outdated claim forms. When the current claim form was designed by the Federal Government, the Type of Service Code field was removed. Since the Type of Service Code is not longer available, this edit enforcing presence and validity was turned off.

**Example Number Three-Edit Code 0221 – Provider Not Certified/Bonded at Time of Service**

Edit code 0221 was originally designed to enforce requirements for providers to be certified as a condition for payment of selected services. The changes to enforce this requirement were implemented into production in early of 1999 with Edit code 0221 being assigned a disposition of Explanation of Benefits (notice sent to provider). Before ever applying the edit, the provider certification requirements were eliminated and this edit was turned off.

**Example Number Four-Edit Code 0606 – High Variance Error**

This edit is posted to an incoming claim when the provider’s charge is more than three times the Medicaid rate allowance. This edit was initially designed to detect “gross” level coding errors on
the part of the provider. Over time it was determined in most cases there were legitimate reasons rather than billing errors generating the difference and the decision was made to turn the edit off.

Example Number Five-Edit Code 0940 – Claim Requires Review – Medicare Part A Attachment

This was meant to review the need for a hard copy attachment explaining Medicare’s involvement in the claim. The edit was posted to an incoming claim when the provider was billing Medicaid as the primary payer and the MMIS documentation indicated that Medicare should first process the claim.

This edit is turned off for HIPAA (electronic) claims since electronic claims cannot be submitted with a hard copy attachment and due to the fact that the information is covered by the HIPAA electronic transaction.

Example Number Six-Edit Code 2035 – Invalid PDP Reject Code for Part D Wraparound Benefit

This edit is posted to an incoming pharmacy point of sale (POS) claim when the claim is for a Medicare Part D covered drug that is part of Medicaid’s wraparound benefit package. The claim must be submitted to and denied by Medicare Part D. If the Medicare Part D rejection code is not a value that is recognized by our MMIS, this edit will post.

The only pharmacy transaction that supports the ability to report an NCPDP reject code is a POS (HIPAA electronic) transaction. As a result, this edit is turned off for paper claims.

Due to the above information, the benefit of a pre-change analysis and a post-change monitoring of all edits turned off appear unwarranted.

Lack of Signatures

We have modified our policy to require full signatures of staff on an approved list as authorization on the Error Text File update forms. It is important that the audit report not give the impression that the Error Text File update forms did not have authorized signatures and did not require any review and approval. The report should mention the procedures that were in place. The appropriate initials have always been deemed acceptable to indicate “signoff” approval and DMAHS does not agree that the lack of full signatures is indicative of the lack of the proper “signoff” approvals. Examples were given to DMAHS by the auditors that were cited as errors when, in fact, full signatures were obtained from State policy staff. Unfortunately, the signatures were deemed to be unacceptable because a formal list had not been developed to indicate the authorized approvers for each functional area. A few of the updates were cited as errors because there did not appear to be a signature from a State policy person. For many of these cases, additional documentation was presented to the auditor to substantiate that the change was related to a PRR and the PRR had the necessary DMAHS Senior Staff approval.

Error Text File Form Not Used

The audit report also stated that there were 17 instances in which the Error Text File Form was not used to collect the appropriate signatures. While our procedures are being altered going forward
to strictly adhere to the policy statement that this official form be used, our practice in the past has been to accept an Error Text File screen print if all of the necessary Unisys and State signoffs are included on the screen print.

The Error Text File Form itself, as well as the written documentation regarding Edit Change Control policy, are being reevaluated in order to determine if any changes should be made and to ensure that everything is in agreement.

“Alternative” Procedures

The OLS recommends that “alternate” procedures for making changes to the Error Text File be eliminated and that the existing PRR process be used for all changes to edits within the NJMMIS. We believe the use of the term “alternate” is inappropriate. Within the NJMMIS environment there are two very different sets of events that may in fact trigger an update to the Error Text File, each with its own procedure.

The first set of events involves the decision to change the disposition of an edit, change the recycle rules for an edit, change the location code for an edit, change the lay person edit message, or change the Pend Resolution instructions. There are two common denominators associated with this first set of events: 1) all of the changes can be accomplished without any changes to NJMMIS software and 2) the changes do not include any modification to the system logic or conditions which are tested when determining if the edit is to be posted. We have formal sign off procedures (which are being strengthened) for these types of changes that include signoff by State staff who are able to assess the impact of the edit change without having to go through the PRR process.

The second set of events that triggers the need for updates to the Error Text File is when a request is initiated by the State or Unisys to either change the existing logic for an edit or to develop a new edit. In either case, NJMMIS software must be modified to accomplish this change. The change to NJMMIS software is what triggers the need for a PRR and not the edit change being requested. The distinction of “emergency” changes was made for this second scenario. Changes to the Error Text File which do not require software changes are not considered emergencies.

Since the inception of the fiscal agent contract with Unisys, the State has emphasized the need to have a system that supports a very broad set of functions to allow for extensive changes to master files through online update facilities that can be accomplished without the need for software changes. This core functionality is supported through the online update capabilities to the Error Text File. Because of this, we believe a better solution is to reinforce the current process to update the Error Text File when there is no requirement for corresponding changes to NJMMIS software rather than using the PRR process.

As suggested by the OLS auditors in a meeting several months ago, the State Monitoring Unit is now receiving and reviewing the Error Text File Online Update Audit Trail on a daily basis in order to ensure that there are no changes made to the Error Text File without the State’s knowledge.
FINDING 3- Security:

The division does not maintain appropriate formal information technology security policies and procedures for the NJMMIS. Such policies help ensure that employees at every level understand how to protect data and agree to fulfill their obligations to do so. Failure to maintain such policies and procedures led to the following conditions.

We requested and received a listing of users from the security table for the NJMMIS as of August 17, 2007. We noted there were 1,038 state users suspended in the three days leading up to our receipt of the file. We learned that although the Division of Medical Assistance and Health Services (DMAHS) Help Desk had been receiving quarterly reports from Unisys regarding the number of users that have not accessed the NJMMIS in 90 and 365 days, no action was taken by DMAHS because they thought Unisys was running a batch process to remove the users automatically. When this was realized, the division suspended the 1,038 users.

When a new user is created, the help desk assigns a temporary password to the user identification. When the new user accesses the application for the first time, the new user enters their user identification and temporary password. The user is then prompted to select a new password. If the new user does not access the application, the new user identification and default password can remain indefinitely.

We were able to gain access to the NJMMIS by utilizing a well-known temporary password for four of the 12 user identifications from the August 17, 2007 listing that had never accessed the system. A follow-up listing was then obtained on November 25, 2007. We again attempted to determine whether we could access the accounts of users who had never accessed the system by utilizing the same well-known default passwords. We were able to successfully gain access in 19 of 41 attempts.

In addition, an analysis of users that had not accessed the system in over 90 days but were not suspended was completed as of August 17, 2007. We noted 54 state users and 69 Unisys users that were not suspended. Upon further review, we noted 42 users had not accessed the system in more than 365 days, but were flagged only as not accessing the system in greater than 90 days. A follow-up review was completed of the security table as of November 25, 2007. Based on the results of the query, we noted 119 state users and eight Unisys users that had not accessed the NJMMIS in over 90 days but were not suspended.

RECOMMENDATION:

We recommend the division develop and distribute security policies and procedures which would ensure:

- all users, regardless of their agency affiliation, that have been assigned a user identification but never logged on are suspended within a specified number of days;
- passwords assigned by the help desk for new users are different or not easily guessed for all users; and
- users that have not logged into the NJMMIS in a specified number of days are suspended and then terminated from the NJMMIS.
DMAHS RESPONSE:

The Division has stopped the practice of using standard passwords for MMIS accounts for Unisys staff. Unique passwords are created for each new account. This new procedure is being implemented for the State NJMMIS login IDs as well. Extensive consideration has been made as to how to implement this process with emphasis placed on communicating the password to the State user. We no longer send the passwords via email; we now phone the User directly.

We are writing a PRR so that the internet programming team can change the Helpdesk Login Administration application for Unisys and State IDs in order to automatically generate a password for every new account request as well as temporary passwords issued for the resetting of a password when a login account has been suspended due to inactivity or unsuccessful access attempts.

We have initiated another PRR to implement an automatic suspension of an account after one business day of non-use for a new or reactivated login ID issued with the temporary password. This will be done for Unisys and State NJMMIS login IDs. The User will be forced to call the Unisys help desk if s/he wants to use his/her ID after this point in time.

The Division has corrected the security reports that show the time period when the system was not accessed. The auditor found 42 users that did not access the system for more than 365 days but were only flagged for 90 days.

In response to the finding that no action was taken by the State to suspend login IDs for users that had not accessed the system in over 90 days, we have initiated a PRR to implement a process that will automatically suspend inactive IDs and to send a notice to the State for the deletion of IDs that meet the inactivity criteria.

The Division acknowledges that its security procedures and policies need to be updated, better documented, and distributed to all users. While the audit report specifically references the State, the report should clarify that Unisys does have formal written procedure manuals that address both policy and security, has a site security officer, and a site policy officer.

Both the State and Unisys require all new employees to go through formal training on both security and privacy and their responsibilities to comply with these policies.

FINDING 4-Personally Identifiable Information:

Personal information is available on both the Provider General Information Inquiry screen and the Medicaid Base Information Inquiry screen for recipients. Provider information available includes provider name, social security number and/or tax identification number, Drug Enforcement Agency number (used to prescribe narcotics), and birth date. Recipient information available is name, social security number, address and birth date. As of August 17, 2007 there were 899 current users representing 78 percent of total users with access to the provider inquiry screen, and 1,132 current users representing 98 percent of total users who have access to the recipient inquiry screen.
Inquiries to these highly critical screens are not logged. There is no way to determine whether an employee is making inappropriate inquiries to the NJMMIS, such as accessing personally identifiable information for fraudulent purposes. When presented with this issue, division staff seemed unaware that there was no monitoring of inquiry access. Unisys was aware that there was no monitoring of this access, and claimed the control was the knowledge that if management learned of an incident involving inappropriate inquiry, the employee would be terminated for improper use of data.

The provision of access to individuals should be implemented in a manner that reduces the possibility for disclosure of confidential information. This includes monitoring of that access.

RECOMMENDATION:

We recommend that the division log access to this highly personal, sensitive information and forward the logs to supervisors for review and follow up. Such review and follow up can be done on a sample basis. While we realize the undertaking will take a substantial amount of time and effort, the sensitivity of the personally identifiable information certainly demands the attention.

DMAHS RESPONSE:

We acknowledge the importance of limiting access to sensitive, personally identifiable information. Every employee must take training in the security requirements of the Health Information Portability and Accountability Act (HIPAA) covering personal health information. In addition, initial access to this data by any employee must be supervisor approved and limited to the specific duties of the employee.

The security of sensitive information is an important issue that must be considered with the associated effort and costs; the level of security achieved; the potential consequences; and the impact on operational efficiencies. The adoption of the best security procedures can not guarantee the security of sensitive information. As indicated by the auditors, the implementation of this recommendation would require substantial time and effort. This cost would be continuous as resources and staff time would be needed to monitor and maintain this function. The Division believes an overall analysis of this subject within current circumstances indicates the current security provisions are adequate. The auditor's recommendation to implement these 'best practice' procedures will be considered for future implementation should the circumstances change.

We appreciate the work performed by the auditors and the assistance in improving Division operations. All recommendations by the auditors for improvements and any identified during our review will be considered for implementation. However, revision of the draft audit report to reflect the information provided above is requested.
The courtesy and professionalism of the audit staff has been greatly appreciated. If you have any questions or require additional information, please contact me or David Lowenthal at (609) 588-7933.

Sincerely,

[Signature]

John R. Guhl
Director

JRG: L

C: Jennifer Velez
   David Lowenthal