

Board of Community Health
Audit Committee Meeting
November 9, 2006

The Board of Community Health Audit Committee met November 9, 2006, Twin Towers West, Floyd Room, 200 Piedmont Avenue, Atlanta, Georgia.

Committee members present were: Mark Oshnock, Chairman, Mary Covington, Ross Mason, and Richard Holmes.

DCH Staff available were: Carie Summers, CFO; John Hankins, Director, Internal Audit and Program Evaluation; Doug Colburn, Inspector General; Sonny Munter, CIO; Barbara Prosser, Director, MMIS; and Kim Hinton, Director of Accounting and Financial Services.

Mr. Oshnock called the meeting to order at 10:09 a.m. The October 12, 2006 minutes were UNANIMOUSLY APPROVED and ADOPTED.

Mr. Oshnock called on Carie Summers. She made preliminary remarks about the agenda and the Department's vendors who are present to talk about the SAS 70 Audit, the related follow up, reaction and response to that report from both the Department as well as ACS; the estimation report—estimation of payment errors that are used to book liabilities or receivables on the FY 06 Statement; and the Department's responses and recommendations related to the benefit payment errors.

Ms. Summers gave an overview of the FY 06 Audit. The independent auditors are expected to wrap up field work Friday, November 17. Their review staff will perform a peer review and ensure that the auditors have done everything they should do. The Department is looking for delivery of the final report by December 11. She asked Mr. Hankins to introduce the various vendors attending today's meeting.

Mr. Hankins said staff has invited BKR Metcalf Davis/Mauldin and Jenkins to the December Audit Committee meeting. He introduced Dan Klapheke and Chris Chandler of Mayer Hoffman McCann PC, and Jared Duzan and Shelley Llamas of Myers and Stauffer.

Mr. Klapheke said Mayer Hoffman McCann (MHM) has been engaged continually for three years to perform the SAS 70 audit on the MMIS. He said the period MHM would discuss is July 1, 2005 through March 31, 2006. There are seven control objectives. That report resulted in a qualification on Control Objective 3 that deals with access to computer resources and duties of the individuals who have access to certain computer resources. MHM noted that terminated individuals still had access to the system, there were incompatible duties within the organization, some employee listings that MHM requested were not complete and accurate, and the IDS system was down during periods of the SAS 70 reporting period. MHM issued an opinion and ACS responded to

that opinion to DCH. DCH engaged MHM to come back to the field to perform a SAS 70 follow up procedures. MHM was charged two tasks: to validate the response that ACS provided to the SAS 70 and to look at the issues that took place during the SAS 70 to determine if there was use of inappropriate access.

Mr. Klapheke said in order for MHM to accomplish the task, they observed procedures that were taking place after the SAS 70 period and compared those to the procedures during the SAS 70 period to see what changes had taken place and to see whether the responses that ACS provided were accurate. MHM also looked at the changes in the IDS monitoring process, reviewed firewall logs to determine if any inappropriate activity had taken place, used data mining techniques to review claims activity from December 2005 to March 2006, and compared that to the same period a year previous to that time to determine if there were any anomalies in the activity. The results of that task were MHM did not find any inappropriate claim activity. No intrusions to the system were noted through the various tests that were performed. He said MHM did note some areas that they felt that some strengthening of the internal controls could take place beyond what was responded to from the SAS 70 by ACS. Some of the areas are the monthly activities to cleanse the access list to the systems to various applications on a monthly basis. Certain procedures were performed to determine if the individuals who had access were appropriate. MHM felt that there were some areas where ACS could have gone further and made recommendations to that point. Mr. Klapheke said as it relates to the IDS, MHM confirmed that the IDS went down during a particular period within the SAS 70. What MHM noted was that ACS has since engaged an outside group to handle the monitoring of the IDS. MHM recommended that the firewall logs/server logs be maintained for a period of time (two years). MHM felt the current procedures did not provide enough history of those logs so that individuals could go back to test the logs to ensure that no inappropriate activity had taken place.

Mr. Oshnock said it appeared MHM had looked at activity, but did MHM look at process changes and determine if the changes were appropriate. Mr. Klapheke said MHM made recommendations as a result of the SAS 70 follow up procedures that they feel there are areas while changes have been made, ACS could go further to strengthen internal controls. Mr. Hankins brought to the Committee's attention a May 30 letter from ACS, a follow up report dated September 21 that Mr. Klapheke just reviewed, an October 25, 2006 letter from ACS in response to the September 21 report, and a copy of subsequent questions that the DCH CIO has asked. Mr. Oshnock asked if the Department was comfortable with the recommendation on maintaining the IDS logs for one year. Mr. Munter said the Department reviewed the procedures that ACS suggested but has not seen documentation of the procedures that Solutionary, ACS' security operations subcontractor, follows to monitor the IDS. He said ACS has agreed to submit those to the Department. Mr. Munter said the process is Solutionary reviews the IDS logs and if there are discrepancies, they immediately notify ACS Security who then notify the ACS Ravinia Security Group. DCH has asked if there are any major discrepancies, they also should contact the CIO. Mr. Munter stated that since he has not seen the procedures, he is not comfortable with the recommendation.

Mr. John Hammack, Senior Vice President and Managing Director, and Dan Frye, former Security Officer and e-Services Director, of Georgia Health Partnership, ACS Government Healthcare Solutions, introduced themselves. Mr. Hammack stated that as a result of the qualification of Control Object 3, ACS has engaged a firm that provides security services to Fortune 500 companies, strengthened their internal process, and hired a security officer who is onsite. Mr. Hammack said his presentation today would pass the industry standards and represent in a couple of areas corporate-wide initiatives related to security and privacy. Mr. Frye reviewed points that MHM recommended ACS address and follow up:

- Access Control – ACS agreed with MHM's recommendation to maintain a complete list of everyone who has access to the account—not just ACS employees but contractors and subcontractors. Mr. Frye stated that the employee list was current and they are working on the contractors list.
- Deletion of Accounts – ACS was deleting accounts as opposed to deactivating accounts. It was recommended that ACS deactivate rather than delete so that the history of that person's usage is retained. ACS agrees with that recommendation and will implement it. The only exception is ACS security wants LAN accounts deleted after 60 days.
- Intrusion Detection Enhancements – DCH has recommended that ACS initiate a temporary monitoring process until management has in place its corporate security monitoring which should be implemented by June 2007. He said one area that ACS and DCH disagree is DCH has requested that firewall logs are reviewed daily; ACS is unsure this is practical but would like to commit to reviewing monthly. ACS outsourced monitoring detection to Solutionary. Mr. Frye said since Solutionary has been on board two instances of intrusion have been detected; one was an employee attempting to use instant messaging (which is forbidden), and a server was compromised.

Mr. Frye said one area that has not been resolved is MHM recommended that IDS logs are maintained for two years. He said ACS did research with Solutionary and 90-100 days is the industry standard to maintain these logs. ACS has contracted with Solutionary to maintain the logs for one year.

Mr. Oshnock asked if everyone was comfortable that there are no other major areas that either were not reviewed and are potentially open or if once the changes are implemented these issues are finalized. Mr. Munter said that once the steps are implemented they need to be reviewed again. He said he would like to see the standards ACS is referencing that says these files should be maintained for a certain period of time and would still need to see the documentation procedures relating to Solutionary and their security review. Mr. Munter said June 2007 seems like a long time to implement the ACS corporate-wide security changes. He said the monthly reviewing of the firewalls seems to be extreme and there could be people trying to hack into the system on a daily

basis and he says he thinks there should be some flags ACS would recognize to either contact security or Secret Service to let them know that someone is attempting to crack the system.

Mr. Frye responded by saying the purpose of the firewall is to prevent this from happening. He says a daily review is not practical—maybe monthly isn't the timeframe, but daily isn't either. As far as hacking—there is no evidence in any of this work that the system or data was compromised in any way.

Mr. Oshnock asked if the SAS 70 Report indicates a more comprehensive review is necessary. Mr. Klapheke said the SAS 70 review is a review of the internal controls. The SAS 70 follow up was more robust since it looked at the actual activity that took place and went beyond what the SAS 70 does. Ms. Summers said she feels the follow up was the more robust by digging into the ACS response who had suggested that they had made corrections and then had further opportunities to provide extra information. She said that was a good starting point and allowed the Department to have confidence that it is relatively certain that the system was not compromised, and management has done the appropriate follow up and tried to make sure data was not compromised to make sure this does not happen in the future.

Mr. Mason asked if a third-party consultant could be brought in to perform some of the monitoring functions. Mr. Munter said the Department would incur expenses to do this and he would prefer ACS perform this function and supply results of their review.

Mr. Mason asked where the liability would fall if there had been an intrusion into the system. Mr. Munter said DCH as the owner of the data would have to file a HIPAA violation report and would have to work with ACS to investigate the details.

Mr. Hankins added that in FY 2006, DCH feels that particularly with the data mining MHM did, it could stand behind the financial statements. The plan that DCH has been headed toward is one SAS 70 per year, but DCH may need to consider more frequent SAS 70 work or possibly changing the reporting period.

- Firewall Log File Enhancements – Mr. Hammack said MHM's recommendation for reviewing firewall log files was monthly and not daily reviews. He said ACS would work with Mr. Munter and determine where the logical point is for that review.

Mr. Hankins asked Mr. Duzan, Project Director, and Ms. Llamas, Project Manager, of Myers and Stauffer, to give a brief review of the estimation work for the Adjustments to Fiscal Year 2006 Financial Statements for Medicaid/SCHIP Benefit Payment Errors. Mr. Duzan said this is the third time Myers and Stauffer performed the estimation work and this was the largest scope of work. This year additional analysis was done based

on the implementation of the Georgia Health Families program that occurred in June. The objective of the work was to identify payment errors for estimating State Fiscal Year 2006 total liabilities and receivables and the net of those two, and report that information to the Department to see if it would be appropriate to make adjusting journal entries for the financial statement.

Mr. Duzan said there were four groups of claims that they reviewed. Group 1 was fee-for-service claims. They looked at claims from July 2005 through March 2006. They drew up a sample of 43,000 fee-for-service claims, a stratified random sample with 16 strata. Each claim was repriced according to the Department's payments coverage policies.

Group 2 were claims related to Georgia Healthy Families (GHF). These capitation claims were paid in May for June coverage. There were approximately 600,000 claims. All claims were reviewed using a computerized algorithm review approach. Myers and Stauffer looked at paid claims to make sure they were correct and looked at claims that did not pay that should have for otherwise eligible members.

Group 3 was a fee-for-service sample during June 2006 and was very similar to Group 1 claims. Myers and Stauffer pulled a stratified random sampling of 9,010 claims for that period.

Group 4 was all other capitation claims paid for the entire fiscal year which included Georgia Better Health Care, Pre-Admission Screening Resident Review and Disease State Management programs. There were approximately 13 million claims that were paid. Again, the computerized algorithm review approach was used. In Group 4 they looked at each claim to make sure it priced correctly, was for an eligible member, and if there should have been payments made for otherwise eligible members.

Mr. Duzan said the review criteria was specific to the categories of service but there were common things they looked at for all claims: member eligibility, provider eligibility, duplicate payments, prior authorization, claims exceptions, benefits limits, claims repricing, systems corrections. Potential errors were reported to the Department to review the findings and confirm if the findings were correct. Mr. Oshnock asked what the results were.

Mr. Duzan said fee-for-service claims were combined into a single estimate. This group of claims is unique in that it used statistical techniques to extrapolate the findings of those 52,000± claims that were in the sample. The net point estimate is \$13.8 million with a \$7.5± million margin of error. Mr. Duzan said during the statistical analysis a non-random error was identified attributed to a retroactive rate change and claims had not been corrected. Because of the systematic nature of those issues, those claims were pulled out of the extrapolation. The net mispayment was about \$80,000.

Mr. Duzan said for the Group 2 claims, they found \$668,000 in mispayments (overpayments) for June primarily due to duplicate member records. Ms. Summers said

the Department has a multi-pronged corrective action plan to attempt correcting duplicate member records in several areas. Mr. Munter added that there is a project underway to review the DHR SUCCESS system. He said the Department also met with IBM to talk about Entity Analytics software to help detect duplicates early on.

In Group 3, Mr. Duzan said they also looked for claims that were the financial responsibility of the CMOs but were sent to Medicaid (fee-for-service) for payment. Myers and Stauffer found \$49,000 in claims paid as fee-for-service claims that should have been the responsibility of GHF.

In Group 4, Mr. Duzan said Myers and Stauffer found underpayments of \$231,111 and overpayments of \$184,819 with net mispayments of \$46,292.

Ms. Summers said the Department would total the four groups and reflect on the financial statements for FY 2006 in either the receivables or liabilities sections. Ms. Summers said Myers and Stauffer also reported nine observations, action items and recommendations. She asked Mr. Hankins to give a brief work plan of what the Department is doing to address these nine recommendations and errors.

1. System correction tickets – the Division of Medical Assistance is working on this item and Myers and Stauffer sent a supplemental report that shows the category of services (COS) of errors found. Medicaid program staff is reviewing each category to see if a ticket is in place and if not is there one in process.
2. Correct and/or adjust COS of retroactive rate adjustments – procedures are in place and corrections are underway.
3. Correct and/or adjust duplicate claims not requiring system correction tickets – Items 3, 4 and 5 are crucial to GHF and a work group of DCH chiefs is working on these issues.
4. Continue to review and correct member eligibility file issues – referred to DCH chiefs' work group.
5. Correct the member merge problem that DCH communicated to Myers and Stauffer on October 10 – referred to DCH chiefs' work group.
6. Continue to monitor potential FFS payments for members enrolled in the CMO program – ACS made systems changes to correct this error.
7. Update system documentation and policy manuals for co-payment policies for all COS – Myers and Stauffer was asked to give more details and provided a summary. The Division of Medical Assistance is reviewing the documentation and has contacted Systems Management when there may be need for change.

8. Continue to evaluate GHF operational observations to determine if policy changes are needed and fortify policy documentation – DCH staff is working to draft a formal policy for recoupment of capitation payments.
9. Continue to evaluate needs for reprocessing of claims with mispayments – DCH has an ongoing assessment group to determine where reprocessing is needed.

Mr. Oshnock thanked the guests for attending and making their reports. Ms. Summers asked Mr. Oshnock if he would like the Joint Venture to present to the Committee at the December meeting. Mr. Oshnock asked if the JV's report would be ready prior to the December meeting. Ms. Summers said the JV's target date is December 11 to release the report. She would contact the Committee at that time to determine if the JV's presentation is appropriate for the December or January meeting.

There being no further business, the meeting was adjourned at 11:19 a.m.

MARK OSHNOCK, CHAIRMAN
Audit Committee