To: Sandra Cardinal, Assistant Vice Chancellor, Nevada system of Higher Education

Through: Thomas Judy, Associate Vice President, Business & Finance, University of Nevada, Reno

From: Kimberli Quinn, Controller and Jean T. Regan, Chief Financial Officer, University of Nevada School of Medicine

CC: Ole J. Thienhaus, Dean and John A. McDonald, Vice President of Health Sciences, University of Nevada School of Medicine.

Date: 4/26/2010

Re: Grant Thornton Management Responses

The University of Nevada School of Medicine (UNSoM) was audited by independent auditors Grant Thornton.

The following are the Management Responses pertaining to the Multispecialty Group Practice North, Inc.; Multispecialty Group Practice South Inc.; and Nevada Family Practice Residency Program known as a whole as “MedSchool Associates”

I. Internal Control Recommendations - Significant deficiencies

Item: Reporting consistency

Internal Control Recommendation: 1

The three practice plans – MSAN, MSAS, and NFPRP - maintain their own general ledgers and generate separate internal financial statements, which are combined to form the basis for presentation as MedSchool Associates. Currently, there is no “master” general ledger account mapping to consistently classify revenue and expense amounts to the internal financial statements, and no standard reporting from the internal financial statements prepared for each practice plan into the combined statements. The result is an inconsistent classification of expenses when combining the practice plans. Creating a standard reporting format would improve consistency and transparency at the combined level, and would improve the information provided to the Board.

We also noted that for internal plan financial statements, the classification of expenses is not always consistent year to year, particularly with regard to salaries and benefits. The classification of these expenses and is modified to suit the changing needs of internal users of the information. While it may be reasonable to create special reports to suit these needs, the classification of expenses in the internal financial statement should remain consistent from period to period. Changes in classification should be made at the combined level of financial oversight and implemented at each plan.
Response: Revision of the mapping of the chart of accounts for all three entities is in the process of being done and will be completed by February 2010. The revised mapping of the chart of accounts for the separate general ledgers maintained by each of the three practice plans will result in consistent classification of revenue and expense amounts to the internal financial statements. This will enable each practice plan to present a consistent classification of revenues and expenses for the combined statements. The result will be accurate, consistent, and transparent reporting of the financial information to the Board.

Updated responses: The revised mapping of the chart of accounts for all three entities was completed 4/12/2010.

Item: Collection procedures and aged accounts

Internal Control Recommendation: 2

The year-end accounts receivable aged trial balance that was presented to us for MSAS for audit purposes indicates that a large percentage of receivables are over 120 days old. Policies and procedures in place regarding the timely collection of patient account balances had not been followed during the year. We recommend that the entity review its policies and consistently apply those already in place. The procedures over collection should include:

- The continuous review of accounts receivable for old and slow-paying accounts.
- A formal periodic review of the accounts receivable aged trial balance.
- Re-submission of amounts initially rejected for payment.
- The increased use of collection agencies to aid in collecting delinquent accounts. Increased management effort in this area can result in a reduction in the number and amount of delinquent and potentially uncollectible receivables, as well as improve cash flow and profitability.

Response: MSAS has completed a review of its policies and procedures regarding the timely collection of patient account balances. MSAS completed training on the cleanup of the patient account balances 120 day old and older. Training included review of procedures for: 1) continuous review of accounts receivables for old and slow-paying accounts; 2) a formal periodic review of the accounts receivable trial balance; 3) re-submission of amounts initially rejected for payment; and 4) the increased use of collection agencies and other outsources to aid in the collection of delinquent accounts. The review and renewed training on MSAS’s existing policies and procedures in place for the timely collection of patient account balances, especially in the four areas specified, will result in increased management effort and improved success in the reduction in number and amount of delinquent and potentially uncollectible receivables and, accordingly, expectation of improved cash flow and profitability.

Updated responses: Completed in October 2009.

Item: Reconciliation of accounts receivable

Internal Control Recommendation: 3

We noted MSAS does not reconcile its patient account receivable subsidiary ledger to the general ledger. The gross receivable is recorded with a corresponding credit to the allowance account to arrive at the net amount. This practice results in the overstatement of the accounts receivable and
allowance control accounts in the general ledger when compared to the sub-ledgers. Reconciling the subsidiary ledger to the general ledger timely serves as a check on the accuracy of the record keeping process and maintains the integrity and accuracy of system generated reports. Any differences in the reconciliation should be investigated and resolved as soon as possible. Further, this method employed by MSAS in recording its receivables and allowances are not consistent with the other reporting entities.

During our testing of accounts receivable at MSAS, we noted detailed patient accounts that did not reconcile to the subsidiary ledger. We recommend that when differences are noted between the detail and the subsidiary ledger, they be reconciled and resolved on a timely basis.

**Response:** MSAS has corrected these deficiencies. MSAS now reconciles its patient account receivable subsidiary ledger to the general ledger. MSAS no longer records the gross receivables with a corresponding credit to the allowance account. MSAS has implemented timely reconciliation of the subsidiary ledger to the general ledger as a check on the accuracy of the record keeping process and to maintain the integrity and accuracy of system generated reports. Differences in the reconciliation will be investigated and timely promptly resolved. Where detailed patient accounts receivables do not reconcile to the subsidiary ledger, MSAS now timely reconciles and resolves these differences between the detailed patient accounts and the subsidiary ledger.

**Up dated responses:** Completed in October 2009.

**Item: Segregation of duties**

**Internal Control Recommendation 4:**

Presently the various Department Heads can approve services for patients and authorize bad debt write-offs. A basic element of a strong system of internal controls ensures that incompatible duties are not assigned to one person within the organization. To strengthen internal controls, we recommend that the billing department report to the finance department and accounts to be written-off by someone separate from those involved with billing and posting cash receipts to the A/R sub-ledger should be assigned to review and approve write-offs. This could include the following positions: Director of Billing and Collections, Chief Financial Officer, Controller and Accounting Department Personnel.

We also noted that under the current system, the billers and payment posters are able to create patient accounts and register patients. Cash allocation employees have access to edit the charge entry, payment, and adjustment posting modules. We recommend segregating these duties to strengthen controls.

**Response:** Effective October 2009 the billing department reports to the finance department. Approval of bad debt account write-offs by persons involved with billing and posting cash receipts are prohibited. Write-offs will be reviewed for approval only by persons not involved in the billing and posting of cash receipts to the A/R sub-ledger. Such uninvolved persons who may approve write-offs include the following persons: Director of Billing and Collections; Chief Financial Officer; Controller; and authorized Accounting Department supervisory management personnel.

The current system lacks the capability of segregating billers and payment posters from creation of patient accounts and registration of payments. Likewise, the current system lacks the capability of segregating the duties of the cash allocation employees from the editing of charge entries, payments, and adjustments to postings. To address the recommendation the Director of Billing runs periodic random system reports to audit for inappropriate action by billers and payment posters relating to
patient accounts and registration of patients. The Director of billing will run periodic random system reports to also audit for inappropriate editions of charge entries, payments, and adjustment postings by cash allocation employees.

**Up dated responses:** Completed in October 2009.

## II. Internal Control Recommendations - Control deficiencies that are of a lesser magnitude than significant deficiencies

**Items: Journal entries**

**Recommendation 1:**
While internal control standards require that senior financial reporting personnel do not have the ability to make journal entries, certain mitigating controls could be put in place to compensate for this lack of control. We recommend that the Company maintain explanations and support for each entry and that a policy be put in place to require personnel different from those who prepare journal entries to review and approve such entries.

To improve internal controls with respect to journal entries, we suggest the Company do the following:

- Explanations and supporting documentation should be referenced for each entry, so that the purpose and support for each entry is clear to personnel who review them.
- Company policy should require that only personnel different from those who prepare journal entries should be authorized to review and approve such entries. Such review and approval should be documented by having the personnel initial the journal entries.

**Response:** This was resolved January of 2009. Senior financial reporting personnel were temporarily involved in making journal entries prior to January 2009 as a necessary function involved in the training of the person filling the position of Accounting Manager. Once training of the person who filled the position of Accounting Manager concluded prior to January 2009, no financial reporting personnel continued involvement in making journal entries. Current internal controls include references to explanations and supporting documentation showing clearly the purpose and support for each entry. Current policy requires only persons different from those who prepare journal entries are authorized to review and approve such entries. Company policy also requires the person reviewing and approving the journal entries to document such review and approval by initialing the entries.

**Up dated responses:** Completed in January 2009.

**Items: Computer applications – Use of passwords**

**Recommendation 2:**
We believe the Company should establish individual passwords for the accounting system and related modules. Users should be encouraged to understand that the integrity of passwords protects them as well as the Company. They should also understand that if several users know a particular password, the security features can become meaningless. In addition, access rights for all users should be
documented and approved by management.

We noted that password parameters are not currently enforced in MAS200 or MAS90. We recommend that prior to migrating all users onto the upgrade version of MAS200, management set strong password parameters and enforce them. We recommend that:

- all users are required to have a password (with a minimum length of 8 characters).
- users be locked out after three consecutive unsuccessful log on attempts with an invalid password.
- system locks-out the user after a period of inactivity.
- passwords are electronically forced to change at least every 90 days (30 days for users accessing files with sensitive information).
- only three grace logons be permitted after a password has expired.
- new passwords must be different from the last four passwords (approximately one year).
- passwords should be complex requiring it to contain at least one symbol, number or capital letter.

In addition, a policy should be adopted and disseminated discouraging the publication of passwords. If a password is published by an employee, the date of change for that individual’s password should be shortened to every other day and that password not be repeated for at least two years. Security policies and procedures for former employees should also be established.

**Response:** During the process of migration of MAS90 to MAS200, we will have policies and procedures in place to enforce, monitor, and secure access to our financial system. MAS200 has the capability to setup user codes and passwords. MAS200 can limit access by user, by group of defined users based upon roles definitions and relationship responsibilities, which cannot only limit access to modules within MAS200, but to menu items or company codes within the module applications. MAS200 does not have this capability to have only three grace log-ons after a password has expired. We can link with Domain Server Access to prompt password expiration which has this capability and require that when user is prompted to change login to the Domain Server that user used required to change MAS200 password as well.

We are in process of defining those roles by job position/function. With the addition of two domain servers recommend by IT for this migration and working with our outside consultants on MAS200 we will be addressing all these issues, have solutions for security issues, with policies and procedures in place, and develop a monitoring process and reporting of MAS200 access. This will be completed January 30, 2010.

**Updated response: Completed** on 2/24/2010.
Items: Computer applications – Identifying unauthorized system entry

Recommendation 3:
In reviewing the monitoring controls over the IT environment the following was noted:

- Some IT security vulnerability assessment is currently performed, but is presently limited to internal scanning only. Each practice plan network is managed day-to-day by limited IT personnel, and any erroneous or significant event could bring the entire network down, resulting in a loss of physician, staff and patient data. A security vulnerability assessment or scan should be periodically performed to identify areas of weakness that can be exploited on the network. Documentation of the scan results should be maintained, as well as the action plan/steps taken to remediate identified vulnerabilities. Any vulnerability not corrected should maintain a business reason for acceptance.

Response: We agree that security vulnerability assessment of scanning should be periodically performed. As noted, some IT security scanning is currently performed but is limited to internal scanning only on an exception basis. A complete suite of vulnerability scans including internal scanning, intrusion detection and penetration testing is needed. Due to present staffing resources and budget, we plan to continue exception reporting and submit a budget request for FY 2010-2011 to automate this process via software/hardware tools. This will save staff resources by offsetting the multiple hours needed to review security vulnerabilities and enhance security practices to be in a proactive position rather than reactive to potential security threats.

Updated response: Completed on 4/17/2010. The first periodic audit occurred on 4/17/2010, and we are addressing vulnerabilities.

Recommendation 4:
- Intrusion testing is not performed. Management should consider performing (or receiving) an external intrusion test to attempt to breach network security. Intrusion testing would provide a solution of revealing any means of unauthorized entry into the network and financial systems where malicious activity or theft of sensitive data could occur.

Response: We agree that intrusion testing is not performed, but recommend that it be done as a suite of vulnerability testing (see response above). We have assessed the external costs of acquiring these services across all practice plans at $30k to $100k and determined they are beyond the scope of the present budget. As a cost saving measure, we will plan out an internal project and submit this as a FY2010-11 budget request.

Updated response: Complete on 4/17/2010. Scans will be run monthly, and reports will be reviewed by UNR IT.

Recommendation 5:
- Audit and activity logs are available; however, not regularly reviewed. Management should establish an effective protocol to robustly monitor activity within the network devices (Cisco, SonicWall), Windows and applications (i.e. a centralized syslog tool across all practice plans). Without a tool or enforced standard to detect such activity and due to the limited resources available, any security breach would not be discovered or fixed timely causing IT
to shut down the network, resulting in a loss of money and compromise to patient and personnel data.

Response: We agree. IT grasps the importance of extensive, systematic log reviews and agrees that robust monitoring of system and access logs is a necessary best security practice. However, these reviews are staff time intensive in a time with limited staff resources. Due to limited resources we currently scan on an exception bases. IT will look at and propose software-hardware systems for log analysis for the FY2010-11 fiscal year. Estimated costs for such systems and software start around $10,000 and up. IT will research and determine the appropriate software-hardware for its environment and will submit a proposal for budget consideration.

Updated response: An SIEM appliance has been purchased to this end, and currently monitors the MAS200 system. Other servers are being migrated to use the SIEM appliance with an estimated completion date of 12/31/2011.

Items: Computer applications – Security administration

Recommendation 6:
In reviewing the IT security environment for the Practice Plans the following was noted:

MSAN

- A periodic review of network and Mysis access rights is not formally documented or occurring on a regularly scheduled basis. IT management should administer a periodic review (i.e. quarterly, semi-annually) of all existing users and their access rights within the network and Mysis to confirm assigned privileges remain appropriate and no terminated users still exist in any system. The review should be documented, approved by each department manager and IT and retained by IT.

Response: We agree. IT will promulgate an access rights review policy that stipulates the semi-annual review of all user access rights to the Mysis system. This review will be documented and distributed to the necessary individuals/departments for action and documentation purposes. IT will have the initial review by completed by May 31st, 2010 and will have a policy in place to review semi annually.

Updated response: On target for completion.

Recommendation 7:

- A periodic review of MAS 200 access rights is not formally documented or occurring on a regularly scheduled basis. Business user management should review all users and their corresponding privileges that have access to MAS 200 to validate that assigned rights remain appropriate and no terminated personnel exist in the system.
Response: We have been in process of defining those roles by job position/function. With the addition of two domain servers recommend by IT and working with our outside consultants on MAS200 we will be developing policies and procedures to monitor access rights and formally document the process with scheduled review of access rights and as well as events that require changes in corresponding privileges. This will be completed by January 31, 2010.


Recommendation 8:

- Incomplete documentation of the access rights requested and provided to users is available. An e-mail or access request form should be utilized to document all requested user access rights, as well as business and IT approval.

Response: We agree. An incomplete documentation process currently exists but will be enhanced to account for greater system controls and accountability and will be distributed to appropriate individuals and departments. This procedure will be implemented by June 30th 2010.

Updated response: On target for completion.

Recommendation 9:

- The MAS 200 administrator account and Mysis ‘root’ admin accounts are shared amongst the two respective authorized administrators. Individual MAS200 and Mysis administrator accounts should be established and used by each authorized user to provide accountability of functions performed with these high privileged accounts.

Response: We agree and will create two administrator accounts to provide accountability of functions for these accounts. This will be completed by January 31st 2010.


MSAS

Recommendation 10:

- A periodic review of network and Mysis access rights is not formally documented or occurring on a regularly scheduled basis. A regularly scheduled review of user privileges assigned to the network and Mysis should occur in conjunction with the quarterly review of terminated users to validate proper access rights exists within MSAS systems.
Response: We agree. IT will promulgate an access rights review policy that stipulates the semi-annual review of all user access rights to the Mysis system. This review will be documented and distributed to the necessary individuals/departments for action and documentation purposes. IT will have the initial review by completed by May 31st 2010 and will have a policy in place to review semi annually.

Updated response: On target for completion.

Recommendation 11:
A periodic review of MAS 90 access rights is not formally documented or occurring on a regularly scheduled basis. A regularly scheduled review of user privileges assigned to MAS 90 should occur to validate proper access rights exists within MSAS systems.

Response: As we migrate from MAS90 to MAS200 for NFPRP, we are in the process of defining those roles by job position/function. With the addition of two domain servers recommended by IT and working with our outside consultants on MAS200 we will be developing policies and procedures to monitor access rights and formally documenting the process with scheduled review of access rights and as well as events that require changes in corresponding privileges. This will be resolved January 31, 2010.

Updated response: Completed; MAS90 was decommissioned on 2/24/2010.

Recommendation 12:

- The Mysis administrator account is shared amongst the authorized administrators, which prevents individual accountability for user actions. Individual Mysis administrator accounts should be established and used by each authorized user to provide (missing words)

Response: We agree and will create two administrator accounts to provide accountability of functions for these accounts. This will be completed by January 31st 2010.

Updated response: Completed on 4/23/10

Recommendation 13:

- Two Accounts Payable staff accountants were provided MAS90 admin rights for temporary activities; however, their access was never removed and is still enabled. MAS90 administrator access should be revoked for both Accounts Payable staff accountants as they have not been trained to properly perform tasks required with such privileges and do not maintain a justified business case for receiving access.
Response: MSAS has changed the access rights for the two Accounts Payable staff accountants adjusting their access to their appropriate roles as defined in the scope of their position / job function.

Updated response: Completed; MAS90 was decommissioned on 2/24/2010.

Recommendation 14:

NFPRP

- A periodic review of network access rights is not formally documented or occurring on a regularly scheduled basis. IT should perform an ongoing review of user’s access rights to the network along with the review already performed for SoftLinks to affirm no inappropriate privileges are assigned to any system user.

Response: We agree. IT will promulgate an access rights review policy that stipulates the semi-annual review of all user access rights to the Mysis system. This review will be documented and distributed to the necessary individuals/departments for action and documentation purposes. This policy-procedure will be implemented by the end of June 2010.

Updated response: On target for completion.

Recommendation 15:

- A periodic review of MAS 90 access rights is not formally documented or occurring on a regularly scheduled basis. A regularly scheduled review of user privileges assigned to MAS 90 should occur to validate proper access rights exists within NFRPR systems.

Response: This will be completed by January 31, 2010.

Updated response: Completed; MAS90 was decommissioned on 2/24/2010.
Recommendation 16:

- Two Accounts Payable staff accountants were provided MAS90 admin rights for temporary activities; however, their access was never removed and is still enabled. MAS90 administrator access should be revoked for both Accounts Payable staff accountants as they have not been trained to properly perform tasks required with such privileges and do not maintain a justified business case for receiving access.

Response: This will be completed with the upgrade to MAS200. Completion date January 31st, 2010.

Updated response: Completed; MAS90 was decommissioned on 2/24/2010.

Items: Computer applications – IT documentation

Recommendation 17:

In reviewing IT department policies and procedures the following was noted:

- Formalized/documented policies covering MSAN security administration and NFPRP change management procedures do not currently exist.

Response: This will be completed by June 2010.

Updated response: On target for completion.

Recommendation 18:

- MSAS and NFPRP policies and procedures have been established; however, are not signed for approval or periodically reviewed and updated for appropriateness.

We recommend that IT Management perform a reassessment of all medical plan policies for appropriateness and applicability to current operations. All practice plans should follow a uniformed policy and procedural document as standard practices occur throughout the plans. Once reassessed, each policy should be signed for approval, communicated accordingly, reviewed and updated on an ongoing basis.

Response: These policies will be reviewed, updated and approved by the appropriate
individuals and departments. The formalized, signed policies will be completed and in place by June 2010.

Updated response: On target for completion.

**Items: Computer applications – NFPRP Program maintenance**

Recommendation 19:

In reviewing policy and procedures along with program maintenance documentation the following was noted:

- Tasks performed by the IT Contractor are not reviewed. Changes are not logged or tracked to document initial authorization or approvals. IT Management should implement and enforce procedures to document all change requests and track the change lifecycle from inception to migration (in a centralized software or directory). Furthermore, a periodic review of the system tasks performed by the IT Contractor should be performed for awareness and confirm only the appropriate and approved activities were performed.

Response: Completed. We agree that this finding was accurate as of the audit date in March/April, 2009. However, post audit all changes to SoftLinks were reviewed and approved by the NFPRP Steering Committee prior to being placed in to production. These changes are logged in the Steering Committee minutes.

Updated response: Completed September 2009.

Recommendation 20:

- Developer and user test results are not always documented. All testing performed for SoftLinks changes should be documented to verify testing successfully occurred, and to facilitate an effective review of the test procedures performed and the associated results. Any testing errors should be captured as well and provided to the Developer for troubleshooting.

Response: Completed. We agree that this finding was accurate as of the audit date in March/April, 2009. Post audit and as noted above, all changes are approved by the Steering Committee prior to implementation. The minutes of the Committee constitute the documentation of the change management process.

Updated response: Completed September 2009.

**III. Internal Control Recommendations – To strengthen internal control**
We recommend that the Company and those charged with governance consider the following actions.

**Items: Network and server environment**

Recommendation 1:

Currently the three practice plans – MSAN, MSAS, and NFPRP possess limited personnel resources to maintain the network and server environments. Management should maintain an adequate proportion of IT resources with organizational infrastructure to proactively monitor the network/server environment and reduce the potential for single points of failure throughout the department. Tasks performed are based on time dependency by limited IT staff, which presents the risk of the inability to attend to any irregular activity or major attack on the network. There are 99 servers across the three practice plans ran by three people; however, best practices and industry standards require no more than one IT resource to support 15 servers. Maintaining an appropriate amount of technicians to support the network and servers allows personnel to complete all essential tasks rather than performing only mission critical functions and excluding the remainder of significant activities.

**Response:** Staffing resources will be reassessed and a budget request for the FY 2010-2011 will be presented to the ICS Board for approval.

**Updated response:** On target for completion.

**Items: Network equipment**

Recommendation 2:

Currently the network equipment and resources in MSAS and NFPRP are not stored in a physically and environmentally secure location offsite from business operations. Management should consider immediately relocating the network equipment stored all facilities, but especially in the NFPRP West Charleston building to a separate location with appropriate physical and environmental safeguards. Sound best practices indicate servers and other networking resources should be maintained with adequate physical access and environmental security controls (i.e. badge access, visitor login/logout, air conditioning, controlled power, fire suppression) and reside in a separate geographic location than business operations. These measures are not currently met.

**Response:** This finding refers to the collocation project of all equipment within the Las Vegas operations regardless of practice plan. This project is foundational to all other components of audit compliance, and is scheduled for completion in Summer, 2010 contingent on available project and staffing budget.

**Updated response:** On target for completion.
Recommendation 3:

Currently an organizational chart for the NFPRP IT department does not exist. An organizational outline of the IT department should be created to display the framework and reporting structure of the department and to validate that responsibilities are separated.

Response: During the audit time, NFPRP staffing resources have changed significantly. To accommodate audit and other operational needs, a new position of Manager of Information Systems South was created and filled, with responsibilities for all technical, budget, and personnel oversight of all Las Vegas operations. An additional technician position was recruited and filled for NFPRP in Reno. An updated organization chart statewide will be provided.

Updated response: Completed. A current organizational chart is available upon request.