Grant Thornton

August 20, 2015

**Grant Thornton LLP**
757 Third Avenue, 9th Floor
New York, NY 10017

T 212.599.0100
F 212.370.4520
www.GrantThornton.com

Management and Board of Directors
Nassau Health Care Corporation:
2201 Hempstead Turnpike
East Meadow, New York 11554

Ladies and Gentlemen:

In connection with our audit of Nassau Health Care Corporation's (the "Corporation") financial statements as of December 31, 2014 and for the year then ended, auditing standards generally accepted in the United States of America ("US GAAS") require that we advise management and the board of directors (hereinafter referred to as "those charged with governance") of the following internal control matters identified during our audit.

## Our responsibilities

Our responsibility, as prescribed by US GAAS, is to plan and perform our audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether due to fraud or error. An audit includes consideration of internal control over financial reporting (hereinafter referred to as "internal control") as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Corporation's internal control. Accordingly, we express no such opinion on internal control effectiveness.

## Identified deficiencies in internal control

We identified the following internal control matters that are of sufficient importance to merit your attention. The matters discussed herein are those that we noted as of the date of our auditor's report on the financial statements (July 29, 2015), and we did not update our procedures regarding these matters since that date to the current date.

### Material weaknesses

A deficiency in internal control ("control deficiency") exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the Corporation's financial statements will not be prevented, or detected and corrected, on a timely basis.

Our consideration of internal control was not designed to identify all deficiencies in internal control that, individually or in combination, might be material weaknesses; therefore, material weaknesses may exist that were not identified. However, we consider the following identified control deficiencies to be material weaknesses.

**Effectiveness of the Financial Reporting Function**

During our audit we were informed by management that there was turnover in certain key financial management positions and that new individuals were managing the financial reporting processes. These same individuals were spending their time working to improve the financial performance of the Corporation. As a result, there has been a significant amount of lost institutional knowledge as well as competing priorities for managements' time. During the audit process, we noted that the beginning net position of the 2014 financial statements required restatement for five separate matters, the most significant of which related to third-party liabilities and the accounting for interest rate swap agreements. Due to the restatement process, there were significant delays in preparing and issuing the financial statements. Accordingly, we recommend the following in order to improve the accuracy and timeliness of the Corporation's financial reporting process:

- Establish a formal, written policy for the closing process that identifies responsible management, milestones and deadlines to ensure that the financial statements are issued on a timely basis.
- Establish formal, written policies and procedures for all aspects of the Corporation's financial reporting process (i.e. bank reconciliations, receivable valuation, etc.),
- Establish formal, written policies and procedures for reconciling month-end detail accounting records to general ledger accounts.
- Establish formal, written policies and procedures for the preparation and review of cost reports before being submitted to fiscal intermediaries.
- Establish a formal, written continuity plan to ensure that there are experienced resources available to replace key personnel in the financial reporting function in the event of employee turn-over or due to retirement.

Management's Response

We agree with the findings and have taken corrective steps to avoid the recurrence of a restatement. Specifically, NHCC has hired third party rate specialists with significant expertise in Medicare and Medicaid reimbursement matters to provide assistance with rate review and third party receivable/payable balance analysis. In addition, NHCC sent out a Request for Proposals and selected a new audit firm with significantly greater governmental accounting expertise for the 2014 audit.

Management recognizes the need to address personnel losses and is in the process of recruiting and hiring additional staff. In order to alleviate competing priorities for managements' time as noted above, a Patient Accounts Manager is being actively recruited. Management is also implementing cross-training to provide requisite redundancy for job functions. For the 2015

audit, management will work with its external auditors to establish the formal policies and procedures outlined above.

## Control deficiencies

Our consideration of internal control was also not designed to identify deficiencies in internal control that, individually or in combination, might be significant deficiencies; therefore, significant deficiencies may exist that were not identified. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

A deficiency in internal control ("control deficiency") exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis.

We identified the following control deficiencies.

Segregation of Duties within the Information Technology Environment

We noted that the CIO maintains administrator access to the Eagle financial system, although he did not log into the system throughout 2014. Users with IT management responsibilities should not retain security administrator access to key financial systems. Granting a member of IT management such access rights allows him/her to perform administrative functions (e.g., add or remove users, etc.) without proper oversight.

Additionally, the following are personnel who are not members of IT or have duties related to financial reporting that also have elevated access rights:

*Lawson:*
- Accountant I
- Accounting Assistant I

*Eagle:*
- Accounting Assistant II
- CIT - Patients Accounts Supervisor
- SNA - Admissions Officer I
- Director Financial Systems
- CIP - Manager Patient Accounts – NUMC
- CIT - Patients Accounts Supervisor

We recommend segregating responsibilities for administering critical applications or systems to individuals not functionally responsible for financial transactions and reporting. While each department should be responsible for determining which application access rights each employee should be granted, responsibility for administrating privileges should reside with IT staff and not with the functional areas or IT senior management.

If segregation of duties is not attainable, management should consider implementing mitigating controls (e.g., an activity log report of the administrators' actions reviewed by an independent party on a regular basis) to compensate for the lack of segregation around operating and security related duties.

*Management's Response:*

The elevated access to Eagle for the CIO was initially setup due to his familiarity with the system. Effective June 4th 2015 the access has since been demoted to a user level access only. During the tenure of the CIO at NUMC he did not login to Eagle or perform any administrative functions in that system.

The segregation of responsibilities exists for the Lawson system. Staff members who perform account management for Lawson are not involved with financial reporting and vice versa. The staff members who perform account management are members of the Finance department instead of IT. The Finance department has a better understanding of the data sensitivity and need for requested access. To ensure this segregation, staff members who perform financial reporting are not given access to the software required for account management.

The segregation of responsibilities also exists for the Eagle system. Eagle account management is performed by the vendor, but requested by designated IT staff only. That is because Eagle is hosted in a shared environment by the vendor and they can't give us exclusive access to account management functions. Members of the revenue cycle departments including Patient Accounts and Admissions have elevated access to the system for managing key system configurations and tables such as financial class tables, physician tables and payment schedules. They are not authorized in the vendor system to request account changes.

Shared Generic Network Accounts

We noted that nineteen generically named Network administrator accounts are shared by four IT personnel. While these accounts are used for specific services (i.e., backups, desktop management, maintenance, etc.), these accounts have elevated access.

We recommend that, in order to promote accountability for activities performed using privileged accounts, management require unique user IDs be utilized so that system activities are traceable to an individual. If system limitations require the use of these specific accounts, management should consider implementing processes that would allow identification of the individual using the shared accounts.

*Management's Response:*

We agree with the above recommendation and for that reason we have created nineteen separate service specific accounts for different automated services such as backup, patch management, antivirus etc. Instead of using the Administrator account or an individual's Administrative account across all services, designated service accounts are used for accountability and tracking. The normal practice is that the three administrators use their own accounts to troubleshoot or fix the issues. The service accounts are only used for setting up automated processes.

User Information Technology Access Reviews

We noted that the Organization does not perform a formal periodic review of the Network, Lawson, and Eagle user entitlements to ensure access changes were conducted in accordance with management's expectations.

We recommend that management perform a comprehensive review of all user entitlements for the Network and applications on a regular basis (e.g., quarterly). The review should be performed by department heads based on system reports provided by system administrators and include the following:

- Review account listings to ensure generic/group IDs are appropriate (use of such is strongly discouraged and should be minimized if to the extent possible);
- Review individual user access to ensure access is restricted to appropriate functions based on current job responsibilities; and,
- Review access to powerful privileges, system resources and administrative access to ensure access is restricted to a very limited number of authorized personnel.

The access review should be formally documented by each department head and/or data owner and evidence retained. Any identified conflicts in access rights should be followed up and resolved in a timely manner.

*Management's Response:*

All systems in the scope of this audit can only be accessed after the user logs into a PC within NUMC facilities with valid Network credentials. Also, a new process is currently in place to perform periodic account reconciliations based on the above recommendations. Lastly, there are numerous other protocols in place to restrict Network login access for users who separate from the organization or have inactivity for 30 days. These protocols limit an individual's ability to access the above mentioned applications.

Use of Live System for Testing

During our testing of patient accounts receivable, we noted numerous entries in the Eagle system designated as "Test Patients". Upon further inquiry we noted that these accounts were test accounts used to test the Eagle system. Although the amounts noted were not significant, there is a risk that using the production environment to test the system could result in accounting errors. We recommend that test accounts not be used with live files and be only used in a controlled test environment.

*Management's Response:*

NUMC does not have testing environments for all technology system and some of the testing environments have limited capability; for these reasons testing in the production system becomes necessary. Polices are being drafted to limit the use of test patients in the production system and to reverse the activity within the same accounting cycle (month) so it does not have any impact on financial reports.

* * *

The purpose of this communication is solely to describe the scope of our testing of internal control and the result of that testing, and not to provide an opinion on the effectiveness of the Company's internal control. This communication is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the Corporation's internal control. Accordingly, this communication is not suitable for any other purpose.

Very truly yours,

Grant Thornton LLP