

**GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL**

DISTRICT OF COLUMBIA

**NOT-FOR-PROFIT
HOSPITAL CORPORATION/
UNITED MEDICAL CENTER**

**Report on Internal Control and Compliance
Over Financial Reporting
for the Year Ended
September 30, 2012**



**CHARLES J. WILLOUGHBY
INSPECTOR GENERAL**

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



May 31, 2013

The Honorable Vincent C. Gray
Mayor
District of Columbia
Mayor's Correspondence Unit, Suite 316
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

The Honorable Phil Mendelson
Chairman
Council of the District of Columbia
John A. Wilson Building, Suite 504
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Dear Mayor Gray and Chairman Mendelson:

In connection with the audit of the District of Columbia's (the District) general purpose financial statements for fiscal year (FY) 2012, KPMG LLP (KPMG) submitted the enclosed report on internal control and on compliance and other matters for the Not-for-Profit Hospital Corporation, commonly known as United Medical Center (Medical Center), OIG Report No. 13-1-08HW(a). This report sets forth KPMG's comments and recommendations to improve internal control and other operating efficiencies.

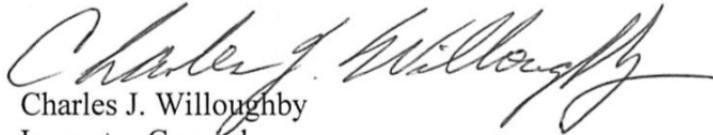
This report identifies two significant deficiencies. A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is important enough to merit attention by those charged with governance. The significant deficiencies identified in the report are: 2012-01, Management Review and Financial Reporting Preparation, and 2012-02, Lack of Access Controls Over Information Technology. Additionally, tests performed of compliance disclosed no instances of noncompliance or other matters required to be reported under *Government Auditing Standards*.

While the Office of the Inspector General will continue to assess the District's implementation of recommendations, it is the responsibility of District government management to ensure that agencies correct the deficiencies noted in audit reports. This Office will work with managers, as appropriate, to help them monitor the implementation of recommendations.

Mayor Gray and Chairman Mendelson
Not-for-Profit Hospital Corporation/United Medical Center
Report on Internal Control Over Financial Reporting
and Compliance for FY 2012
OIG No. 13-1-08HW(a) – Final Report
May 31, 2013
Page 2 of 4

If you have questions or need additional information, please contact Ronald W. King,
Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,



Charles J. Willoughby
Inspector General

Enclosure

CJW/ws

cc: See Distribution List

DISTRIBUTION:

Mr. Allen Y. Lew, City Administrator, District of Columbia (via email)
Mr. Victor L. Hoskins, Deputy Mayor for Planning and Economic Development, District of Columbia (via email)
The Honorable Kenyan McDuffie, Chairperson, Committee on Government Operations, Council of the District of Columbia (via email)
The Honorable Yvette Alexander, Chairperson, Committee on Health, Council of the District of Columbia (via email)
Mr. Brian Flowers, General Counsel to the Mayor (via email)
Mr. Christopher Murphy, Chief of Staff, Office of the Mayor (via email)
Ms. Janene Jackson, Director, Office of Policy and Legislative Affairs (via email)
Mr. Pedro Ribeiro, Director, Office of Communications, (via email)
Mr. Eric Goulet, Budget Director, Mayor's Office of Budget and Finance (1 copy)
Ms. Nyasha Smith, Secretary to the Council (1 copy and via email)
Mr. Irvin B. Nathan, Attorney General for the District of Columbia (via email)
Dr. Natwar M. Gandhi, Chief Financial Officer (1 copy and via email)
Mr. Mohamad Yusuff, Interim Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (via email)
Ms. Yolanda Branche, D.C. Auditor (1 copy)
Mr. Phillip Lattimore, Director and Chief Risk Officer, Office of Risk Management (via email)
Mr. Steve Sebastian, Managing Director, FMA, GAO, (via email)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives, Attention: Bradley Truding (via email)
The Honorable Darrell Issa, Chairman, House Committee on Oversight and Government Reform, Attention: Howie Denis (via email)
The Honorable Elijah Cummings, Ranking Member, House Committee on Oversight and Government Reform, Attention: Yvette Cravins (via email)
The Honorable Thomas Carper, Chairman, Senate Committee on Homeland Security and Governmental Affairs, Attention: Holly Idelson (via email)
The Honorable Tom Coburn, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs, Attention: Katie Bailey (via email)
The Honorable Mark Begich, Chairman, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia, Attention: Cory Turner (via email)
The Honorable Rand Paul, Ranking Member, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia (1 copy)
The Honorable Harold Rogers, Chairman, House Committee on Appropriations, Attention: Amy Cushing (via email)
The Honorable Nita Lowey, Ranking Member, House Committee on Appropriations, Attention: Laura Hogshead (via email)
The Honorable Ander Crenshaw, Chairman, House Subcommittee on Financial Services and General Government, Attention: Amy Cushing (via email)
The Honorable José E. Serrano, Ranking Member, House Subcommittee on Financial Services and General Government, Attention: Laura Hogshead (via email)

Mayor Gray and Chairman Mendelson
Not-for-Profit Hospital Corporation/United Medical Center
Report on Internal Control Over Financial Reporting
and Compliance for FY 2012
OIG No. 13-1-08HW(a) – Final Report
May 31, 2013
Page 4 of 4

The Honorable Barbara Mikulski, Chairwoman, Senate Committee on Appropriations,
Attention: Ericka Rojas (via email)
The Honorable Richard Shelby, Ranking Member, Senate Committee on Appropriations,
Attention: Dana Wade (via email)
The Honorable Frank Lautenberg, Chairman, Senate Subcommittee on Financial Services and
General Government, Attention: Marianne Upton (via email)
The Honorable Mike Johanns, Ranking Member, Senate Subcommittee on Financial Services
and General Government, Attention: Dale Cabaniss (via email)
Mr. Paul Geraty, CPA, Public Sector Audit Division KPMG LLP (1 copy)



KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*

The Board of Directors
Not-for-Profit Hospital Corporation:

We have audited the financial statements of the Not-for-Profit Hospital Corporation, commonly known as United Medical Center (the Medical Center), a component unit of the District of Columbia, as of September 30, 2012 and for the year ended September 30, 2012, and have issued our report thereon dated February 1, 2013. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

Internal Control over Financial Reporting

Management of the Medical Center is responsible for establishing and maintaining effective internal control over financial reporting. In planning and performing our audit, we considered the Medical Center's internal control over financial reporting as a basis for designing our auditing procedures 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 Medical Center's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Medical Center's internal control over financial reporting.

A deficiency in internal control over financial reporting 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 combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting that might be deficiencies, significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.

A significant deficiency is a deficiency, or combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in Attachment I to be significant deficiencies in internal control over financial reporting and are listed as items 2012-01 and 2012-02.



Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Medical Center's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

The Medical Center's responses to the matters identified in our audit are described in Attachment I. We did not audit the Medical Center's responses and, accordingly, we express no opinion on them.

This report is intended solely for the information and use of management, board of directors, others within the entity, and federal awarding agencies and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

February 1, 2013

2012-01. Management Review and Financial Reporting Preparation

Criteria

In order to comply with accounting standards and financial reporting requirements, entities need to maintain financial management systems that provide effective control over accountability for all funds, property, and other assets. In addition, the preparation of financial statements is the responsibility of management, including management's assertions that the financial statements are complete and accurate; that the rights and obligations recorded in the financial statements exist, belong to the entity, and are properly valued; and that the information presented in the financial statements is presented in accordance with generally accepted accounting principles. Pursuant to District and Federal Law, the District's Office of the Chief Financial Officer (OCFO) is directed to oversee and supervise the financial functions of the Medical Center, therefore, the financial reporting process is a collaborative effort between the OCFO and the CEO of the Medical Center.

Condition

The preparation and review of the Medical Center's financial statements is a complex task, necessarily requiring significant time and numerous coordinated processes to ensure the completeness and accuracy of the information presented therein and that the accounting conclusions and financial statement amounts are subject to appropriate review and are properly supported by written documentation. As there are many sources of information outside the accounting system, the extent of analysis over that information results in a financial reporting process that is highly complex and susceptible to errors. During the current year audit, we noted the following control exceptions related to the preparation and review of financial information and the overall financial reporting environment:

- *Account Reconciliations* – We noted that certain general ledger accounts were not appropriately reconciled to supporting documentation and certain large unsupported reconciling items were not investigated and resolved in a timely manner.
- *Management timely review of manual journal entries and their supporting documentation* – Supporting documentation for certain manual journal entries recorded was not properly maintained in order to validate the appropriateness of those journal entries. In addition, we noted that the required review of manual journal entries by someone other than the preparer was significantly delayed at different points during the fiscal year.
- *Management review of underlying data* – We noted that management placed a significant amount of reliance on information held within the general ledger system and the supporting information technology system modules without performing the necessary data checks to ensure that the information in the system generated reports was complete and accurate.
- *Communication within departments*- We noted that management had not fully implemented a formal process to facilitate timely communication between the accounting, risk management and legal departments to ensure that all potential financial exposure items are known and appropriately addressed.

Cause

The conditions noted above are the result of the following:

- Lack of formal documented accounting policies and procedures to facilitate compilation of financial information and management's precision of review; and
- Management's reliance on data output by the system without the appropriate amount of data integrity quality control checks

Effect

Certain accounting adjustments were required to ensure the Medical Center's financial statements were fairly stated as of and for the year ended September 30, 2012. Additionally, if not remediated, the control exceptions could result in a possibility of errors in financial accounting and reporting.

Recommendation

We recommend the Medical Center strengthen its financial reporting process to include certain key controls, including the following:

- Ensure that the underlying data and system generated reports used in conducting management's review of account balance activity is complete and accurate;
- Develop a process such that unsupported reconciling items are followed up on a timely manner when performing monthly and year end account reconciliations;
- Implement a process to ensure that supporting documentation is maintained for all manual journal entries recorded to the general ledger and continue proper segregation of duties such that all journal entries are reviewed timely by someone other than the preparer;
- Continue to implement a more formal process to facilitate timely communication between the accounting, risk management and legal departments of the Medical Center to ensure that all potential financial exposure items of the Medical Center are known and appropriately addressed; and
- Continue to refine management's knowledge of the computation and inputs of the Medicaid Disproportionate Share Hospital (DSH) settlement process to minimize financial take-back and/or maximize operational revenue

Views of Responsible Officials

Management has reviewed the conditions identified and recognizes the need to strengthen our internal control process related to the monthly review and financial reporting process and will institute measures to implement the proposed recommendations based on collaborative discussions with KPMG and consistent with similar healthcare organizations

2012-02. Lack of Access Controls over Information Technology

Criteria

Passwords

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009, section Identification and Authentication (IA-5) states:

“The information system, for password-based authentication:

- (a) Enforces minimum password complexity of [...organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
- (b) Enforces at least a [...organization-defined number of changed characters] when new passwords are created;
- (c) Encrypts passwords in storage and in transmission;
- (d) Enforces password minimum and maximum lifetime restrictions of [...organization defined numbers for lifetime minimum, lifetime maximum]; and
- (e) Prohibits password reuse for [[an] organization-defined number [of]] generations.”

Further, section Access Control (AC-7) states:

“The information system enforces a limit of [[an] organization-defined number [of]] consecutive invalid access attempts by a user during ... [[an] organization-defined time period]... The information system automatically [... locks the account/node for an [.. organization-defined time period] [or] delays [the] next login prompt according to [[an] organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.”

Periodic Application Access Review

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995, states:

“From time to time, it is necessary to review user account management on a system. Within the area of user access issues, such reviews may examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth.

These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis. Both kinds of reviews can be conducted by, among others, in-house systems personnel (a self-audit), the organization's internal audit staff, or external auditors. For example, a good practice is for application managers (and data owners, if different) to review all access levels of all application users every month and sign a formal access approval list, which will provide a written record of the approvals. While it may initially appear that such reviews should be conducted by systems personnel, they usually are not fully effective. System personnel can verify that users only have those accesses that their managers have specified. However because access requirements may change over time, it is important to involve the application manager, who is often the only individual in a position to know current access requirements.”

MEDITECH Vendor Access Review

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995, states:

“Effective administration of users' computer access is essential to maintaining system security. User account management focuses on identification, authentication, and access authorizations. This is augmented by the process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations.”

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009, section Access Control (AC-6) states:

“The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.”

Recommended control enhancements within this section include:

“The organization requires that users of information system accounts, or roles, with access to [for security functions defined as appropriate by the organization], use of non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.”

Condition

Passwords

During our review of the password requirements for the Medical Information Technology, Inc. (MEDITECH) Health Care Information System (HCIS), we noted the following areas in which the enforced password settings did not align with the Medical Center Password Policy:

- Password parameters for the network supporting the MEDITECH HCIS have not been configured to include complexity or account lockout requirements, and minimum length has been configured to only six characters rather than the eight character minimum outlined in the policy noted above.
- Password parameters for the MEDITECH HCIS have not been configured to include complexity, password history, or account lockout requirements and minimum length has been configured to only four characters rather than the eight character minimum outlined in the policy noted above.

Periodic Application Access Review

During our control test work over the periodic access review process for the Medical Information Technology, Inc. (MEDITECH) Health Care Information System (HCIS), we noted that the Director of IT performs an access review by which users and roles are randomly selected to be evaluated for appropriateness of access. However, the following conditions were noted to be present within this process:

- 1) The review is performed by an individual with the ability to grant or modify access for the application, rather than by an independent business owner. This combination of conflicting responsibilities represents a weakness within the control environment.

2) Since the review captures one user or role at random, it does not comprehensively cover all users possessing greater than read-only application access on a consistent time-period basis.

MEDITECH Vendor Access Review

During our fiscal year 2011 audit, we were informed by Medical Center management and representatives of the Medical Center's primary health care information system (HCIS) vendor, Medical Information Technology, Inc. (MEDITECH), that as many as over 3,000 MEDITECH employees may have write-level or greater remote access to UMC's instance of MEDITECH. The current support model from MEDITECH allows the vendor to have full access to the MEDITECH production system on an ongoing basis to support UMC's request for technical support, enhancements, changes, and to apply software updates as needed. Although MEDITECH remote user access to the HCIS was tracked in audit logs available on MEDITECH's customer portal, UMC management was not proactively reviewing the logs on a periodic basis to determine whether the vendor's remote access was authorized by the Medical Center's Information Technology department.

A review process was implemented by management during fiscal year 2012 and was documented beginning July 20, 2012 in remediation of the issue noted above. However, a deficiency in the control environment existed for the period during the year under audit of October 1, 2011 through July 19, 2012.

Cause

Passwords

Upon implementation of the Medical Center's instance of the MEDITECH HCIS, MEDITECH (the implementing vendor) did not configure password parameters for the HCIS application and database in accordance with the Medical Center Password Management Policy for password-based authentication. Management has not subsequently coordinated with MEDITECH to have the parameters updated.

Additionally, at the network and O/S levels, management has not implemented password requirements in accordance with defined policy due to limited resources in managing password resets for lost passwords and locked out accounts.

Periodic Application Access Review

During FY2011, management began performing and documenting the periodic review of access activities noted within the condition above, which it considered sufficient to mitigate the risks related unauthorized user access/activity within the HCIS.

MEDITECH Vendor Access Review

MEDITECH's customer support and security models are structured so that a large number of its employees are provided logical access to its customers' instances of the HCIS; this model was designed to provide support on a near-continuous basis.

In response to prior-year audit findings, the Medical Center implemented a proactive review of MEDITECH remote user access logs as such that this review was performed throughout FY2012. However, management did not begin fully documenting the performance of this review until the period of time noted in the condition above.

Effect

Passwords

Weakly configured password settings increase the risk that unauthorized users can access sensitive system functions, which can negatively impact the confidentiality, integrity and availability of application data.

Periodic Application Access Review

By not segregating the responsibility for performing the periodic review of access for the application from those who procedurally administer access to the MEDITECH HCIS, the potential exists that unauthorized access changes made to MEDITECH HCIS user accounts go unnoticed.

In addition, the fact that the current review covers randomly selected roles and users, there is an increased risk that all users and roles granted update privileges to the application are not reviewed over consistent periods of time.

MEDITECH Vendor Access Review

For the period of time indicated in the condition above, the risk was increased that unauthorized changes could be made to the Medical Center's instance of the MEDITECH HCIS, without detection, which could have negatively impact the confidentiality, integrity and availability of the system and data.

Recommendation

Passwords

We recommend that management reconfigure existing password configuration settings at application, the operating system, and database level, where applicable, in accordance with the Medical Center Password Management Policy, which includes requirements for enabling password complexity and requiring a password length of eight characters.

Periodic Application Access Review

We recommend that management refine the current periodic access review process to include the following characteristics, which will strength it to consistently capture and remediate, in a comprehensive manner, cases of excessive access privileges stemming from either changes in job functions or unauthorized modifications to access rights:

- The review should be comprehensive of all user IDs with greater than read-only privileges to the application, which is performed quarterly or semi-annually depending on considerations such as the volume of user access and likelihood of changes, the operation and strength of access controls around provisioning, de-provisioning, and management of changes for transfers, and the relative risk of the system with respect to operational and financial importance to the company.
- The review should be conducted by business owners that are knowledgeable and can certify appropriateness of user access within the system and who do not also have access to modify users and privileges.
- The review should be based upon system-generated reports, even if these reports are re-formatted into Excel to facilitate the review process.

- The required changes resulting from the review should be remediated within one week of the required change being identified.
- The results of the review, including the original review access reports reviewed and management's requested changes and sign-off of the review, should be documented for audit trail purposes.

MEDITECH Vendor Access Review

While we consider this condition to be remediated, we recommend that UMC IT enable the configuration within their Help Desk workflow to log the specific individual on the Help Desk staff who has completed the review of MEDITECH remote access for the date in question.

Views of Responsible Officials

Passwords

Management will extend the minimum length required to 8 characters for passwords. Passwords must be alpha numeric and will remain encrypted when entering. After 3 consecutive failed login attempts, the system will continue to timeout for 60 seconds before allowing user to attempt to sign into the system again. Users must change password upon expiration. System does not allow use of same password with change. Policies will be updated to reflect changes.

Parameter changes will go in affect as of February 1, 2013.

Periodic Application Access Review

- Management shares and agrees with the need for the monitoring of user access.
- Management shall provide business owners access list for the roles for their areas to review and sign off on for appropriateness.
- Business owners (Managers, Supervisors and Department Heads) will review and either approve or modify access to users during semi-annual reviews.
- Identified changes will be made to access within one week of the review as recommended when possible.
- Management will work with key stake holders to review, modify and sign off on identified roles and access for their areas. Management will also assist business /data owners with defining their process for auditing.

MEDITECH Vendor Access Review

Last year's audit by KPMG informed Management that the Medical Center must show documented evidence of monitoring remote activity by Meditech. Management immediately instituted a workflow that captured monitoring, and documents were provided to auditors upon request. Subsequently, Management was later informed that documentation must show that review was performed by Management. This additional request was also implemented by modifying the daily helpdesk log so that Management will check off when their review has been performed. The effective date for this was January 2013