



**AUDIT DEPARTMENT**

**UNIVERSITY MEDICAL CENTER OF SOUTHERN NEVADA  
HIPAA COMPLIANCE**

**for the period May 17, 2010 through October 7, 2010**

**JEREMIAH P. CARROLL II, CPA**  
Audit Director



# Audit Department

500 S Grand Central Pky Ste 5006 • PO Box 551120 • Las Vegas NV 89155-1120  
(702) 455-3269 • Fax (702) 455-3893

Jeremiah P. Carroll II, CPA, Director



March 31, 2011

Mr. Don Burnette  
County Manager  
500 S. Grand Central Parkway, 6<sup>th</sup> Floor  
Las Vegas, Nevada 89106

Dear Mr. Burnette:

In accordance with our annual audit plan, we conducted a review of HIPAA Compliance at University Medical Center. Our procedures included observations and interviews for the period May 17, 2010, through October 7, 2010.

The objectives of this audit were to determine employees' level of awareness and understanding of UMC's privacy policies and their use of appropriate safeguards in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Our criteria were based on 24 types of observations and specific questions for employees in three main HIPAA areas:

- Notice of Privacy Practices (NPP) and Patient's Rights
- Privacy and Security Policies and Procedures, and
- Safeguard Practices

The results of our evaluation showed an overall compliance rating of 93% for the 27 departments included in this review. Eight departments merited a "HIPAA-Star" in recognition of 100% compliance ratings. Another fifteen departments (56%) scored 90% or higher compliance. The compliance rates for the remaining 4 units (14%) ranged from 64% to 89% compliance.

A draft report was provided to the Chief Executive Officer of UMC, and a response has been received. The assistance and cooperation of UMC's staff is sincerely appreciated.

Sincerely,

/s/ Jeremiah P. Carroll II, CPA

Jeremiah P. Carroll II, CPA  
Audit Director

## TABLE OF CONTENTS

<b>BACKGROUND .....</b>	<b>1</b>
<b>OBJECTIVES, SCOPE, AND METHODOLOGY .....</b>	<b>2</b>
<b>RESULTS IN BRIEF .....</b>	<b>2</b>
<b>DETAIL OF FINDINGS .....</b>	<b>3</b>
<b>Knowledge of Privacy Policies and Assigned Responsibilities .....</b>	<b>3</b>
<b>Compliance to Safeguard Policies .....</b>	<b>5</b>
<b>Inconsistent Disclosure Recording Procedures.....</b>	<b>6</b>
<b>Follow Up to Prior Findings .....</b>	<b>7</b>
<b>APPENDIX A .....</b>	<b>8</b>
<b>Management’s Response.....</b>	<b>8</b>

# **CORPORATE COMPLIANCE, HIPAA AND INTERNAL AUDIT**

## **HIPAA COMPLIANCE REVIEW**

**For the period May 2010 through October 2010**

### **BACKGROUND**

In accordance with our annual audit plan, we conducted a review of HIPAA Compliance at University Medical Center (UMC). Due to the number of departments within the UMC organization, our audit plan was structured to review one third of the departments each year, randomly selected by division, ensuring that all departments are reviewed over the course of a three year period. A summary report is issued to management annually, and this report is the third of the three year plan.

As a healthcare provider who conducts standard electronic transactions, UMC must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In 2003, UMC developed and implemented several administrative policies to comply with the HIPAA Privacy Rule. Additional policies were implemented in 2005 to comply with the HIPAA Security Rule, and in 2010 to comply with the data breach notification rule added to HIPAA in August 2009.

HIPAA-related functions vary between departments to some extent and overlap in some areas. Consequently, organizational procedures were developed where feasible and attached to the applicable administrative policy. Additionally, each department manager is expected to have procedures specific to its operations, when necessary. For example, the Patient Care Services division adopted a manual log to record disclosures during a hospital stay and assigned recording responsibilities to the office technicians at discharge.

Tools are in place to assist employees with compliance. For example; the HIPAA Compliance Questionnaire Screen program was added to communicate patient privacy requests, the HIPAASafe program was added to provide a centralized method to document certain disclosures required by the Privacy Rule, and guidance documents are available on the hospital's intranet for all users to access. All members of UMC's workforce are required to complete awareness training. Self-study and classroom programs are offered, and a summary of policies and safeguards is issued as part of the UMC Orientation program. Annual refresher training programs are also required for all employees and volunteers.

UMC policies require all members of its workforce to adhere to certain requirements:

- Administrative safeguards; i.e., complete initial HIPAA awareness training during orientation and annual refresher training, access protected health information (PHI) only for a legitimate business reason, and know how to assist patients with privacy requests and report violations.
- Physical safeguards; i.e., all papers or media containing PHI must be shredded or placed into a secured shredding bin for destruction, do not place any PHI in public view.
- Technical safeguards; i.e., log off workstations, do not share passwords, and do not transmit PHI without encryption.

## OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this audit were to determine employees' level of awareness and understanding of UMC's privacy policies and their use of appropriate safeguards in accordance with HIPAA. Our criteria were based on 24 types of observations and specific questions for employees in three main HIPAA areas:

- Notice of Privacy Practices (NPP) and Patient's Rights
- Privacy and Security Policies and Procedures
- Safeguard Practices

For example, observations included whether the NPP is issued to patients, whether papers containing PHI are disposed of properly, whether specific procedures have been implemented as required, and if computers are locked when not in use. Additionally, we followed up on findings identified in prior reviews.

To accomplish our objectives, we interviewed appropriate personnel, reviewed policies and procedures, and conducted observation rounds in 27 departments of UMC. Departments surveyed included 12 clinical or direct patient contact units, 4 ambulatory care units, and 11 non-direct patient care support service units.

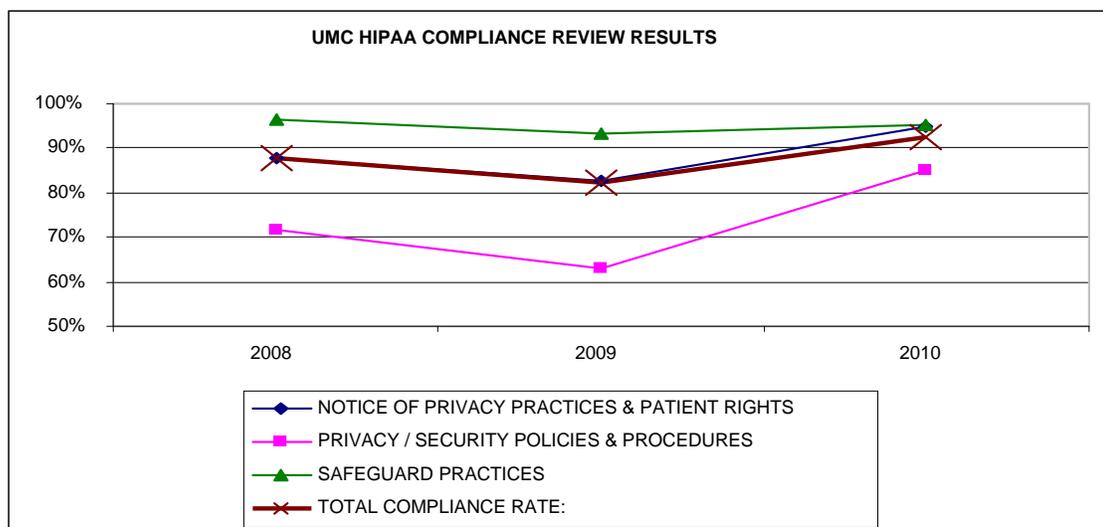
Fieldwork began on May 17, 2010 and concluded October 7, 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## RESULTS IN BRIEF

The overall compliance rating was 93% for the 27 departments included in this review, an increase from 82% found in last year's audit. Eight departments (30%) merited a "HIPAA-Star" in recognition of 100% compliance ratings. Another 15 units (56%) scored 90% or higher compliance. The compliance rates for the remaining four units (14%) ranged from 64% to 89% compliance. Of the total 87 departments that were audited over the three years, 24 (28%) achieved 100% ratings.

The following chart shows the average compliance rates for each objective and an overall rate for each of the three years audited.





When employees were unable to answer questions about UMC's policies or procedures, education was provided to them at the time of the interviews.

When incidences of non-compliance were observed, or staff was unable to demonstrate understanding of policies and procedures, we provided the pertinent education to staff, issued memos, or spoke directly with the managers and included recommendations for corrective actions.

The findings for criteria measuring less than 90% are discussed in detail below.

## **DETAIL OF FINDINGS**

### Knowledge of Privacy Policies and Assigned Responsibilities

Eight of nine (89%) departments that register patients were able to describe the procedures for providing patients with the Notice of Privacy Practices (NPP). We found one department recently reorganized and added the patient registration process to its operations. However, the training provided to staff omitted procedures related to issuing the Notice of Privacy Practices (NPP) and obtaining acknowledgement of receipt from the patient.

Excepting this one department, we found notable improvement in the employees' awareness of the HIPAA Compliance Questionnaire Screen. This screen indicates whether a privacy restriction was granted and whether the patient was provided with the Notice of Privacy Practices. As in prior audits, we found that employees' awareness varied based on job role, with employees involved in the registration process having more awareness than the clinical staff interviewed. Seventeen of 19 (89%) departments knew how to locate the screen and knew what information is contained on the screen. This criterion rate in the prior report was 38%.

Another area of significant improvement was found in employees being able to explain the privacy restrictions available to patients and how they are applied, 24 of 26 departments (92%,



up from 85%). Staff in one finance department was educated about the need to verify a patient's privacy status before initiating telephone calls to them about accounts payable issues.

None of the five employed physicians interviewed were able to explain the process for responding to a patient's request about an amendment to health information. All indicated they have not received such requests from patients.

Almost all of the employees in Transplant Services are new to the department and a new manager recently started. Registration training was done on one system without including use of the HIPAA Screen, and training on the other system was planned at the time rounds were conducted. As a result, employees were not aware of the different HIPAA related screens and their use.

Every member of UMC's workforce is expected to know how to identify a privacy request and how to direct the patient to the appropriate department or individual. Employees involved in use and disclosure of PHI are expected to know how to identify when a patient's privacy request has been accepted. Employees are educated about these expectations which are outlined in administrative policies, in new hire orientation, and annual refresher training programs. In addition, education is provided by the Privacy Officer when requested by employees, when needs are identified, or in response to new rules, such as the data breach notification rule.

Employee awareness of UMC's privacy and security policies is necessary to avoid violating a patient's privacy right because staff does not know how to identify one is in place, for example, a disclosure made without obtaining the required password, even though that restriction was requested by the patient. As a result of these errors, UMC's patients may be denied their rights or have requests delayed, leading them to believe that UMC does not value privacy. Additionally, patients may not receive a copy of the NPP, and consequently, not be aware of their privacy rights.

Patient complaints may prompt the Office for Civil Rights to review UMC's compliance to the HIPAA regulations, which could result in civil monetary penalties or civil action by the patients.

At the conclusion of each department visit, the Privacy Officer provided the manager with a summary of the specific findings, actions and recommendations via email. When warranted, such as with the Transplant Services employees, an education program was delivered by the Privacy Officer.

We recommend the Associate Administrator of Ambulatory Services direct staff to document procedures for the Ambulatory Services department that describe the process for receiving and processing an amendment request. Additionally, we recommend the Associate Administrator of Ambulatory Services provide an education program to all staff about the amendment procedures. Objectives of the education program should include recognizing when a patient is requesting an amendment, knowing how to locate the procedure, and understanding the process for notifying Health Information Management Department of the results of an amendment request.



### Compliance to Safeguard Policies

We found three offices and four nursing stations or 26% that had unattended protected health information, an improvement over the prior report finding of 39%. Files were left on counters and desks in areas staff presumed were under constant supervision or accessible only by authorized personnel. One clinic had highly sensitive records that were accessible to contracted cleaning staff after the clinic had closed.

One department had confidential information in wall pockets viewable to passersby. Another had a computer screen visible from the lobby.

The registration desk configuration at one ambulatory care center allows anyone in the lobby to potentially overhear information discussed at the registration desks. Televisions are in the ambulatory care center lobbies, and could provide enough background noise to minimize the risk of others overhearing registration activities. However, there is no sound with the informational programs shown on the televisions. Additionally, signs advising patients of their right to request a more private area for the registration process had been removed in that center.

Paper containing protected health information is routinely removed from hospital property by authorized persons in one department. The program coordinators in Transplant Services are required to keep lists containing personally identifiable and protected health information with them at all times in the event a donor becomes available. UMC plans to assign encrypted flash drives to replace the paper lists, but they were not implemented at the time of this report. This creates a risk of the paper being stolen or lost, possibly resulting in a data breach.

User ID and passwords to two systems containing protected health information owned by external entities were found posted in one nursing unit. Two external entities had provided their user identification and passwords to information systems owned by them to UMC nursing staff in one unit to facilitate patient care.

A failure by any of UMC's workforce to comply with the technical, physical and administrative safeguards outlined in its policies makes the hospital vulnerable to unauthorized access, unauthorized disclosures, loss or compromise of patient information. Each of these potential events presents a risk to patient safety, loss of customer confidence, while significant failures may result in federal and state investigations that can result in fines and corrective actions. Further, the Secretary of the Health and Human Services Department added data breach notification regulations to HIPAA in 2009. In addition to eroding customer confidence, data breach notification entails additional expenses and reporting to the Department of Health and Human Services.

Recommendations made to managers to improve physical safeguards included:

- Close off one end of a file shelving unit to prevent anyone from being able to remove a record. We were notified this recommended was accepted and is completed.
- Change the cleaning schedule to times when staff is present. We were notified this recommendation was accepted and is completed.



- Change the locks on offices to limit access. We were notified this recommendation was accepted and is completed.
- Use confidential covers in wall pockets to protect against unauthorized access.
- Move the scanning station or use a privacy screen to prevent unauthorized view from the lobby.

In addition, the following recommendations were made to managers to improve technical safeguards:

- Request door access audit reports and review periodically to ensure that only authorized persons are accessing areas containing protected health information.
- Follow through on the plan to replace paper patient lists with encrypted portable devices for transplant coordinators.
- Discontinue allowing staff to use the posted user identification and password for access to electronic protected health information in systems owned by two external entities and require them to issue unique user accounts to authorized employees. The posted user IDs and passwords were removed at the time of the review.

Further, we recommend the Chief Operating Officer direct staff to add a soundtrack to the video that is shown on the ambulatory care center televisions. A soundtrack will help prevent those in the lobby from overhearing conversations at the registration desks.

Finally, we recommend the Chief Operating Officer verify that all departments have completed their risk assessments, which will enable departments to proactively identify and correct issues such as those found during our audit.

We noted a distinct improvement in staff awareness during this review; our presence in restricted areas was challenged and our business reason verified in all but one instance. We commend the staff on their heightened awareness and attention to what is going on in their areas.

#### Inconsistent Disclosure Recording Procedures

We did not find significant change from prior reviews in complying with the required disclosure rule. Eight of 20 departments had evidence that disclosures are being recorded (40%).

Employees in 12 departments could not explain the disclosure tracking requirement. Although the log form is added to inpatient charts, we seldom observed entries and the office technicians and monitor technicians are unaware that they are expected to transfer entries into HIPAASafe. Further, ambulatory care centers are not consistent in the way disclosures are recorded. Some note the disclosure in the chart and others use a notebook.

The Privacy Rule § 164.528 accounting of disclosures of protected health information standard requires certain disclosures be recorded and retained for six years. UMC Administrative policy, V-5 Patient Access to Protected Health Information, Restrictions, Amendments and Accounting of Disclosures, assigns responsibility to the department manager to have documented procedures



and assigned responsibilities for recording disclosures. The organization-wide Required Disclosure Recording Procedures posted on the UMC intranet, Policies and Procedures, describes the disclosures that must be recorded.

We made recommendations in the 2009 report to require clinical managers to document procedures for staff about how to record disclosures and assigned responsibility for doing so, and to have organizational procedures adopted as required by the Red Flag Rules. We did not find any evidence these recommendations were implemented. We note that UMC's ability to improve compliance has been hindered by the lack of reliability of the software application intended to serve as a central repository for disclosures. UMC Information Systems is working with the vendor to determine whether the application can be fixed or discontinued and alternative methods developed to meet this standard. At this time, there is no assigned data owner for the application.

In addition to the previously identified risks of federal fines and penalties, UMC's operations will be impacted when resources must be directed toward retrieving and reviewing every encounter for the patient to determine if a disclosure may have been made. It is also difficult to determine if all disclosures that should have been made were actually made. For example, a permitted disclosure to law enforcement is made but no documentation can be found in either HIPAASafe or the medical record. Similarly, an accidental disclosure, such as a mis-dialed fax transmission, would not be recorded.

The Privacy Officer sent memos to the managers recommending they review the administrative policy and procedures that are on the intranet, and verify that staff understands their responsibilities and know how to record disclosures.

We again recommend the Chief Executive Officer direct staff to require all cost center managers to write procedures that describe how disclosures are to be recorded and by whom. The procedures should be included in the department's new employee orientation training and annual competency evaluations.

Further, we recommend the Chief Executive Officer direct staff to assign data owner responsibility to the disclosure tracking software application, should the decision be made to continue using the application.

### Follow Up to Prior Findings

We followed up on findings identified during previous HIPAA Compliance Review audits. Those findings included improper physical safeguards, such as not shielding PHI from view and improper disposal of paperwork. We noted no repeat observations of those issues in the affected five cost centers.



**APPENDIX A**

**Management's Response**

**UMC HIPAA Compliance Review**  
**for the period May 17, 2010, through October 7, 2010**  
**Findings, Recommendations, and Corrective Actions Status**  
**As of March 31, 2011**



**AUDIT DEPARTMENT**  
**Jeremiah P. Carroll II, CPA**  
**Audit Director**

**Original Report Issuance Date:**

Summary Audit Findings & Recommendations			Summary Management Disposition			Follow Up Status		
Ref	Finding	Recommendation(s)	Concurrence	Management Response & Action Plan	Mgmt Action Due Date	Implemented	Not Implemented	Other
1	One department (Transplant Services) recently reorganized and almost all staff was new to the department. The department began registering patients but the training failed to emphasize the procedures for issuing the Notice of Privacy Practices (NPP) and obtaining the patient's acknowledgement of receipt.	The interim manager was advised to provide education to the staff to ensure the NPP is offered and acknowledged by the patients. The manager immediately scheduled education, and that was provided by the Privacy Officer on October 7, 2010.	Y	Recommendations were accepted and have been completed.	10/07/2010			
2	Employed physicians were asked to describe the procedures for patients who want to request an amendment to protected health information. None of the five were aware of a procedure, and none of them recalled having any requests made of them.	Document procedures for Ambulatory Care Services Department and provide education to all staff in the Ambulatory Services division about the amendment request process.	Y	The Ambulatory Care medical record policy was revised February 2011. In-service education will be delivered to all Ambulatory Care staff about the amendment request procedures.	05/31/2011			
3	Physical safeguards can be enhanced in the Ambulatory Services care centers to reduce incidental disclosures of the information being exchanged at the registration desks or that can be seen by people in the lobbies.	Add a soundtrack to the UMC programming on the televisions in the Care Center lobbies.  Add a privacy screen or move computers that can be seen from the Care Center lobbies.  Verify that all departments have completed a risk assessment.	Y	We concur with the recommendations, however, the current programming does not support music at this time. The company that provides the service hopes to have the ability to add this feature in the next 6-12months. In the meantime, we will look at another source of music to mask the noise.  Staff has been directed to review locations of computers that do not provide for a secure view and take appropriate action. A risk assessment is currently underway to evaluate areas where potential disclosures may occur.	04/29/2011			

Summary Audit Findings & Recommendations			Summary Management Disposition			Follow Up Status		
Ref	Finding	Recommendation(s)	Concurrence	Management Response & Action Plan	Mgmt Action Due Date	Implemented	Not Implemented	Other
4	Use of technical safeguards can reduce the risk of unauthorized disclosure in the event of loss or theft of the paper the Transplant Services program coordinators are required to keep with them at all times when on call. The information, "the transplant list", is in paper form and contains protected health information.	Assign encrypted flash drives to the program coordinators in Transplant Services.	Y	The Director, Transplant Coordinators, Data Coordinator, and Transplant Surgeon have all received iron keys to protect confidential patient information.	01/10/2011			
5	We did not find significant change in compliance with the required disclosure recording rule. We found some staff know there are some disclosures that need to be recorded, but awareness and the method of recording varied. We did not find evidence of written procedures in the departments as recommended in the previous reports. The third party software application has not been functioning reliably due to a lack of upgrades made by the vendor. Staff is working with the vendor to determine resources required to upgrade and restore full function to staff. No data owner is assigned to the application.	Require cost center managers to document disclosure recording responsibilities and include training in their department orientation.  Decide if the third party software application will be upgraded and continued or develop alternate recording procedures.  Assign a data owner or team to the application, if it is to be retained.	Y	We concur with these findings and will execute an action plan to ensure department managers understand the disclosure recording rule, and have written procedures for their employees who make or record disclosures. We will focus our efforts only on those cost centers that make any one of the disclosure types described in the Privacy Rule and obtain a list of those cost centers from the Privacy Officer. The Corporate Compliance Committee will oversee the action plan through completion. We are presently negotiating an upgrade to the disclosure tracking application and anticipate a decision to be finalized by June 2011.	06/30/2011			