AUDIT DEPARTMENT
UNIVERSITY MEDICAL CENTER HIPAA COMPLIANCE

For the period October 2008 through May 2009

JEREMIAH P. CARROLL II, CPA
Audit Director

Audit Department

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

Jeremiah P. Carroll II, CPA, Director • Angela Darragh, CPA, HIPAA PMO Manager

September 15, 2009

Ms. Virginia Valentine
County Manager
500 S. Grand Central Parkway, 6th Floor
Las Vegas, Nevada 89106

Dear Ms. Valentine:

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 October 28, 2008 through May 13, 2009.

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
- Safeguard Practices

The results of our evaluation showed an overall compliance rating of 82% for the 29 departments included in this review. Seven departments merited a "HIPAA-Star" in recognition of 100% compliance ratings. Another four departments (14%) scored 90% or higher compliance. The compliance rates for the remaining 18 units (62%) ranged from 60% to 89% compliance.

A draft report was provided to the Chief Executive Officer of UMC, and the response is included. 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

CORPORATE COMPLIANCE, HIPAA AND INTERNAL AUDIT
HIPAA COMPLIANCE REVIEW
For the period October 2008 through May 2009

BACKGROUND

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

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.

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 a summary of the policies and safeguards is issued as part of the UMC Orientation program.

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

- Administrative safeguards, i.e., complete initial HIPAA 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 recycle 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 rounds.

To accomplish our objectives, we interviewed appropriate personnel, reviewed policies and procedures, and conducted observation rounds in 29 departments of UMC. Departments surveyed included 20 clinical or direct patient contact units, 4 ambulatory care units, and 5 non-direct patient care support service units.

Fieldwork began October 28, 2008 and concluded May 13, 2009. 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 82% for the 29 departments included in this review, a decrease from 88% found in last year's audit. Seven departments (24%) merited a "HIPAA-Star" in recognition of 100% compliance ratings. Another four units (14%) scored 90% or higher compliance. The compliance rates for the remaining 18 units (62%) ranged from 60% to 89% compliance.

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

As in prior audits, we found that employees' awareness of the HIPAA Compliance Screen varied based on job role. Employees involved in the registration process had more awareness than the clinical staff interviewed. Eight of 21 (38%) departments knew how to locate the screen and knew what information is contained on the screen, while eight of 18 (44%) knew how to update the screen. Patient Accounts staff stated there has been no education provided about their role in responding to amendment requests. Individual nurses and unit office technicians were taught how to change the "publish field" flags during the audit.

We found improved awareness and understanding of UMC's privacy restrictions, NFP (Not for Publication) and Passwords since our last review. Employees in 23 of 27 departments (85%) were able to explain about the assignment or use of a password. Specifically, we noted improved awareness by employees in the Emergency Department and Ambulatory Care division. Variations in practice were found in Ambulatory units regarding the method of documenting passwords. Awareness and use of the Request for Hospital Directory Restrictions form was found in one unit, the remaining employees were aware of the form but have not seen it in use. Additionally, we found a lack of awareness of the need to verify patient privacy restrictions by staff in the Patient Accounts department.

Additionally, we found staff in 14 of 20 departments (70%) knew the patient's acknowledgement of receipt of the Notice of Privacy Practices (NPP) is on the Consent for Admission form. Generally, clinical staff is unable to verify when a patient has or has not received the NPP. Further, we found a decrease in employees' ability to explain the contents of the NPP since our last review. Staff in 13 of 19 departments (68%) was able to describe the contents of the NPP. Consistent with findings in the previous audit, we found clinical staff perceives the NPP is part of the registration function.

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 specific needs are identified, such as the education to UMC's cost center managers on December 18, 2008 that included a review of each manager's responsibilities for compliance.

Employee awareness of UMC's privacy and security policies is necessary to avoid violating a patient's privacy right because staff do not know how to identify one is in place, for example a disclosure made despite the presence of a password. 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.

There are also other negative consequences to this issue. For example, a patient's future health care may be adversely impacted by the failure to identify amended information. Similarly, UMC may not be able to rely on a legal medical record if amendments are not done properly. Further, in the absence of organizational procedures for identifying and responding to a person's claim of possible identity theft, employees are taking a variety of actions, including no action. Consequently, the issue is not always properly resolved or appropriate amendments added to the medical records. As a result, a person's plan of care may be based on false information if his/her personal identifying information is used by another individual.

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. Additionally, new privacy and security regulations introduced in the American Recovery and Reinvestment Act of 2009 include improved enforcement actions such as authorizing the State of Nevada's Attorney General to enforce the regulations, a tiered structure for civil monetary penalties; and increased audits by the Department of Health and Human Services. Finally, UMC faces enforcement by the Federal Trade Commission for non-compliance to the Red Flag rules which required policies and procedures to be implemented by November 1, 2008 to detect, prevent and mitigate identity theft.

We offer the Chief Executive Officer the following recommendations to improve employee awareness and knowledge of UMC's privacy policies, procedures and designated responsibilities:

- Direct administrative division heads to verify that cost center managers include education in staff meetings about the NFP and Password restrictions, the HIPAA Compliance Screen, and the NPP.
- Direct the Director of Revenue Cycle to document and implement an organizational process to detect, prevent and mitigate identity theft in accordance with the Red Flag rules. Specific departments; such as Patient Access, Health Information Management and Patient Accounts, have key roles to play and the process significantly impacts several other departments. A comprehensive process will ensure that each UMC department that creates, stores and uses patient information acts in a consistent manner.

Compliance to Safeguard Policies

We found appropriate use of the recycle bins for disposal of paperwork containing PHI in 26 of 29 departments (90%). We note this represents a 3% improvement from the report issued March 25, 2008. However, we found unlocked recycle bins in three departments. Interviews indicated the bins are unlocked by staff and left unlocked for staff convenience. Each of the departments had keys available for staff to use. We advised managers to verify that the bins are locked at all times in accordance with UMC policy.

We found 11 of 29 departments (39%) had unsecured sensitive and protected health information in open offices and in several nursing stations. Files are left on counters and desks in areas staff presume are under constant supervision; however, our observations demonstrate there are times when no one is in the area. Access to areas containing personal, sensitive or protected information must have electronic access controls and should not be left open or unattended at any time.

Additionally, we found active computer sessions in four of 29 departments (14%). In all but one of these incidences we discussed the issue with the responsible employees at the time of the review. Employees must log off or lock their computers to avoid unauthorized access to ePHI when leaving their workstation. Several employees were taught how to lock the computer, and others admitted they knew they were supposed to, but had not developed the habit of locking or logging off. In one instance, we logged off the user when the responsible employee had not returned after waiting for more than five minutes.

We found that staff in the Patient Accounts department was unable to demonstrate the method for encrypting outgoing emails that contain protected health information. UMC policy requires the user to ensure data is securely transmitted. Education has been provided to employees about encrypting personal information through annual mandatory education and UMCPost Security Alert messages. During our review, employees were taught the method to encrypt and where they can locate the instructions on the UMC intranet.

Additionally, we observed Patient Accounts employees speaking with customers on the telephone who were easily overheard by others in the department. UMC policy requires employees use low voices whenever possible to avoid unauthorized disclosures to others who have no need to know.

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 American Recovery and Reinvestment Act of 2009 regulations require data breach notification for violations that occur after the final regulations are enacted. In addition to eroding customer confidence, data breach notification entails additional expenses and reporting to the Department of Health and Human Services.

We recommend the Chief Executive Officer direct administrative division heads to verify that cost center managers have conducted risk assessments to identify vulnerabilities within their departments and evaluate their staff competencies with complying with UMC's privacy and security policies.

Additionally, we recommend the Revenue Cycle Director consider the feasibility of relocating the customer service staff to a more private part of the department and enforce the use of lower voices to avoid unauthorized disclosures.

Inconsistent Disclosure Recording Procedures

We found that disclosures that must be recorded are not consistently captured in all departments. We found only seven of 20 departments (35%) had any evidence that disclosures are being recorded.

Employees in 13 departments did not know what the disclosure tracking requirement involved. Although the log form is added to inpatient charts, entries are seldom seen. The HIPAASafe application was taught to several employees during the course of this audit and all managers were notified via email memos of this finding.

Only one office technician knew she was responsible for entering disclosures from the log into the HIPAASafe application, but said a prior manager told her it was no longer required and she stopped about two years ago. We discussed the finding with the unit manager who was unaware of the requirement or the fact she was expected to have a procedure in place.

There are several regulations and policies related to recording of disclosures. The Privacy Rule § 164.528 Accounting of disclosures of protected health information standard requires certain disclosures be recorded and retained for six years. The American Recovery and Reinvestment Act of 2009 will require disclosure tracking for a three-year period for all disclosures made from electronic health records. 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.

Based on our review, we believe UMC is unable to demonstrate significant compliance to this HIPAA requirement. The prevalence of medical identity theft is increasing. To mitigate negative consequences, national advocacy groups advise victims to request the accounting of disclosures report. The report is expected to help them ensure all legitimate recipients of the stolen information are notified and possibly identify unauthorized recipients. However, UMC is currently unable to provide patients with a meaningful report of disclosures.

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, although it will not be possible to determine if all 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.

We recommend the Chief Executive Officer direct administrative division heads to verify that cost center managers have reviewed the checklist provided to them in December 2008, identified where department specific procedures are needed, assigned responsibilities and verified that those procedures have been implemented.

Additionally, we recommend the Chief Executive Officer direct administrative division heads to review the orientation and training checklists used for new directors and managers for completeness, and to revise them to include specific required procedures for which they are accountable.

Failure to Adhere to Administrative Policy

We found only a few of the Patient Account staff wearing their UMC badges at the time of this review. The Patient Accounts department is located off-campus and is electronically secured by code pads. Employees do not need to use the badge for access into the department or to record work hours. As a result, employees do not perceive the badge as necessary while in the department.

UMC Administrative Policy, V-39 Facility Access Controls and UMC Administrative Policy, III-5.1 Identification Badges, requires all members of the UMC workforce to have their UMC badge on at all times for the safety and protection of UMC's patients, visitors and employees. Failure to wear the badge may result in loss or theft, allowing unauthorized persons to gain access to secured areas or to misrepresent their identity for purposes of illegal activity.

We notified the Financial Operations Manager for Patient Financial Services via email memo with recommendations she review the policy with staff and to enforce the policy.

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 in the affected twelve cost centers.

We will continue to conduct these HIPAA Compliance Review audits to ensure that departments comply with HIPAA regulations and UMC's administrative policies in applying appropriate safeguards to protected health information.

APPENDIX A

HIPAA REVIEW RESPONSE

FINDING	Why It's a Problem	What's Expected	Recommendation	Action Plan
Lack of knowledge about the HIPAA Compliance screen, procedures and designated responsibilities.	The screen provides information about a patient's privacy requests, failing to use it can cause a denial of a patient right.	Registration staff, Nurses and Unit Clerks should all know how to change the NFP or password and where the form is. Patient Account staff should know they need to check the screen for an NFP or password before disclosing PHI to family. Nurses and Unit Clerks should know that the Notice of Privacy Practices is acknowledged on the COA form and to give one if requested.	Administrators require their directors and managers to demonstrate evidence of staff meetings and in-services include use of the HIPAA screen, updating the Publish flag, using the restrictions request form, knowing how to tell if a patient has received a Notice of Privacy Practices.	• Request a copy of at least one meeting or in-service that included one or all of these items. • Review / in-service Managers at Cost Center Managers meeting. • Request Managers to review at least once a quarter at their staff meetings. • Request Privacy Officer to ask random Nurses and Unit Clerks to show how to change the publish flag. Ask where the restriction form is; ask if a patient got the notice. Request feedback to Managers & Administrative staff.
	Changes are made to the medical and billing records without follow-through to make sure every system is updated properly.	Anyone who creates or changes medical or billing records is supposed to know the amendment procedures. Patient Accounts & Ambulatory Services staff said they didn't know about the process, despite procedures being in place for 6 years and included in multiple education activities. Patient's wanting entries or bills changed in any way have to request an amendment through HIM.	Verify procedures are documented and staff is inserviced. Amendment process should include responding to ID theft issues.	• In-service employees • Review and revise P&P recommendations sent to Director of HIM in January 2008.
	ID theft issues are not cleared up properly, can cause a patient safety issue is the wrong information is used.	Employees should know that the amendment procedures will work through an ID theft issue and include correcting records in every system, including correcting credit reports. Reg Flag Rule procedures were due by 11-1-08 and they were not done yet.	Revenue Cycle Director – Complete and publish procedures.	• Red Flag Administrative Policy will be complete by 8/31. • Department specific policies complete by 10/31.
Departmental procedures not evident	Required activities are not being done	Managers know what operations fall under HIPAA rules and have procedures documented with responsibilities assigned.	Administrators verify managers have reviewed the "to do" checklist, identified where procedures are needed and have them done.	• All training material to be redesigned by Privacy Officer and Education Department to be completed August 2009 for presentation at the Sept. Cost Center Managers meeting after Administration review and approval.
Inconsistent disclosure	Accounting of disclosures cannot be	Disclosure recording logs are to be used and then moved into HIPAA Safe. Nurse managers	Revenue Cycle Director develops and publishes the	• Red Flag Administrative Policy will be complete by 8/31.

recording	provided, a denial of a patient right.	should have procedures and make sure people are following them.	organizational procedures required by the FTC for the Red Flag Rules.	• Department specific policies complete by 10/31.
Lack of awareness of threats and vulnerabilities	Violations of HIPAA many occur by not being aware	Managers and data system owners have conducted risk assessments and know adequate security measures and behaviors are in place to protect against loss, theft, unauthorized access or disclosure.	Administrators require their directors and managers to demonstrate evidence of a risk assessment for their areas and identified mitigation efforts.	• Require all SRA risk assessments to be signed off at the administrator level. • Request sample of one when doing performance eval.
Unsecured records	Theft or loss of medical records	Doors are locked when offices are vacant, nursing units keep charts behind station and always under observation.	Lock doors when leaving; make sure somebody is in nursing stations at all times.	Observe on rounds; perform risk assessments as needed.
Active computer sessions without a user	Unauthorized access, change to records that may create a patient safety issue.	Users log off or lock computers when stepping away.	Log off or lock computers.	• Ask random employees to show how to lock a computer. • Management evaluating privacy screens for computers in public areas.
Encrypting PHI	Unsecured PHI may require breach notification to patients and HHS. State Law prohibits sending SSN without encryption.	Everyone knows how to force encryption in outgoing e-mails, when it needs to be done and does it.	Managers provide department in-services and require competency demonstrations.	• Discussed at June 2009 Cost Center Managers meeting. • Request Education Department to integrate into New Employee Orientation. • Ask random employees to show how to send secure messages and explain when they must use encryption.