



Audit Department

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

Angela M. Darragh, CPA, CFE, CISA, Director

October 29, 2015

Mr. Mason VanHouweling
Chief Executive Officer
1800 W. Charleston Blvd.
Las Vegas, Nevada 89102

Dear Mr. VanHouweling:

We completed our audit of University Medical Center's (UMC) compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The primary purpose of HIPAA is to ensure healthcare providers properly protect and secure individually identifiable health information. The U.S. Department of Health and Human Services Office for Civil Rights can levy significant financial penalties for non-compliance.

Our objectives were to determine employees' level of awareness and understanding of UMC's privacy policies and their use of appropriate safeguards to protect patient information. We developed criteria of 20 observations and specific questions for employees that we categorized into three main HIPAA areas:

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

The departments that we evaluated achieved a better than 90% compliance rate in seven compliance categories. Where departments did not achieve a 90% compliance rate we outlined findings in our report, specifically:

- Risk assessment policies continue to require attention.
- Inconsistent Staff Awareness of Privacy Responsibilities.
- Notice of Privacy Practices Not Always Posted.
- Staff Not Consistently Safeguarding PHI.
- Shred Bin Keys Not Well Controlled.

The assistance and cooperation of UMC's staff during our rounding and observations was sincerely appreciated.

Sincerely,

Angela M. Darragh, CPA
Audit Director



Audit Report

HIPAA Compliance

October 29, 2015

TABLE OF CONTENTS

REPORT DETAILS	- 2 -
BACKGROUND	- 2 -
PURPOSE, SCOPE, AND OBJECTIVES	- 2 -
CONCLUSION	- 3 -
FINDINGS, RECOMMENDATIONS, AND RESPONSES	- 5 -
FINDING 1 – RISK ASSESSMENT POLICIES CONTINUE TO REQUIRE ATTENTION (HIGH)	- 5 -
FINDING 2 – INCONSISTENT STAFF AWARENESS OF PRIVACY RESPONSIBILITIES (MEDIUM)	- 7 -
FINDING 3 – NOTICE OF PRIVACY PRACTICES NOT ALWAYS POSTED (MEDIUM)	- 9 -
FINDING 4 – STAFF NOT CONSISTENTLY SAFEGUARDING PHI (MEDIUM)	- 10 -
FINDING 5 – SHRED BIN KEYS NOT WELL CONTROLLED (MEDIUM)	- 12 -

REPORT DETAILS

BACKGROUND

As a healthcare provider that conducts standard electronic transactions, University Medical Center (UMC) must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This law, along with amendments and additions for the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), as well as implementation rules promoted by the U.S. Department of Health and Human Services (HHS), are designed to protect the privacy rights of patients and secure their medical information. In general, UMC must protect and secure individually identifiable health information (protected health information, or PHI) from unauthorized access, use, or disclosure.

Protected health information (PHI) touches virtually every business operation at UMC, and tools are in place to assist employees across the organization with compliance. UMC makes organizational policies and procedures available to all staff in electronic form on its intranet. In addition, each department manager is responsible for implementing procedures specific to their operations. Finally, a summary of expected privacy and security safeguard practices is provided to workforce members as part of the UMC Orientation program.

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

- Administrative safeguards, such as completing HIPAA training during orientation, accessing protected health information (PHI) only for legitimate business reasons, knowing how to assist patients with privacy requests, and knowing how to report violations or breaches;
- Physical safeguards, such as shredding or placing into a locked container designated for shredding all papers or media containing PHI, and ensuring PHI is not placed in public view.
- Technical safeguards, such as logging off workstations, not sharing passwords, and transmitting PHI only when encrypted.

HHS' Office for Civil Rights (OCR) conducts audits and investigations to enforce the privacy and security protections required by HIPAA. In addition, HIPAA-covered entities such as UMC are required to self-report unauthorized access, use, or disclosure of PHI to OCR. Any person at any time can also report a potential HIPAA violation to OCR for investigation. OCR can impose significant monetary penalties to organizations that do not sufficiently protect and secure PHI. Violations of HIPAA standards can result in fines of up to \$1.5 million per standard not followed for every year the standard is not followed.

PURPOSE, SCOPE, AND OBJECTIVES

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. To

accomplish our objectives, we interviewed managers and staff at selected business units, reviewed policies and procedures, and conducted observations in UMC departments. We developed a checklist with 20 observations and specific questions for employees, which we categorized into three main HIPAA areas:

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

Observations in these three main areas included determining whether the NPP is issued to patients, whether papers containing PHI are disposed of properly, whether specific procedures such as risk assessments were implemented as required, and if computers are locked when not in use. Additionally, we followed up on findings identified in prior audits.

Due to the number of departments within the UMC organization, we generally review one third of departments each year, ensuring that all departments are reviewed over the course of a three year period. This audit included 23 total departments: 13 clinical or direct patient contact units, 2 ambulatory care units, and 8 non-direct patient care support service units. We scored this group of departments’ compliance according to our 20 observation criteria, and we detailed findings for any criteria that did not meet a 90% compliance rate.

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.

CONCLUSION

Overall we found that departments were collectively stronger with some safeguards designed to protect patient privacy and weaker with others. As a whole, departments achieved a better than 90% compliance rate in 7 of 20 categories we evaluated. Where departments scored less than 90% compliance, we outlined findings and recommendations in the Findings, Recommendations, and Responses below. The findings and recommendations indicate a need for improvement in certain areas because auditors observed inconsistent responses, awareness, and safeguard practices among workforce members.

When workforce members were unable to answer questions about UMC’s policies or procedures, or when we observed instances of non-compliance, we provided immediate education. We also followed-up with managers and provided department-specific findings and recommendations.

Each finding includes a ranking of risk based on the risk assessment that takes into consideration the circumstances of the current condition including compensating controls and the potential impact on reputation and customer confidence, safety and health, finances, productivity, and the possibility of fines or legal penalties.

FINDINGS, RECOMMENDATIONS, AND RESPONSES

FINDING 1 – RISK ASSESSMENT POLICIES CONTINUE TO REQUIRE ATTENTION (HIGH)

45 CFR 164.308(ii)(A) of the HIPAA regulations requires covered entities to “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity”. In order to maintain HIPAA compliance with this regulation, UMC is required to complete initial and recurring (as part of the change management process) risk assessments of all systems in departments that create, process, store, or transmit electronic PHI (ePHI). According to data maintained by the UMC Information Technology department, UMC has not met this requirement. From 2010 through 2012, 143 risk assessments were completed in departments at UMC. Since 2012, the time of the implementation of the electronic health record, only 4 department risk assessments were completed. We believe the reduction in completion of risk assessments is primarily due to the lack of policies and procedures requiring and defining a risk assessment process at UMC. In 2013 we recommended these policies be developed, but no policies have been finalized.

UMC did contract with a vendor to conduct a HIPAA Security Risk Assessment as part of the Meaningful Use attestation process and received the vendor’s final report on December 1, 2014. The assessment provides valuable information on status and current gaps in HIPAA-required safeguards, and helps achieve compliance with HIPAA risk assessment requirements. By itself, however, this assessment only helps to demonstrate compliance for a limited time because it does not provide an assessment of risks to UMC’s ePHI as system changes occur.

Without defined policies and procedures governing risk assessments it is difficult to determine on an ongoing basis whether UMC is maintaining regulatory compliance and whether risks to the confidentiality, integrity, and availability of UMC’s ePHI are sufficiently addressed. As a result, UMC is at increased risk for privacy violations.

AUDITOR’S RECOMMENDATION

1. We recommend UMC finalize and implement policies and procedures governing a process for assessing and mitigating risks to the confidentiality, integrity, and availability of UMC’s ePHI in accordance with HIPAA.

MANAGEMENT RESPONSE

In Fiscal Year 2015, UMC contracted with a vendor, with security risk assessment expertise, to complete a risk assessment of UMC's compliance with HIPAA. It is acknowledged of this risk assessment, as with any risk assessment, that the findings are pertinent to a specific time when the assessment was conducted. A re-assessment with the selected vendor has been planned. Although the specific date has

yet to be determined, a risk assessment will be completed in FY2016 and each fiscal year thereafter. As discussed below, a policy related to this implementation will reflect this annual requirement.

In addition to performance of annual risk assessments, existing HIPAA-related policies will be reviewed, identifying revisions as needed and any additional policies developed and implemented, including but not limited to risk assessment/risk management policies.

Anticipated Completion Date: March 31, 2016

**FINDING 2 – INCONSISTENT STAFF AWARENESS OF PRIVACY RESPONSIBILITIES
(MEDIUM)**

Overall, we noted that staff in some departments inconsistently demonstrated awareness for how to respond to privacy issues that might arise during the course of their duties. When we interviewed staff, we received varied and, in some cases, incorrect answers. We found the following:

- Staff in 3 of 9 departments we queried (33%) were not always able to effectively describe the content of the Notice of Privacy Practices or direct patients wishing to exercise their privacy rights.
- Staff in 8 of 22 departments we queried (36%) were not always able to recognize a data breach, how to effectively respond to a data breach, or appropriate avenues to report a data breach.
- Staff in 3 of 14 departments we queried (21%) were not always able to describe the purpose of Directory Restrictions such as Not-for-Publication restrictions or Password restrictions, or how to recognize when such a restriction is in place.

In many cases, staff ultimately responded that they would seek out a manager to respond to the request, which would likely result in the patient’s concerns being addressed. However, directing patients to the Notice of Privacy Practices, and informing patients of their right to file a complaint with the Privacy Officer are important to ensure patients are properly advised of their options and patient concerns receive an appropriate response.

Timely recognition and reporting of potential data breaches to the Privacy Officer is critical to ensure breach response is handled appropriately and in accordance with regulations.

All workforce members need to ensure they are familiar with directory restriction procedures (patient Not-for-publication or Password procedures) so that a patient’s presence in the hospital is not inappropriately disclosed resulting in a Privacy Rule violation.

AUDITOR’S RECOMMENDATION

1. Where staff did not provide an appropriate response, we provided immediate education and follow-up with email memos to managers. We recommend that managers in those departments with incorrect responses provide training on workforce members’ privacy responsibilities and appropriate response procedures at staff meetings.

MANAGEMENT RESPONSE

UMC disagrees with the Report recommending that department managers be responsible for providing training to staff when deficiencies are identified. UMC acknowledges the importance of education, and that all workforce members have a duty and responsibility to maintain their knowledge of and compliance with HIPAA. However, ensuring workforce knowledge starts with the Privacy Officer. While

assistance from a department manager is necessary, education should be commenced by the Privacy Officer to ensure that UMC's practices are consistent throughout the Organization.

The Privacy Officer and Security Officer will develop materials and a training plan for educating all UMC Departments addressing the identified knowledge deficits.

Anticipated Completion Date: October 31, 2015

The Privacy Officer and Security Officer will ensure that all UMC Departments receive specific education addressing the identified knowledge deficits.

Anticipated Completion date: March 31, 2016

FINDING 3 – NOTICE OF PRIVACY PRACTICES NOT ALWAYS POSTED (MEDIUM)

Two of five departments we visited that register patients did not post the Notice of Privacy Practices in accordance with HIPAA regulations. Not only is posting the Notice of Privacy Practices required, but it is an important tool to communicate to patients their right to access their information, UMC's use and disclosure of patient information, and important safeguard procedures that UMC must employ.

In addition to posting the notice, UMC is required by regulation to offer a personal copy of the Notice of Privacy Practices when a patient is first registered. UMC documents compliance with this requirement by asking patients to initial their acceptance or declination of UMC's Notice of Privacy Practices on consent forms when registering a patient. We reviewed 28 consent forms for this acknowledgment and found a 93% success rate. This represented a significant improvement from the 64% success rate we noted when we tested for this patient acknowledgment in our previous annual audit.

AUDITOR'S RECOMMENDATION

1. We asked both departments to immediately post the Notice of Privacy Practices in the registration areas.

MANAGEMENT RESPONSE

UMC has confirmed that the deficiency in the named Departments was remedied.

Anticipated Completion Date: Completed

FINDING 4 – STAFF NOT CONSISTENTLY SAFEGUARDING PHI (MEDIUM)

All members of UMC's workforce must adhere to policies and procedures designed to safeguard the privacy and security of patient information. These safeguards are communicated in workforce training and are available in policies and procedures on the intranet.

Overall, we noted several areas where safeguard compliance needs improvement. The need for improvement in these areas does not imply that any PHI was inappropriately accessed or used, but does indicate a greater risk for inappropriate access or use. Specifically, we found:

- Not all staff in 4 of 23 departments (17%) demonstrated awareness or challenged auditors when auditors accessed units or reviewed charts. In one case, the auditor removed their badge and successfully accessed patient charts without being challenged.
- Patient charts or other PHI not in active use in 10 of 23 departments (43%) were left unattended on nursing station counters or left on fax machines or in copy rooms.
- Staff in 9 of 23 departments (39%) did not always log off their computers when leaving their workstation, relying on either the system time-out or co-worker diligence to prevent another person from accessing the system.
- Staff in 4 of 23 departments we observed (17%) did not always immediately or appropriately place PHI in secured destruction bins.

We also noted some safeguard procedures working as intended. Voices were generally lowered to avoid incidental disclosures fax cover sheets were readily available, exam room doors were shut and charts were turned toward walls, and passwords were not posted at computer workstations.

AUDITOR'S RECOMMENDATION

1. Where we observed non-compliance with safeguard procedures we provided immediate education and followed-up with email memos containing findings and recommended corrective actions. We recommend that managers and staff in all departments be reminded to do the following:
 - Question unknown visitors particularly when visitors attempt to access secured areas or patient charts. Immediately secure charts that unknown persons attempt to access.
 - Return patient charts to their designated location, and report anyone that repeatedly fails to comply.
 - Log-off workstations and secure areas that contain hospital equipment, confidential information, or PHI when not in use.
 - Immediately and appropriately place PHI in secured shred bins.

MANAGEMENT RESPONSE

UMC feels that increased collaboration with the privacy officer and department managers is necessary. While acknowledging the importance of education, and the role of the workforce members in ensuring compliance with HIPAA, it is the Privacy Officer that should assist in the development and implementation of education programs and should recommend HIPAA compliant solutions through the privacy program. Again, while assistance from a department manager is necessary, education should be commenced by the Privacy Officer to ensure that UM C's practices are consistent throughout the Organization.

The Privacy Officer and Security Officer will develop materials and a training plan for educating all UMC Departments addressing the identified knowledge deficits.

Anticipated Completion Date: October 31, 2015

The Privacy Officer and Security Officer will ensure that all UMC Departments receive specific education addressing the identified knowledge deficits.

Anticipated Completion Date: March 31, 2016

FINDING 5 – SHRED BIN KEYS NOT WELL CONTROLLED (MEDIUM)

We found that staff in three of the twenty departments (15%) we observed with locked PHI shred bins had unsupervised access to keys for the bins. Unsupervised access to shred bin keys does not imply that the information was inappropriately accessed, but does indicate that compliance with this safeguard procedure should be improved.

Where keys were unsecured, we observed that keys were placed in a cabinet or drawer or otherwise left unattended where multiple staff had access to where the shred bin key was stored. Therefore, these keys were not secured in accordance UMC's administrative policy and procedure: I-199 Confidential Paper Disposal and Shredding Bins, which requires department managers to keep keys to the locked shred bin secure in order to prevent loss or unauthorized access to PHI.

AUDITOR'S RECOMMENDATION

1. Where we observed unaccountable key access we provided immediate education. We recommend managers evaluate key control procedures to ensure key accountability in accordance with UMC policy.

MANAGEMENT RESPONSE

UMC is re-evaluating the appropriateness of the shred bin keys being widely disseminated and will take necessary action to ensure that PHI is adequately secured at all times.

The Privacy Officer will investigate the reason(s) for the issuance of keys to the shred bins throughout the facility and will recommend an appropriate solution that balances operational needs with optimum PHI security in these areas.

Anticipated Completion Date: November 15, 2015