



AUDIT DEPARTMENT

Audit Report

University Medical Center HIPAA Compliance

June 2013

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

AUDIT COMMITTEE:

Commissioner Steve Sisolak

Commissioner Chris Giunchigliani

Commissioner Lawrence Weekly



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



June 27, 2013

Mr. Don Burnette
Clark County Manager
500 South Grand Central Parkway, 6th Floor
Las Vegas, Nevada 89106

Dear Mr. Burnette:

We have 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

We found an overall compliance rating of 82% for the 24 UMC departments we audited, based on the scoring method outlined in our full report. We also identified areas where UMC should seek to improve:

- Risk assessment procedures and risk assessment documentation are incomplete.
- Acknowledgment of the Joint Notice of Privacy Practices is inconsistent.
- Patient privacy restrictions are not routinely checked.
- Employees are not consistently safeguarding information.
- Compliance with key control policy is inconsistent.

We provided a draft of this report to the Chief Executive Officer of UMC, and his response is included as an attachment. The assistance and cooperation of UMC's staff was sincerely appreciated.

Sincerely,

/s/ Angela M. Darragh

Angela M. Darragh, CPA
Audit Director

TABLE OF CONTENTS

BACKGROUND	1
OBJECTIVES, SCOPE, AND METHODOLOGY	2
RESULTS IN BRIEF	3
DETAILED RESULTS	3
Risk Assessment Procedures & Risk Assessment	
Documentation Are Incomplete.....	3
Inconsistent Acknowledgement of the Notice of Privacy	
Practices	5
Patient Privacy Restrictions Not Routinely Checked.....	6
Employees Not Consistently Safeguarding PHI	7
Inconsistent Compliance With Key Control Policy	8
APPENDICES	9
Appendix A: Management Response Letter	9

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 promulgated 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.

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, when necessary. 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, i.e., complete HIPAA training during orientation, access protected health information (PHI) only for legitimate business reasons, know how to assist patients with privacy requests, and know how to report violations or breaches;
- Physical safeguards, i.e., all papers or media containing PHI must be shredded or placed into a locked container designated for shredding, and PHI is not placed in public view; and
- Technical safeguards, i.e., log off workstations, do not share passwords, and do not transmit PHI without encryption.

HHS' Office for Civil Rights (OCR) utilizes 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.

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. 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 criteria of 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 have been 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 24 departments: 13 clinical or direct patient contact units, 3 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.

Fieldwork began December 17, 2012 and concluded February 14, 2013. 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 for the 24 departments reviewed was 82%. Six units (25%) scored 90% or higher compliance. The compliance rates for the remaining 18 units (72% of the departments reviewed) ranged from 50% to 89% compliance. Additionally, we found 100% compliance in nine of the 20 measurements, demonstrating consistent integration of UMC's administrative, physical and technical safeguards into daily operations and individual behavior.

When employees were unable to answer questions about UMC's policies or procedures, or when we observed instances of non-compliance, we provided immediate education and recommendations for corrective action.

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

DETAILED RESULTS

Risk Assessment Procedures & Risk Assessment Documentation Are Incomplete

We reviewed UMC policy I-212: Information Security Program, and found references to risk assessments, but no written procedures for who, how, or when assessments will be conducted across the UMC enterprise. Specifically, there are no risk assessment procedures to:

- Describe the criteria to be used to determine when risk assessments shall be conducted.
- Assign responsibility for conducting risk assessments.
- Describe how completed assessments move through a review that allows Senior Leadership the opportunity to evaluate and agree that risks are reasonable and appropriate.
- Describe how mitigation plans will be monitored to ensure completion and effectiveness.
- Assign responsibility for documenting the review and resulting decisions.
- Assign responsibility for retaining the documentation for six years as required by HIPAA.

As a result, the internal controls that UMC utilizes to remain compliant with HIPAA-required information system risk assessments are not well documented, and it is difficult to measure or determine on an ongoing basis whether UMC is maintaining compliance. This

places UMC at-risk for a negative finding from external reviewers.

We did find that, despite the lack of clear procedures, more than 90% of the departments we audited had completed a risk assessment of business operations and information systems under their sphere of responsibility. UMC Senior Leadership directed all departments to conduct such an assessment, and the HIPAA Executive Steering Committee (ESC) approved a standard format and method for the departments to utilize.

Departments, did not, however, document that they completed the “Threat Assessment” component of the approved assessment method. This component of the method required assessors to recognize via an affirmative “No” or “Yes” whether 31 specific scenarios pose a risk to the unit’s information assets. Scenarios requiring an assessment and affirmation included determining whether a disclosure, modification, or complete loss of data could occur from:

- Workforce members or business associates intentionally or accidentally accessing information assets;
- Software defects;
- Hardware defects;
- Interrupted power supply;
- Natural or man-made disasters, etc.

Without documentation that the 31 threat scenarios have been assessed, we cannot determine that the approved risk-assessment method was fully completed in each of the departments. We also cannot determine that information assets in each of the departments were adequately or sufficiently risk-assessed.

Recommendation

We recommend the Director of Information Technology/Information Security Officer Revise Policy I-212: Information Security Program to include:

- A description of criteria used to determine when risk assessments shall be conducted.
- Assigned responsibility for conducting risk assessments.
- A description about how completed assessments move

through a review that allows Senior Leadership the opportunity to evaluate and agree that risks are reasonable and appropriate.

- A description about how mitigation plans will be monitored to ensure completion and effectiveness.
- Assigned responsibility for documenting the review and resulting decisions.
- Assigned responsibility for retaining the documentation for six years as required by HIPAA.

We also recommend that the Director direct staff to complete and document the “Threat Scenario” component of the currently approved risk-assessment method, in order to help ensure that information assets within the departmental sphere of responsibility are adequately and sufficiently risk-assessed.

Inconsistent Acknowledgement of the Notice of Privacy Practices

Overall, we found a low success rate for obtaining appropriate patient acknowledgement of the Joint Notice of Privacy Practices (NPP), and a lack of documented procedures for staff to follow in order to appropriately obtain acknowledgment, or appropriately document the reasons for a lack of acknowledgment.

UMC complies with § 164.520 of the HIPAA Privacy Rule by offering patients a copy of its NPP at each registration. The NPP explains how UMC uses information about patients and their rights with respect to their health information. Hospital patients are asked to initial the Conditions of Admission (COA) form to indicate whether they accept or decline the copy. Patients visiting care centers are asked to initial the Consent for Outpatient Services (COS) form. In this way, UMC demonstrates attempts to obtain the patient acknowledgement as required by HIPAA Privacy Rule.

During our inspection of medical records, we found:

- 63% (15 of 24) of the Conditions of Admission (COA) forms included the patients’ initials, indicating a copy of the NPP was accepted or declined.
- 67% (12 of 18) of the Consent for Outpatient Services (COS) forms included the patient’s initials, indicating a copy of the NPP was accepted or declined.

Where a patient's acceptance or declination was not appropriately acknowledged, we noted blanks or checkmarks rather than a patient's initials where an acknowledgment belonged. In one case, a patient had acknowledged both acceptance and declination of the NPP.

Recommendation

The current implementation of McKesson admitting systems in the hospital, and subsequently in the ambulatory care centers, provides an ideal opportunity to revisit, update, and document procedures.

We recommend that the Director of Patient Access Services and the Ambulatory Care Center Patient Access Manager:

- Develop written procedures for all employees who register patients. The procedures should specify the process for obtaining the patient acknowledgement or documenting attempts to do so.
- Document that new and existing staff is trained on procedures and that such documentation is retained for six years.
- Periodically monitor admission forms and account notes to ensure compliance and appropriate patient acknowledgment.

Patient Privacy Restrictions Not Routinely Checked

Front desk staff at both the Health Information Management (HIMD) and Patient Financial Services (PFS) departments exhibited a general understanding of Not-For-Publication and Password restrictions, but stated they do not routinely navigate information systems to check for privacy restrictions. Staff at both desks either could not, or did with difficulty, navigate to the HIPAA compliance screen to check for privacy restrictions, ID theft alerts, or notices of revocations or amendments that may be on file. Staff in HIMD indicated they check census screens when answering calls about in-patients, but do not check for privacy restrictions on discharged patients or outpatients.

Recommendation

The current implementation of McKesson electronic health record systems in the hospital and financial services office provides an ideal opportunity to revisit, update, and document procedures.

We recommend that managers at both HIMD and PFS:

- Develop written procedures for all workforce members who respond to inquiries regarding patient medical or billing information. The procedures should specify the requirement and process for checking and responding to patient privacy restrictions in all utilized information systems.
- Document that new and existing workforce members are trained on procedures and that such documentation is retained for six years.

Employees Not Consistently Safeguarding PHI

All members of UMC's workforce must adhere to the policies designed to protect the privacy of patients and to keep their information secure.

Overall, we found a high incidence of unattended PHI during our observations. Unattended PHI does not imply that the information was inappropriately accessed, but does indicate that compliance with safeguard procedures should be improved.

Unattended PHI was found in half (50%) of the departments we audited. Some examples we observed include the following:

- Charts not in active use were found on nursing station counters;
- Staff does not always close and lock doors to offices when leaving them, leaving unsecured paperwork in areas where someone would be able to enter without being observed;
- Managers do not audit access logs when office access is controlled electronically;
- Staff does 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; and
- Staff does not always immediately or appropriately place PHI in secured destruction bins.

Recommendation

Where we observed non-compliance with safeguard procedures, we immediately followed-up with email memos containing findings and recommended corrective actions. We recommend that managers and

staff in all departments:

- Always directly return patient charts to their designated location, and report anyone that repeatedly fails to comply.
- Lock all offices and rooms that contain confidential or PHI when they are not in active use.
- Audit access logs at office locations that rely on electronic entry to control access.
- Always log-off when leaving workstations.
- Always immediately and appropriately place PHI in secured shred bins.

Inconsistent Compliance with Key Control Policy

We found that staff in four of twelve departments we evaluated 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 hanging on a wall, unattended on a cart, or multiple staff has 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.

Recommendation

Where we observed that keys were unsecured, we immediately notified managers. Overall, we recommend that department managers review their key control procedures to ensure that only authorized individuals have accountable access to shred bin keys.

MEMORANDUM

BRIAN G. BRANNMAN
Chief Executive Officer

University Medical Center
Administration

TO: Angela Darragh, Director, Clark County, Audit Department
FROM: Brian G. Brannman, Chief Executive Officer *BGB 6/18/13*
SUBJECT: Management Response to HIPAA Compliance Audit
DATE: June 18, 2013

We respectfully offer the following in response to the Clark County Audit Department's HIPAA Compliance Audit Report for the University Medical Center, dated April 2013.

1. Recommendation: That UMC revise its Information Security Policy I-212 to include:

- A description of criteria used to determine when risk assessments shall be conducted.
- Assigned responsibility for conducting risk assessments.
- A description about how completed assessments move through a review that allows Senior Leadership the opportunity to evaluate and agree that risks are reasonable and appropriate.
- A description about how mitigation plans will be monitored to ensure completion and effectiveness.
- Assigned responsibility for documenting the review and resulting decisions.
- Assigned responsibility for retaining the documentation for six years as required by HIPAA.

We also recommend that the Director direct staff to complete and document the "Threat Scenario" component of the currently approved risk-assessment method, in order to help ensure that information assets within the departmental sphere of responsibility are adequately and sufficiently risk-assessed.

Concur. The Director of Risk Management will assume responsibility for the revision of Policy I-212. The revised policy will include the following:

- Criteria used to determine risk assessments will encompass every process that touches PHI.
- Responsibility for conducting risk assessments will be at the Department level.

- The approval of completed assessments will move from Department Head for low risk; to Division Head for moderate risks; and CEO for high risks.
- A copy of all documentation, reviews and resulting decisions will be maintained by the Department Head and will be stored by IT in a sequel database for six years prior to destruction.
- The Director of Information technology will complete a Threat Scenario for the approved risk-assessment.

2. Recommendation: That the Director of Patient Access Services and the Ambulatory Care Center Patient Access Manager:

- Develop written procedures for all employees who register patients. The procedures should specify the process for obtaining the patient acknowledgement or documenting attempts to do so.
- Document that new and existing staff is trained on procedures and that such documentation is retained for six years.
- Periodically monitor admission forms and account notes to ensure compliance and appropriate patient acknowledgment.

Concur. The Health Information Management Department has implemented a new policy for employees that responds to inquiries regarding medical and billing information to check for not for Publication and password restrictions. Patient Accounting has provided education on verifying the HIPA compliance display and verification of passwords.

3. Recommendation: That managers at both HIMD and PFS develop written procedures for all workforce members who respond to inquiries regarding patient medical or billing information. The procedures should specify the requirement and process for checking and responding to patient privacy restrictions in all utilized information systems. Furthermore there should be documentation that new and existing workforce members are trained on procedures and that such documentation is retained for six years.

Concur. The Health Information Management Department has implemented a new policy for employees that respond to inquiries regarding medical and billing information to check for not for Publication and password restrictions. Patient Accounting has provided education on verifying the HIPA compliance display and verification of passwords.

4. Recommendation: That managers and staff in all departments:

- Always directly return patient charts to their designated location, and report anyone that repeatedly fails to comply.
- Lock all offices and rooms that contain confidential or PHI when they are not in active use.

- Audit access logs at office locations that rely on electronic entry to control access.
- Always log-off when leaving workstations.
- Always immediately and appropriately place PHI in secured shred bins.

Concur. Risk Management will in-service all UMC managers on the importance of:

- Returning charts to their designated areas
- Securing areas that contain PHI when not in use
- Auditing access logs at locations that have electronic entry control
- Logging off workstations when not in use
- Placing PHI in secured shred bins

Managers will be requested to address these issues at their next staff meeting, and audit for continued compliance.

5. Recommendation: That department managers review their key control procedures to ensure that only authorized individuals have accountable access to shred bin keys.

Concur. Risk Management will in-service all managers on the importance of key control and locking of all shred bins. Managers will be requested to address these issues at their next staff meeting and will be asked to periodically check to make sure that the shred bins remain locked.

We would like to thank the Clark County Audit Department for identifying these areas of potential loss exposure and providing recommendations for continued improvement.