



AUDIT DEPARTMENT

Audit Report

University Medical Center HIPAA Compliance

August 2012

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



August 30, 2012

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

Dear Mr. Burnette:

In accordance with our annual audit plan, we conducted a review of compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at University Medical Center (UMC). The audit covered the period from November 30, 2011 through May 2, 2012.

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 of 20 observations and specific questions for employees are 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 the compliance rating for the 25 departments reviewed was 86%. Ten of the 20 measures had 100% compliance. However, we identified the following opportunities for improvement:

- Patient acknowledgement of receipt of the Notice of Privacy Practices is not being obtained in a consistent manner.
- Employee compliance to safeguard policies is inconsistent.
- Incomplete risk assessment process.
- Inconsistent compliance with the key control policy.
- Physical access allowed to individuals without current business need.
- User activity audits are not documented.

A draft report was provided to the Chief Executive Officer of UMC, and his response is included as an attachment to the report. 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	2
DETAILED RESULTS	3
Inconsistent Acknowledgement of the Notice of Privacy Practices	3
Employees Not Consistently Following Safeguard Policies	4
Incomplete Risk Assessment Process	6
Inconsistent Compliance With Key Control Policy	8
Physical Access Allowed to Individuals without a Current Business Need.....	8
Failure to Document Activity Review Audits.....	10
APPENDICES	12
Appendix A: Management Response	12

BACKGROUND In accordance with our annual audit plan, we conducted a review of compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at University Medical Center (UMC). Due to the number of departments within the UMC organization, we 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 is issued to management annually.

As a healthcare provider that conducts standard electronic transactions, UMC must comply with 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 and overlap in some areas. Consequently, organizational procedures were developed where feasible and attached to the applicable administrative policy. Additionally, each department manager is responsible for implementing procedures specific to their operations, when necessary. For example, any department authorized to make disclosures about patients must have procedures describing how those disclosures are recorded and retained for six years.

Tools are in place to assist employees with compliance. For example, the HIPAA Compliance Questionnaire Screen facilitates communication of patient privacy requests. UMC makes policies and procedures available to all staff in electronic form on its Intranet. In addition, a summary of the privacy and security 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 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.

**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 of 20 observations and specific questions for employees are categorized into three main HIPAA areas:

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

Observations include items such as 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 follow up on findings identified in prior reviews. Each department is scored based on the percentage of items with noted errors.

To accomplish our objectives, we interview appropriate personnel, review policies and procedures, and conduct observations in UMC departments. This audit included 25 departments: 12 clinical or direct patient contact units, 5 ambulatory care units, and 8 non-direct patient care support service units.

Fieldwork began November 30, 2011 and concluded May 2, 2012. 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 25 departments reviewed was 86%. Three of 25 departments merited a "HIPAA-Star" in recognition of 100% compliance ratings. Another three units (12%) scored 90% or higher compliance. The compliance rates for the remaining 19 units (76% of the departments reviewed) ranged from 75% to 89% compliance. Additionally, we found 100% compliance ratings in 10 of the 20 measurements, suggesting that UMC's administrative, physical and technical safeguards are becoming integrated into daily operations and individual behavior.

When employees were unable to answer questions about UMC's policies or procedures, we provided immediate education. Similarly, observations of non-compliant practices were followed up with educating staff, issuing memos, or speaking directly with the managers, and included recommendations for corrective actions.

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

DETAILED RESULTS

Inconsistent Acknowledgement of the Notice of Privacy Practices

The Joint Notice of Privacy Practices (NPP) explains how UMC uses information about patients and their rights with respect to their health information. UMC is obliged to obtain a patient's acknowledgement of receipt of the NPP or document the attempts to provide the NPP to patients.

UMC complies with § 164.520 of the Privacy Rule by offering patients a copy of its Joint Notice of Privacy Practices (NPP) at each registration. Patients are asked to initial the Conditions of Admission (COA) form to indicate whether they accept or decline the copy. In this way, UMC demonstrates attempts to obtain the patient acknowledgement as required by HIPAA.

During our inspection of randomly selected medical records, we found:

- 58% (18 of 31) of the Conditions of Admission (COA) forms included the patients' initials, indicating a copy of the NPP was accepted or declined.
- 46% (12 of 26) of the Consent for Outpatient Services (COS) forms included the patient's initials, indicating a copy of the NPP was accepted or declined.
- One patient's COA was marked as "unable to sign" but the account notes indicate that the patient signed the COA.
- In another instance, the COA form was not found on the medical record.

Some registration staff indicated patients tend to make a checkmark instead of initialing, and that they were not instructed to return the form to be properly initialed by the patient.

We found two Ambulatory Services policies, AC 2.46 Chartless Procedures and AC 2.47 Bedside Registration. However, these policies only reference the previous versions of the Consent for Services and Financial Agreement forms and describe their placement on the medical records. Neither includes instructions about obtaining patient acknowledgement of the NPP or documenting attempts to provide the NPP. Further, we did not find any Patient Access policies on the intranet and none were provided when requested from the department directors.

Why is this Important? UMC may face financial risks of civil monetary penalties by the Office for Civil Rights if it is unable to demonstrate that an effective process exists for complying with this requirement.

Recommendation The Director of Patient Access Services and the Ambulatory Care Center Patient Access Manager should 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. Further, in recognition that the implementation of the McKesson registration products is scheduled to begin in a few months, we recommend developing the procedures based on the functionality of the McKesson products.

Upon completing the written procedures, an education program needs to be delivered to the staff and added to new employee training materials. Documentation of that education needs to include the content and evidence that the staff understand the importance of having the patient initial the NPP area of the form and must be retained for six years. Additionally, we recommend periodic monitoring of COA forms and account notes to ensure compliance.

Finally, the Director of Ambulatory Care Services should revise existing policies with the current form title.

Employees Not Consistently Following Safeguard Policies All members of UMC's workforce must adhere to the policies designed to protect the privacy of patients and to keep their information secure.

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

- Charts not in active use were found on nursing station counters;
- Staff do 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; and
- In some Ambulatory Care Centers, unlocked and open rooms are being used to store records and are not under constant observation by employees.

Three of the departments containing PHI cannot apply a "clear desk" policy when the departments are closed. These departments rely on UMC badge access privileges, locks, or fob controls to prevent unauthorized access to PHI. However, managers do not routinely review audit logs to monitor access to their department after hours, reducing the effectiveness of this control.

Employees in three of 25 departments were observed walking away from their computers without locking them, relying on either the system time-out or co-worker diligence to prevent another person from accessing the system. People waiting in the Ambulatory Care Center lobbies can easily overhear conversations at the registration desks in several locations.

In a prior audit published March 31, 2011, we recommended having a soundtrack added to the televisions to reduce the risk of people being able to overhear conversations at the registration desks when waiting in the Ambulatory Care Center lobbies. Management responded that the current vendor could not accommodate a soundtrack and that they would seek other options. We did not find any soundtracks in any of the care center lobbies during this audit, and in some cases the televisions were turned off.

Conversations held at the counter in the Outpatient Pharmacy can also be overheard by those waiting in the lobby. Outpatient Pharmacy staff make every effort to keep people away from the counter and use low voices when possible but are unable to eliminate all incidental disclosures.

Why is this Important? When any member of UMC's workforce fails to comply with the technical, physical, and administrative safeguard practices outlined in UMC policies, UMC risks complaints and potential data breaches involving unauthorized access, use or disclosure. Failing to keep PHI secure risks losing or compromising the integrity of patient information. Each of these potential events presents a risk to patient safety and loss of customer confidence. Significant failures may result in federal and state investigations that can result in fines and corrective actions.

Recommendation Managers were notified via e-mail memos with findings, actions and recommendations for corrective actions specific to their departments. Recommendations to improve physical safeguards included:

- Lock all offices and rooms that contain confidential or protected health information when they are not in active use.
- Encourage staff to continue reminding providers that they need to return medical records to a staff person or to the chart rack when finished, and to report anyone who is repeatedly failing to comply.
- Change the locks on rooms used to store records to limit access.
- Use confidential covers to protect against unauthorized disclosure.

In addition, to improve the effectiveness of technical safeguards we recommend the managers of departments that are not staffed 24/7 request and review access audit reports periodically to ensure that only authorized persons are accessing areas containing protected health information when their departments are closed.

Further, we recommend the Chief Executive Officer direct staff to propose solutions that will reduce the ability for people in the Care Center lobbies from overhearing conversations at the registration desks.

**Incomplete Risk
Assessment Process**

The HIPAA Security Rule § 164.308 requires UMC to have policies and procedures that prevent, detect, contain and correct security violations. An effective risk management plan provides a structure for evaluating, prioritizing, and implementing risk-reducing measures.

While the Security Rule requirement is specific to electronic protected health information, UMC Senior Leadership elected to apply a broader scope to include assessing its business processes, not just its information systems. All Patient Service Leaders were directed to attend training, conduct an initial assessment, and to reassess risks prior to making any significant changes to their operations.

At the time fieldwork began on this audit, UMC had 116 completed assessments; 76 were done by the departments included in this audit scope, and 46 of those were completed by the Information Technology department.

Nine of the 25 (36%) departments have not completed the department-level assessment, six of the nine are in the Ambulatory Services division, two are main campus departments, and one is a contracted department.

Three of 16 (19%) hospital departments have not completed a department level assessment but have conducted assessments on specific business processes within their operations.

However, we did not find evidence that Senior Leadership is evaluating completed assessments and mitigation strategies, and is agreeing to accept residual risks.

UMC has three organizational policies about various risk management programs, of which one is specific to information systems. Policy I-212, Information Security Program, is a new policy implemented in 2011 as part of a comprehensive review and revision of UMC's administrative policies required by the Security Rule. The policy

includes UMC's plan for its information systems, references risk analysis in the context of system activity reviews, and mentions situations in which an assessment will be considered, but there are no procedures described. Additionally, the policy refers to "UMC's Risk Management Program" and two other administrative policies, V-12 Risk Analysis and V-13 Risk Management. We did not find "UMC's Risk Management Program". Further, we did not find V-12 Risk Analysis and V-13 Risk Management posted as active policies.

Why is this Important? To be an effective program, the assessments need to be evaluated to ensure risk reduction strategies are appropriate and that residual risks are acceptable to the Chief Executive Officer with respect to both patient safety and compliance to federal law. The risk management process is even more critical now as UMC begins work on implementing various products that will create its electronic health record environment. In order to receive meaningful use incentive payments UMC must attest that a risk assessment has been done and must be able to demonstrate such if audited by the Office for Civil Rights.

Recommendation We recommend the Director of Information Technology revise Policy I-212 - Information Security Program to remove references to policies that were retired and 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.

Should the Chief Executive Officer elect to delegate responsibility for the review process, we recommend the delegated position be one of sufficient authority to ensure adequate resources will be allocated to achieve accepted risk reduction strategies.

**Inconsistent Compliance
With Key Control Policy**

UMC's administrative policy and procedure, I-199 Confidential Paper Disposal and Shredding Bins, requires department managers to keep keys to the locked shred bins secured to protect against unauthorized access to discarded papers containing confidential or protected health information.

Fifteen of 25 departments (68%) comply with the policy. In six departments we found employees had access to the key, either in unlocked drawers or pinned on bulletin boards, and in two departments the managers did not have any keys. Several clinical managers delegated the keys to charge nurses, and some charge nurses remove the key from their duty rings and put them in unsecured drawers accessible to employees.

Managers have varying understanding of the policy key controls. Some use the Pyxis system to track who is retrieving the keys while other smaller departments rely on the honor system.

Additionally, we observed over-full bins in several locations.

Why is this Important?

Failing to keep the keys secure defeats the purpose of the key control policy, i.e., preventing loss and unauthorized access. Further, when bins are filled to capacity, it is possible to remove items without having access to a key. The cost to mitigate a data breach resulting from misuse of shred bins could be extremely large, in terms of both reputational and financial costs.

Recommendation

We recommend the UMC Associate Administrator of Professional Services direct department managers to review their key control practices and verify that only authorized people have access to recycle bin keys. We also recommend that she direct Plant Operations to periodically audit how keys and fobs are issued, verify that the responsible employee signs receipt for the key, and understands their duty to immediately report loss or theft of a key or fob. Such audits will identify if the policy and procedure is effective or requires revision. Audit reports and actions taken as a result need to be documented and retained for six years.

**Physical Access Allowed to
Individuals without a
Current Business Need**

We reviewed a list of individuals authorized to access a department that stores protected health information and found 35 users listed as active without current business reasons for such access.

Public Safety, who administers the badge access system, provided a list of 185 active users with access to the Physician Referrals department. In addition to 150 current employees, contractors and

physicians the list included 35 (19%) users that do not have business reasons for access:

- 16 users who are not employees, contractors, vendors, or members of the medical staff
- 6 employee users no longer employed by UMC
- 8 employees who transferred to other departments and no longer work on the 5th floor
- 4 physicians without an apparent business need to access the 5th floor
- 1 volunteer without any apparent reason to have access to the 5th floor

UMC has well-established processes for authorizing users to have certain levels of access privileges, including two organizational policies, although neither describes modifying or terminating access:

- I-205 Access Control, that describes information systems access authorization
- Environment of Care policy, “Identifying Individuals Entering the Hospital” that describes how UMC badges may be issued by Public Safety, Plant Operations, Materials Management and the Volunteer Office.

We found one division level procedure, Human Resources Procedure 5 – Termination Process, that describes collecting UMC badges from employees when separating from UMC, but it does not include a description of how it compiles and distributes the list of separating employees to all data owners, although the process has been in place for several years. Additionally, that process only applies to employees and certain contractors managed by Human Resources.

UMC does not have written procedures for identifying and notifying all data owners (Information Technology, Health Information Management, Emergency Medicine, Medical Staff Services, Imaging Services, and Public Safety) about non-employee accounts to be modified or terminated. For example, there is no mechanism for notifying Public Safety when badges issued to County or Metro employees should be inactivated. Similarly, data system administrators may not know about medical and allied health staff terminations.

Why is this important? This lack of organizational process presents the risk that people may be able to access protected information to which they are no longer authorized. A stolen UMC badge that is still active may be used to gain access to secured areas of the hospital presenting a safety risk to patients and staff.

Further, the HIPAA Security Rule § 164.310 requires that Covered Entities implement policies and procedures to control physical access to electronic protected health information. Violations of the Security Rule could result in fines.

Recommendation The Chief Executive Officer should direct staff to identify and document procedures that will ensure all UMC data owners are routinely and consistently notified when any workforce member separates from UMC. The organizational procedures should assign responsibility for coordinating and periodically monitoring the process to ensure all user access is terminated in a reliable fashion. The Director of Public Safety should document how UMC badge access provided to outside entities, such as law enforcement or surveyors, is controlled.

Additionally, the Director of Information Technology should revise administrative policy I-205 to correctly label the Information Security Program policy as "I-212".

Failure to Document Activity Review Audits The Security Rule § 164.308 requires that UMC review audit logs and access reports to verify users are accessing only that information needed for a permitted use or disclosure.

The Emergency Services department has a procedure to support complying with this requirement, 5.02 Monitoring Procedure for Routine Audits of EmSTAT Accesses. According to the procedure, the department will conduct quarterly audits and store documentation for six years. However, we could not find any evidence that the audits were being conducted. Thus, the Emergency Department is unable to demonstrate that it is complying with the Security Rule requirement.

We also found that there is no documented matrix for role based access to the application used by the Emergency Department. This is a best practice to ensure that employees are only given access to functions they need to perform their jobs.

Why is this Important? To avoid risks of fines UMC needs to be able to produce evidence that it complies with the Security Rule standards.

Recommendation The Director of Emergency Services should document the methodology being used to conduct user audits, the results and any actions taken in response to the results and retain the documentation for at least six years. Additionally, he should formalize the role-based access matrix as part of department policy.

APPENDICES

Appendix A: Management Response



INTEROFFICE MEMO

To: ✓Angela Darragh, Audit Director
From: John Eddy, Associate Administrator Ambulatory Services *JE*
Subject: UMC HIPAA Compliance Audit – June 2012
Date: August 7, 2012

Attached please find the completed UMC HIPAA Compliance report with our management response and action plans. If you have any questions regarding our response, please feel free to contact me at (702) 383-3864.

Thank you.

Attachment(s)

cc: Cindi Roehr, Associate Administrator Professional Services
Ernie McKinley, Chief Information Officer
Hope Hammond, Privacy Officer



INTEROFFICE MEMO

To: Admitting Supervisors, Specialists, Representatives and Office Assistants
From: Tiffanie Fleming, Director PAS
Subject: Properly Completing JNOPP Forms
Date: August 6, 2012

UMC complies with § 164.520 of the Privacy Rule by offering patients a copy of its Joint Notice of Privacy Practices (NPP) at each registration. Patients are asked to initial the COA and COS form to indicate whether they accept or decline the copy. In this way, UMC demonstrates attempts to obtain the patient acknowledgement as required by HIPAA.

A recent County Audit of HIPAA Compliance was performed and the results showed that the Joint Notice of Privacy Practices is not being documented correctly.

Please review the JNOPP section of the Conditions of Admission and General Consent (COA) and the Conditions of Outpatient Services (COS) forms. The form states "Initial the applicable acknowledgement." Below that are two choices.

1. _____ I received a copy of the Joint Notice of Privacy Practices
2. _____ I declined a copy of the Joint Notice of Privacy Practices

The patient is to place their initials next to the applicable acknowledgement. A checkmark is not an acceptable form of acknowledgement.

Frequent reviews of this document will be performed to monitor compliance.

Please print, sign and return this memo to your supervisor by August 20, 2012.

Employee Signature _____

Date _____



Findings, Recommendations, and Corrective Actions Status
 As of August 2012

Original Report Issuance Date:

Summary Audit Findings & Recommendations			Summary Management Disposition		
Ref	Finding	Recommendation(s)	Concurrence	Management Response & Action Plan	Mgmt Action Due Date
1	Inconsistent Acknowledgement of the Notice of Privacy Practices				
	<p>Patient acknowledgement of receipt of the Notice of Privacy Practices is not being obtained in a consistent manner. There are no written procedures that describe how the patient acknowledgement is to be obtained. Two Ambulatory Services procedures reference old forms.</p>	<p>The Director of Patient Access Services and the Ambulatory Care Center Patient Access Manager should develop written procedures for all employees who register patients. Upon completing the written procedures, an education program needs to be delivered to the staff and added to new employee training materials. Additionally, we recommend periodic monitoring of COA forms and account notes to ensure compliance. Finally, the Director of Ambulatory Care Services should revise existing policies with the current form title.</p>	Y	<p>In the process of updating Ambulatory Care policies AC-2.46 & AC-2.47 to include instructions on obtaining patient acknowledgement on the NPP and documenting attempts to provide the NPP. Ambulatory Care PAS staff education to be completed on the proper process by November 2012. Ambulatory Care and Main PAS have two different registration systems thus need to be addressed in two different policies. A memo from the Director of PAS provided all Admitting Staff with a memo on "Properly Completing JNOPP Forms" on 8-6-12. Employees were required to read and sign that they received (copy attached). Main Admitting does not currently have an actual policy that addresses the JNOPP but is currently working with McKesson to develop a new form. This form will be addressed in the policies that will be developed on the new registration system when up and running.</p>	<p>Ambulatory Care policies updated by November 2012; Ambulatory Care PAS staff education completed by November 2012. Main Admitting staff education provided August 6, 2012.</p>

Summary Audit Findings & Recommendations			Summary Management Disposition		
Ref	Finding	Recommendation(s)	Concurrence	Management Response & Action Plan	Mgmt Action Due Date
2	Employees Not Consistently Following Safeguard Policies				
	Unattended protected health information was found in half the departments audited. Three departments that are not staffed around the clock rely on door controls to limit access, yet the managers do not review audit logs to monitor access to their departments after hours. Employees were observed leaving computers without locking or logging off. Ambulatory departments have not addressed previously noted concerns with lobby areas and preventing others from being able to hear conversations at the counters.	Managers were notified via e-mail memos with findings, actions and recommendations for corrective actions specific to their departments. We recommend the managers of departments that are not staffed 24/7 request and review access audit reports periodically to ensure that only authorized persons are accessing areas containing protected health information when their departments are closed. Further, we recommend the Chief Executive Officer direct staff to propose solutions that will reduce the ability for people in the Care Center lobbies from overhearing conversations at the registration desks and pharmacy counters.	Y	Suggestions for improvements in the Care Centers: 1) Overhead music piped in; 2) Enhance privacy booths; 3) Remodel Front Office; 4) Working with Public Relations on installing TV's that will run continuously in the waiting areas this will help create a buffer between the lobby and the registration area. Suggestions 2 & 3 require funding which was not appropriated in this fiscal year budget. Ambulatory Care Staff re-education provided during monthly staff meetings on PHI and correct process when leaving their workstations unattended.	Ambulatory Care staff education completed by November 2012; TV installation planned for completed by November 2012

Summary Audit Findings & Recommendations			Summary Management Disposition		
Ref	Finding	Recommendation(s)	Concurrence	Management Response & Action Plan	Mgmt Action Due Date
3	Incomplete Risk Assessment Process				
	Not all departments have completed their risk assessments as directed by the CEO. At the start of this audit UMC had completed 116 risk assessments, some were done on the business unit and many were on specific systems or processes. There is no evidence that completed assessments are reviewed, or that mitigation strategies are appropriate and adequate. There is no written policy or procedure describing the risk management plan.	We recommend the Director of Information Technology revise Policy I-212 - Information Security Program to remove references to policies that were retired and to include: <ul style="list-style-type: none"> • 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. Should the Chief Executive Officer elect to delegate responsibility for the review process, we recommend the delegated position be one of sufficient authority to ensure adequate resources will be allocated to achieve accepted risk reduction strategies. 	Y	Currently, risk assessments are conducted primarily by the Information Technology Division in support of system changes or new system implementations. Once assessments are completed, they are filed for review by the CEO. At this time there is no process for briefing the CEO on the assessments slated for review. Further, at this time there is no process to track or otherwise ensure mitigation plans are submitted and executed. Recommendation one: The risk assessment program falls under the purview of the newly hired Director of Risk Management. Oversight will include development and ongoing support of all policy, procedure and standards documentation related to the program. Recommendation two: Only those assessments that result in a high risk score should be submitted to the CEO for approval. Assessments that result in a moderate risk score should be addressed by the appropriate Administrator. Assessments that result in a low risk score should be addressed by the appropriate Department Director. Recommendation three: The risk assessment database be converted to a web-based application, made available to all UMC management personnel and support as a production application by UMC IT.	11/01/2012

Summary Audit Findings & Recommendations			Summary Management Disposition		
Ref	Finding	Recommendation(s)	Concurrence	Management Response & Action Plan	Mgmt Action Due Date
4 Inconsistent Compliance With Key Control Policy					
	Department managers are inconsistent in applying the key controls outlined in administrative policy for the locked shredding bins.	We recommend the UMC Associate Administrator of Professional Services direct department managers to review their key control practices and verify that only authorized people have access to recycle bin keys. We also recommend that she direct Plant Operations to periodically audit how keys and fobs are issued, verify that the responsible employee signs receipt for the key, and understands their duty to immediately report loss or theft of a key or fob. Such audits will identify if the policy and procedure is effective or requires revision. Audit reports and actions taken as a result need to be documented and retained for six years.	Y	Policy will be reviewed and revised if needed; staff education will be provided on the proper procedure regarding key control and access to recycle bins. Public Safety and Plant Ops will conduct periodic audits on keys and fobs.	11/01/2012
5 Physical Access Allowed to Individuals without a Current Business Need					
	There is no written organization-wide procedure for notifying all data systems owners about terminations or changes to be made to users access privileges.	The Chief Executive Officer should direct staff to identify and document procedures that will ensure all UMC data owners are routinely and consistently notified when any workforce member separates from UMC. The organizational procedures should assign responsibility for coordinating and periodically monitoring the process to ensure all user access is terminated in a reliable fashion. The Director of Public Safety should document how UMC badge access provided to outside entities, such as law enforcement or surveyors, is controlled. Additionally, the Director of Information Technology should revise administrative policy I-205 to correctly label the Information Security Program policy as "I-212".	Y	Public Safety does not issue hospital access to outside non-county agencies. We issue identification badges (visitor) badges only that have no access capabilities. Public Safety does have 3-Master Access badges in a safe in our control should a law enforcement emergency develop and there be a need for them to have access throughout the facility. IT will review policy changes will be made and sent for approval.	11/01/2012

Summary Audit Findings & Recommendations			Summary Management Disposition		
Ref	Finding	Recommendation(s)	Concurrence	Management Response & Action Plan	Mgmt Action Due Date
6	Failure to Document Activity Review Audits				
	The Emergency Services Department policy describes periodic reviews that are done to ensure access to its information system is done for legitimate business reasons only. No evidence was found that such reviews are being done. Users are granted access based on job role but there is no documentation of what roles are given which privileges.	The Director of Emergency Services should document the methodology being used to conduct user audits, the results and any actions taken in response to the results, and retain the documentation for at least six years. Additionally, he should formalize the role-based access matrix as part of department policy.	Y	ED policy 5.03 has been in place since 9-7-06 and specifically outlines the ED quarterly follow up. It describes the methodology that is used to audit the charts, and how management will respond to any concerns. I have updated the policy to include the role-based access matrix that had previously been established. In addition, the ED Informatics Coordinator has developed a database that will be used from this point forward to track the quarterly audits, the results, and any resulting actions.	08/15/2012