Audit Brief

UMC HIPAA Compliance Review

Twenty-nine UMC cost centers achieved a compliance rate of 82% in awareness and application of privacy and security policies.

Why we did this audit

We performed the second of a three-part audit of UMC employees' awareness and understanding of its privacy and security policies and their use of appropriate safeguards to protect health information based on our annual audit plan.

Background

UMC, as a covered-entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), is required to have administrative, physical and technical safeguards in place that meet the privacy and security standards. Policies and procedures, awareness training and annual refresher training are provided to employees about patients' rights, appropriate use of information systems and secure destruction of information.

UMC's policies require all members of its workforce to comply with the established privacy and security practices. Individual awareness minimizes UMC's risk of denying a patient his or her rights to privacy and confidentiality.

Using observations and staff interviews, each UMC department is reviewed once in a three-year audit cycle.

Summary of Significant Findings

UMC has administrative policies and procedures in place regarding the required privacy and security standards. Seven departments earned commendations for achieving a 100% rating. Consistent with the findings reported in the first part of this audit in 2008, we found awareness varies according to job role. Additionally we found:

- A low level of understanding of how patients are educated about their privacy rights or how to confirm a patient has received the Notice of Privacy Practices.
- Lack of awareness of how patients exercise their privacy rights.
- Lack of organizational procedures for identity theft response.
- Unsecured computer workstations and medical records.
- Inconsistent compliance to the required disclosure recording procedures.
- Improved compliance with disposal practices.

We Recommend

- Administrative division heads verify that managers provide staff education regarding patient privacy rights education.
- The Revenue Cycle Director develop and implement organizational procedures to detect, prevent, mitigate and respond to situations involving possible identity theft.
- The administrative division heads verify that risk assessments are conducted by appropriate managers to identify vulnerabilities in cost centers.
- The administrative division heads verify that managers have identified where procedures need to be implemented and that those procedures are implemented.
- A review of the manager orientation and training checklists to ensure awareness of specific responsibilities related to privacy procedures.

Jeremiah P. Carroll II, CPA
Audit Director
Clark County Audit Department

September 2009

View the entire report at www.accessclarkcounty.com.