UNIVERSITY OF CALIFORNIA, IRVINE
ADMINISTRATIVE AND BUSINESS SERVICES
INTERNAL AUDIT SERVICES

HIPAA PRIVACY
Report No. 2012-202

January 17, 2012

Prepared by:
Gregory Moore
Audit Manager

Reviewed by:
Mike Bathke
Audit Manager

Reviewed by:
Bent Nielsen
Director

IRVINE: INTERNAL AUDIT SERVICES

January 17, 2012

MARION MALLORY
CHIEF COMPLIANCE AND PRIVACY OFFICER
ASSISTANT DEAN OF COMPLIANCE
SCHOOL OF MEDICINE DEAN'S OFFICE

RE: HIPAA Privacy
Report No. 2012-202

Internal Audit Services has completed the review of HIPAA Privacy and the final report is attached.

We extend our gratitude and appreciation to all personnel with whom we had contact while conducting our review. If you have any questions or require additional assistance, please do not hesitate to contact me.

Bent Nielsen

Bent Nielsen
Director
UC Irvine Internal Audit Services

Attachment

C: Terry Belmont, Chief Executive Officer, UC Irvine Medical Center
Ralph Clayman, Professor and Dean of the School of Medicine
Alice Issai, Chief Operating Officer, UC Irvine Medical Center
Jim Murry, Chief Information Officer, UC Irvine Medical Center
Audit Committee

HIPAA Privacy
Report No. 2012-202

I. BACKGROUND

University of California, Irvine (UCI) Internal Audit Services (IAS) conducted a review of selected components of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule at the request of the University of California (UC), Office of the President. The HIPAA Privacy Rule was enforceable on April 14, 2003, and imposed a number of obligations on covered entities regarding the manner in which they use and disclose protected health information (PHI) and provided certain rights to patients related to the use and disclosure of their PHI. This review focused on the following specific obligations and patient's rights.

Obligations:

1. Use and disclosure of PHI for fundraising purposes;

2. Proper disposal of PHI in both paper and electronic formats; and

3. Accounting for certain disclosures of PHI to enable the covered entity to produce an accounting of such disclosures should a patient request one.

Patient Rights:

1. Right to access and/or copy information in the designated record set held by a covered entity.

This review was performed at all UC campuses with medical centers using a standard system-wide audit program that was developed for the HIPAA Privacy review.

II. PURPOSE, SCOPE AND OBJECTIVES

The purpose of the audit was to determine whether health system process controls implemented by UCI effectively mitigate the compliance risk associated with selected HIPAA privacy regulations identified for focused review by UC HIPAA Privacy Officers. The scope of the audit included the following processes impacted by the HIPAA Privacy requirements:

- Fundraising;
- PHI disposal;
- Patient access to PHI; and
- PHI disclosure documentation and monitoring.

The audit period for this review was from July 2010 to present. The following objectives were established:

1. Determine whether patient information has been used appropriately for fundraising purposes and whether existing procedures for collecting and using patient information is in compliance with federal and UC policy on HIPAA Uses and Disclosures for Fundraising;

2. Determine whether procedures have been established for the disposal of PHI and if UCI policies and procedures are in compliance with federal and UC policy requirements for safeguarding and disposal of PHI;

3. Determine whether patients' requests for access to PHI are fulfilled in accordance with federal, state, and UC policy requirements;

4. Determine whether PHI disclosures are documented, monitored, and reported in accordance with federal and state regulations and UC policy; and

5. Perform a limited review of related IT operations.

III. CONCLUSION

In general, the processes that have been implemented appear to be functioning as intended to mitigate compliance risks associated with the selected HIPAA Privacy regulations. However, business risks and control concerns were identified in access and accounting for PHI used for research purposes, security and storage of electronic media devices, and retaining medical waste certificates of disposal.

Observation detail and recommendations were discussed with management, who formulated action plans to address the issues. These details are presented below.

IV. OBSERVATIONS AND MANAGEMENT ACTION PLANS

1. Access and Accounting for PHI used for Research Purposes

Background

Under the HIPAA Privacy Rule, covered entities are required to account for disclosures of PHI for research purposes under Institutional Review Board (IRB) approved waivers of authorization.

Observation

IAS reviewed the procedures for requesting, documenting and reviewing patient medical record charts for research purposes for hospital based clinics. One of the clinics reviewed did not have an adequate process in place to ensure compliance with policy and as a result, the clinic may not be able to provide an accurate accounting for a research disclosure request under a HIPAA wavier of authorization. The following issues were noted:

a. Clinic personnel do not verify on a consistent basis that a protocol has been approved by the IRB to access medical records for research and that the individuals requesting and reviewing the charts are listed on the protocol and are authorized to access the data for research purposes under a HIPAA wavier of authorization. In addition, a copy of the IRB approval letter and the protocol narrative was not maintained at the clinic to ensure compliance with University policies;

b. The clinic is not maintaining on a consistent basis an official list of patient medical records used for research. This process makes it difficult and very time consuming to provide an accurate accounting for a research disclosure request under a HIPAA wavier of authorization for protocols of less than 50 enrolled patients.

To ensure compliance with the HIPAA Privacy Rule clinics that maintain their own medical records should establish a process that is consistent with Health Information Management's (HIM) procedures.

Management Action Plan

The Privacy Analyst and Assistant Director of HIM will prepare directed training specific to the HIPAA compliant process regarding the release of medical records for research for those areas maintaining their own medical records. Nurse managers and medical record staff from those areas will be required to attend the training sessions. The training sessions will include the following:

a. Instruction on how to read an IRB approved protocol granting waiver of authorization to ensure individuals requesting and reviewing the medical records are listed on the protocol and are authorized to access the data for research purposes;

b. Documenting and retaining adequate information specifically identifying medical records as being used for research purposes.

The estimated completion date is July 2012.

2. Security and Storage of Electronic Media Devices Prior to Disposal

Background

Electronic media devices that have been removed from mainframes, servers, desktops, laptops, and other hardware are stored in two locations prior to disposal.

Observation

IAS performed a walkthrough of the Network and Desktop Computing suite and noted that devices containing PHI are stored in a locked filing cabinet. However, the key to the cabinet is a common key number so anyone with that same key number and access to the office would have access to the devices containing PHI.

In addition, there was no formal process established to track electronic media devices prior to disposal.

Management Action Plan

IAS brought this to the attention of the Information Security Officer who took immediate action to resolve the issue and has implemented and/or revised the following policies and procedures.

- A thorough inventory of all media to be destroyed is now being maintained.
- Health Affairs Information Services (HAIS) has established an agreement with a media disposal vendor, Shred Confidential, who will provide UCI with secure locking containers for holding all media during the collection process. The keys for these containers will be controlled by HAIS Security.
- HAIS has relocated the holding area for electronic media and this area is a badge access controlled location restricted only to limited HAIS workforce.

3. Medical Waste Certificate of Disposal

Background

Environmental Services is responsible for ensuring that all medical waste and waste containing PHI generated by UCI Healthcare facilities are stored, transported, and disposed of in accordance with federal regulations, regulatory agencies, UC and local policies and procedures.

Observation

IAS reviewed the 2010 and 2011 binders containing the medical waste documentation to determine if the certification of destruction was on file for each Medical Waste Tracking form and Service receipt and determined there was no certification of medical disposal on file in the binders for several dates reviewed.

The Medical Center is required to track medical waste and retain treatment/disposal documentation on site for a minimum of three years. Failure to track the waste and maintain treatment documentation may result in misappropriation of PHI information and/or regulatory actions.

Management Action Plan

This information was brought to the attention of the Director of Environmental Services. He stated they will audit the binders for 2009, 2010, and 2011 and request any missing certifications of medical waste disposal from Stericycle and retain them on file in the respective binders. Estimated completion date is June 2012.