

**THE UNIVERSITY OF IOWA**

**Internal Audit Department**

**University HIPAA Compliance**

**Issued: June 28, 2004**

**Distribution List**

**David J. Skorton – President**

**Michael Hogan - Provost**

**Christopher Squier – Interim Associate Provost, Health Sciences**

**Ann Rhodes – Assistant to the Provost and HIPAA Privacy Officer**

**Mark Schantz – General Counsel**

**Gay Pelzer – Senior Associate Counsel**

**Grainne Martin – Senior Associate Counsel**

**Terry Johnson – University Controller**

**Internal Audit Management Committee**

**Board of Regents Office, State of Iowa**

**Office of Auditor of State**

# **INTERNAL AUDIT REPORT**

## **University HIPAA Compliance**

### **BACKGROUND**

On April 14, 2003, the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations were implemented. The federal privacy standards associated with HIPAA were created to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. The new standards provide patients with access to their medical records and more control over how personal health information is used and disclosed. The standards represent a uniform, federal floor of privacy protections for consumers across the country.

The University of Iowa has been designated a Hybrid Entity. A hybrid entity is a covered entity whose business activities include both covered and non-covered components.

Covered components fall under the HIPAA Privacy Rule and include three categories; 1) health plans, 2) health providers, and 3) healthcare clearing houses.

The HIPAA Privacy Rule has four main requirements which are:

1. Training and education.
2. Creation of a Privacy Notice to be given to patients.
3. Creation of Policies and Procedures.
4. Business Associate agreements.

The University has designated a HIPAA Privacy Officer to ensure that procedures are adopted and followed in all areas of the University. UI Health Care HIPAA compliance is handled by the Joint Office for Compliance.

### **PURPOSE AND SCOPE**

In January 2004, an audit report was submitted to the Iowa Board of Regents regarding UI Health Care HIPAA compliance, which is excluded from this report. The purpose of this audit was to identify and review processes in other areas of the University where the HIPAA regulations apply and to verify that:

- Policies and procedures are in place.
- All appropriate University employees have attended HIPAA training.
- University of Iowa employees are compliant with the HIPAA privacy regulations.
- Privacy Notices are given when appropriate.
- Business Associate agreements are in place.

The following Colleges and departments were included in the scope of this audit:

- College of Dentistry
- College of Pharmacy
- College of Nursing
- College of Public Health

- Research - IRB
- The University Hygienic Laboratory
- University Staff Benefits
- The Department of Speech Pathology and Audiology
- The Department of Psychology
- University Athletic Trainers

## DISCUSSION AND CONTROL RECOMMENDATIONS

### 1) Training

***Discussion*** - The HIPAA Privacy Officer has made a concerted effort to provide training for all areas of the University where the HIPAA Privacy Regulations apply. Training presentations are tailored to the audience and specific concerns are addressed. However, interviews with key personnel and auditing of documentation within the departments identified significant gaps in training. Some departments had controls in place to ensure that newly hired employees received HIPAA training as part of their orientation while others did not. Students, who have access to protected health information (PHI), received HIPAA training during new student orientation and through reminders during course work. Pharmacy and Nursing students, who do teaching or clinical rotations, go through HIPAA training at each site.

Gaps exist in training for employees who occupy the same physical space. Staff Benefits personnel have received HIPAA training but Payroll personnel who are separated from Benefits personnel by a simple walkway and have the ability to see PHI on desks and computer screens have not been trained. Also, custodians who clean the University Services Building and Information Systems personnel who manage sensitive data and systems in that building have not been through HIPAA training. University HIPAA training is necessary to ensure that all employees and appropriate students are familiar with the rules and University policies.

***Control Recommendation*** – Management must ensure that all appropriate students and staff have attended HIPAA training and are familiar with the associated University policies. Corrective action should include the following:

- Each department/college HIPAA contact must be responsible for identifying individuals who need training and create and maintain a database to track attendance.
- HIPAA training forms should be signed by the employee when they attend training sessions and be retained in personnel files to provide documentation of training completed.
- Support personnel, who have access to PHI, must be trained, i.e. Payroll, Facilities personnel, Information technology, Accounts Payable, etc.
- Training should include the need to prevent access to PHI through casual observation of computer screens and hard copy forms by clearing desks, locking data at night and logging off unattended computers.

- Training should emphasize the need to restrict the data transfer of PHI through email to ensure confidentiality in the absence of an encrypted email system.
- Create web based HIPAA training to increase accessibility of training materials and to track those who have accessed the material using the HawkID system.

**Corrective Action by Management** – Basic information about HIPAA confidentiality and privacy protection will be included in the general University orientation for new employees. Departments will be required to identify and train new staff members in the specifics of HIPAA compliance within their area and document attendance via the HIPAA training form. The form will be retained in the employee's personnel file. Each department will also be tasked with creating a system for tracking HIPAA training at the point of employment or transfer to a covered unit. Spot audits will be conducted within 30 days and each quarter thereafter to ensure continued compliance.

Web based training, using the HawkID as a tracking mechanism, will be implemented. The training will be located on the UI Benefits website and be available when information on additional HIPAA security procedures are disseminated to staff. Training for staff housed in the University Services Building will take place during the summer of 2004.

**Individual Responsible** – University HIPAA Privacy Officer **Target Date** –December 2004

**Auditor's Comment** – Training documentation will be tested during a follow-up review.

## 2) Privacy Notice

**Discussion** - Testing was performed for the College of Dentistry to determine the level of compliance for documenting the distribution of Privacy Notices. Privacy notices are readily available in the clinics and at the reception desks. The Windent patient accounting system has an alert that tells check-in staff whether the patient has received a notice. If the alert is not present on the screen, the notice has been given. A report was run out of the Windent system for all patients who had appointments after April 2003. The report identified a large number of patients who still had the alert present in the system and therefore had not received the privacy notice.

A review of the hard copy patient records was also performed to determine compliance with the privacy notice rule and to validate the accuracy of the Windent privacy alert. The review identified four instances where there was no hard copy acknowledgement that the Privacy Notice was given. Assuming that the hard copy records are correct, the Windent alert was incorrect on three of the patients. Conflicting data exists between the hard copy record and the Windent system.

The Department of Speech Pathology and Audiology, in the College of Liberal Arts and Sciences, records PHI in a medical record that is separate and distinct from

University of Iowa Hospitals and Clinics. The medical records are stored in the Wendell Johnson Speech and Hearing Center and are locked in a secured area. Per University policy, a written acknowledgement of the receipt of the HIPAA privacy notice should be stored in the medical record. A random sample of 10 medical records was reviewed to test for compliance with the policy. The acknowledgement form was missing in more than half of the records.

**Control Recommendation** – College of Dentistry management must take prompt action to synchronize the data between the Windent system and the hard copy records. Privacy notices should be mailed to every patient on the Windent report to bring the College into compliance with the HIPAA regulations. Once the privacy notices are mailed, the Windent system alert should be edited to reflect the activity. Training for check-in staff should re-enforce the need to address the HIPAA Privacy Notice acknowledgement form and the alert in the system. Periodic audits of the medical records and the Windent report would provide good controls to ensure continued compliance.

The Department of Speech Pathology and Audiology must ensure that all patients seen after April 14, 2003 have signed a privacy notice acknowledgement form. The department Secretary can utilize the database flag, "Privacy Notice Given," in the software used to assign new patient numbers to track and record the acknowledgement form. A report of all patients seen after April 14, 2003 should be created so that Privacy Notices can be mailed to bring them into compliance. A copy of that form or letter must be retained in the medical record and the database flag must reflect the same activity.

**Corrective Action by Management** – Immediate actions will be taken in the College of Dentistry to send privacy notices to those patients for whom the Windent system report does not show receipt of the privacy notice. Short term actions include staff training to document, on the registration form and on the Windent system, that the patient was given the notice. Long term actions include quarterly audits to reconcile the Windent report with patient records and to observe clinic procedures.

In the Department of Speech Pathology and Audiology, immediate steps will be taken to ensure that deficiencies are corrected regarding documenting the receipt of the privacy notice and filing the information in the patient record. In addition, the HIPAA Privacy Officer will review all consent forms and other documents currently in use in the clinic, as well as the policy and procedure manual.

***Individual Responsible*** – HIPAA Privacy Officer ***Target Date*** – December 2004

**Auditor's Comment** – The College of Dentistry and Department of Speech Pathology and Audiology have agreed with the corrective actions. Auditor will test patient records and review information from the Windent system to ensure compliance during the follow-up review.

### 3) Address for HIPAA Privacy Officer

**Discussion** – Various HIPAA documents were reviewed in each of the areas to determine whether they were adequate to address compliance with the Privacy Rules. The address for filing complaints or submitting questions on several of the forms was incorrect. The HIPAA Privacy Officer's office has moved locations several times in the past year, and the address on the forms has not been modified to reflect the move.

**Control Recommendation** – The mailing address of the HIPAA Privacy Officer must be accurate on all forms so that patients are able to contact the office. Any change in office location or mailing address must be communicated to all appropriate departments so that forms can be updated. Periodic reviews or random audits of the forms used in each area would assist in ensuring accuracy.

**Corrective Action by Management** – The office of the HIPAA Privacy Officer has been permanently located, and all forms will be revised to reflect the new location.

**Individual Responsible** – HIPAA Privacy Officer **Target Date** – July 2004

**Auditor's Comment** – A review of pertinent forms will take place during the follow-up review.

### 4) Accessibility of PHI

**Discussion** - The College of Dentistry's Windent system contains a vast amount of PHI. The HIPAA privacy rules require that employees have access to the "minimum necessary" amount of information to do their jobs. There are approximately 700 Windent users set up in 29 different security categories. Of the 29 security categories, 24 have the ability to "View All Clinic Appointments" and 24 have the ability to view the "Patient Ledger." Each of those functions gives the user access to PHI for all patient populations which may not be needed for their job. Users include Staff, Students, Faculty, Residents, etc. Deactivation of access to the Windent system for terminated employees should take place immediately upon notification of termination from the Human Resource Office. Testing was performed to identify terminated employees who still have active user ID's. A small number of ID's were identified.

One department stored computer backup tapes with PHI in a fire proof safe in the Information System Administrator's home. Another department was transmitting large volumes of PHI to a business associate via an attachment to email. Casual observation during a walk through of the departments identified PHI on computer screens and on desks that should be secured when the work station is unattended.

**Control Recommendation** - Management should refine/restrict user security within the Windent system so that employees and students have minimum necessary information to do their jobs. Absent the ability to refine the security because of software constraints; 1) monitoring tools should be put in place to identify users who inappropriately access a patient's account and 2) additional training and

reinforcement should take place via newsletters, mass emails to the college or through other appropriate media to ensure continued compliance with the HIPAA privacy regulations. User ID's for terminated employees should be deactivated immediately. A consistent process should be implemented to ensure future employee terminations are communicated to the appropriate IT personnel responsible for system security.

An alternative means of storage should be identified for all University data stored at the employee's home. Management should work with University ITS to identify storage space for the data so that security of PHI is maintained and information is readily accessible.

Although the use of encrypted email systems are not a requirement of the HIPAA Privacy Rule, the risk of a material breach or disclosure of PHI is very high using email attachments in an unencrypted system. Because the liability to the University is significant, alternative means of transferring PHI to business associates must be found. Secure servers or virtual private networks are options that may be available for secure transmittal of data.

*Corrective Action by Management* - The HIPAA Privacy Officer has met with the College of Dentistry's HIPAA Officer to discuss 1) monitoring tool for Windent access; 2) ensuring that employees who have terminated no longer have access to PHI or the system; 3) educational programs for new and current staff to address this issue and 4) a system and communication plan for reminding staff of their responsibilities under the Privacy Rule. The limitations of the Windent system present some challenges which will need to be addressed through robust education efforts, rigorous monitoring and continuous testing. A process will be put in place to notify the information technology office of transfers and terminations.

The Privacy Officer has discussed storage of PHI in the employee's home, and the department has taken corrective action regarding this item.

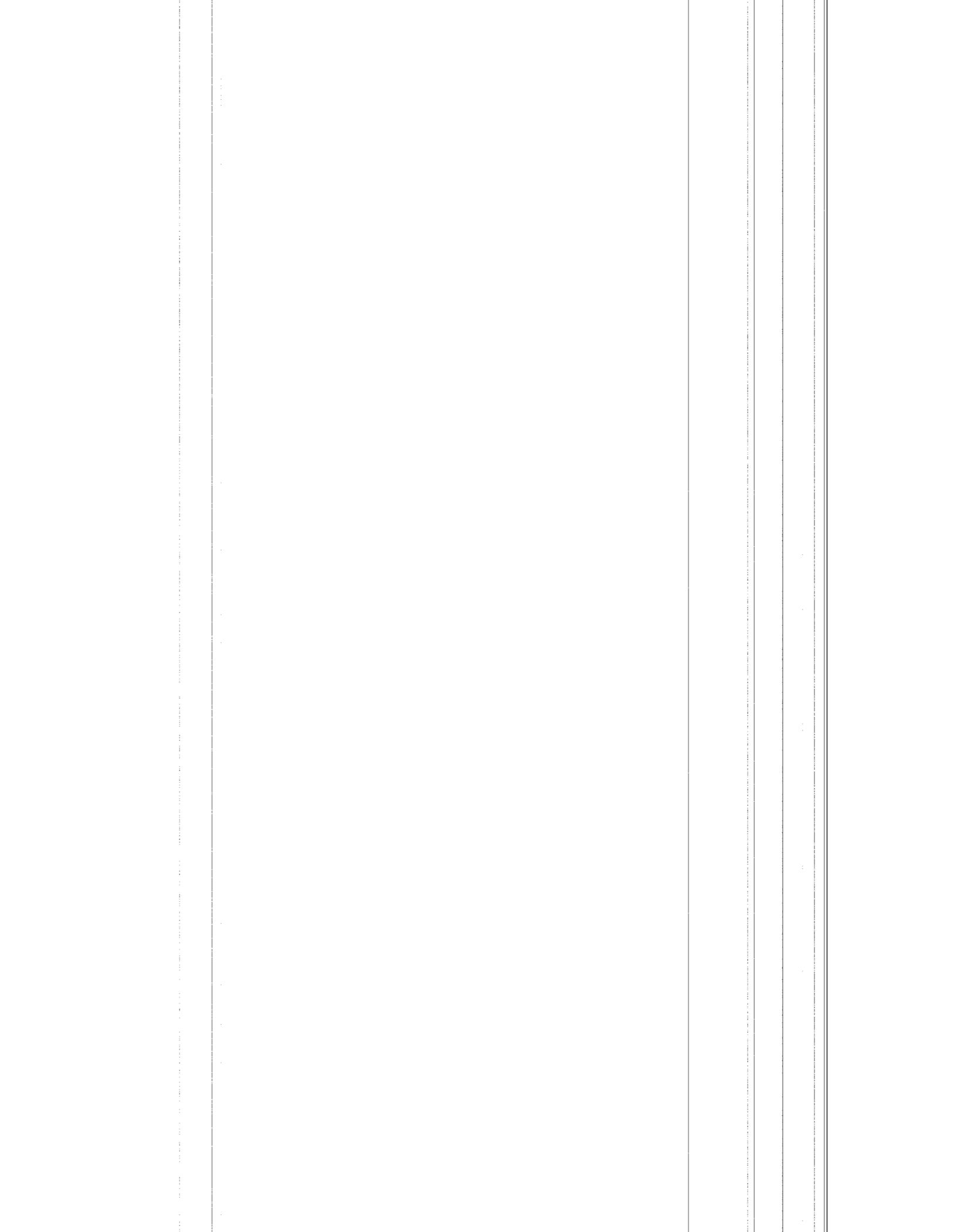
Implementation of a new process which requires the business associate to sign into a secure server to access PHI was implemented on April 19, 2004.

*Individual Responsible* – HIPAA Privacy Officer *Target Date* – December 2004

*Auditor's Comment* – Auditor will verify that the new controls are in place and working as intended during a follow-up review.

##### 5) Business Associate Database

*Discussion* - Business Associate agreements are required for a person or entity that provides services on behalf of any covered entity at the University involving the use and/or disclosure of PHI. The University's Business Associates policy states, "The University will identify its Business Associates and maintain a database of Business Associates." Internal Audit requested a copy of the database information or a listing



of business associates. The information was not readily available. The HIPAA Privacy Officer was not aware of several pending business associate agreements.

**Control Recommendation** - The HIPAA Privacy Officer should create and maintain a database for all Business Associate agreements per University policy. Re-enforcement of the University's policy on Business Associate agreements must also take place through additional training or other means of communication to ensure the HIPAA Privacy Officer is aware of pending agreements.

**Corrective Action by Management** - The Privacy Officer will compile a complete database of Business Associate Agreements. Currently, there are several lists and copies of Business Associate Agreements contained in hard copy files at the Associate Provost for Health Science Office. The lists will be merged and will include those that are in the files. The need to notify the HIPAA Privacy Officer of new or pending business associate agreements will be addressed during training.

***Individual Responsible*** – HIPAA Privacy Officer ***Target Date*** – August 2004

**Auditor's Comment** - Auditor will verify that the database exists and is current during a follow-up review.

#### **6) Covered versus Non-covered Components**

**Discussion** - The University has been classified as a "hybrid" entity because there are covered and non-covered components within the entity. The initial evaluation and classification of departments and colleges within the University took place via a survey that was sent out by the General Counsel's office. One factor influencing the covered/non-covered decision was whether the unit had a billing function.

There are areas currently considered non-covered which should be reviewed again to determine whether the HIPAA rules apply. The University Counseling Service provides a variety of assistance and accumulates sensitive health care data. Some of the services they provide include: individual counseling and psychotherapy, group counseling and psychotherapy, psychological testing, etc. Per the Counseling Service brochure, "Except for selected tests, our services are provided without charge." The Counseling Service does charge for selected tests, and therefore meets the billing criteria.

**Control Recommendation** – The HIPAA Privacy Officer should evaluate the status of all covered and non-covered components of the University. Benchmarking with peer institutions would also provide perspective regarding classification of like units on other campuses. Documentation of whether a unit should/should not be re-classified as a covered component should be kept on file. If re-classification does take place, personnel must immediately be trained to gain an understanding of the HIPAA Privacy regulations and to ensure consistent application of the University's HIPAA policies and procedures.

Corrective Action by Management – The HIPAA Privacy Officer will review the classification of entities under the current hybrid designation and report to upper management the methodology used for the new review, and documentation for any resulting recommendations to change a specific components status.

*Individual Responsible* – HIPAA Privacy Officer *Target Date* – December 2004

Auditor's Comment - Auditor will review the documentation and reports during a follow-up review.

## 7) HIPAA Committee

Discussion – During the initial implementation of the HIPAA privacy regulations, a committee of various University personnel from different disciplines was put together to assist in guiding implementation of the rules. The committee met once a month to discuss specific concerns but was disbanded after the initial implementation. The HIPAA Privacy Officer has the authority to make decisions regarding HIPAA compliance but should work with other University personnel knowledgeable about the HIPAA regulations for support in their implementation.

Discussion is on-going regarding interpretation of the HIPAA Privacy regulations and how they apply to non-covered components in the hybrid designation, i.e. Athletic Trainers. However, a committee's evaluation of these components 18 months after the original implementation date would be helpful in resolving conflicts.

Control Recommendation – The HIPAA Privacy Officer should re-convene members of the disbanded HIPAA committee to assist in addressing areas of concern throughout the University. Meetings should be held on a regular basis with meeting minutes to document progress towards compliance in critical areas. The committee would provide support to the Privacy Officer by encouraging areas throughout the University to remain focused on HIPAA compliance both now and into the future.

Corrective Action by Management – The HIPAA Privacy Officer will re-convene the HIPAA committee to provide support and guidance in the implementation of current and future HIPAA regulations.

*Individual Responsible* – HIPAA Privacy Officer *Target Date* – August 2004

Auditor's Comment – Auditor will attend a committee meeting and read meeting minutes to verify the committee is in place.

## SUMMARY

Implementation of the HIPAA Privacy Regulations at the University of Iowa has in large part been very successful. While gaps in training and documentation still exist, the HIPAA Privacy Officer has immediately responded to recommendations for addressing

University of Iowa Internal Audit Department

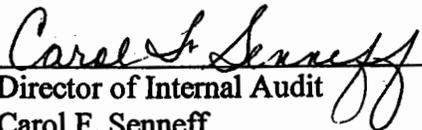
areas of continued risk. Monitoring compliance will require dedicated resources going forward, especially in light of the pending HIPAA Security Regulations which are to be implemented in the spring of 2005. A follow-up review will be conducted in the third quarter of fiscal 2005.



Auditor In-charge  
Debra A. Johnston



Audit Manager  
Richard R. See



Director of Internal Audit  
Carol F. Senneff