OFFICE OF AUDITOR OF STATE

STATE OF IOWA

David A. Vaudt, CPA
Auditor of State

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834 Facsimile (515) 242-6134

NEWS RELEASE

Contact: Andy Nielsen
515/281-5834

FOR RELEASE January 28, 2013

Auditor of State David A. Vaudt today released a report on a review of selected general and application controls over the University of Iowa Hospitals and Clinics' GE Centricity System for the period May 28, 2012 through July 30, 2012.

Vaudt recommended the University of Iowa Hospitals and Clinics strengthen procedures for the encryption of laptop computers. The Hospital has responded positively to the recommendation.

A copy of the report is available for review at the University of Iowa, in the Office of Auditor of State and on the Auditor of State's web site at http://auditor.iowa.gov/reports/1361-8010-BT01.pdf.

# # #

REPORT OF RECOMMENDATIONS TO THE UNIVERSITY OF IOWA HOSPITALS AND CLINICS ON A REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE GE CENTRICITY SYSTEM

MAY 28, 2012 THROUGH JULY 30, 2012

Office of

AUDITOR OF STATE

State Capitol Building • Des Moines, Iowa

David A. Vaudt, CPA
Auditor of State

OFFICE OF AUDITOR OF STATE
STATE OF IOWA

David A. Vaudt, CPA
Auditor of State

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834 Facsimile (515) 242-6134

January 2, 2013

To the Members of the
Board of Regents, State of Iowa:

In conjunction with our audit of the financial statements of the State University of Iowa (University of Iowa) for the year ended June 30, 2012, we conducted an information technology review of selected general and application controls for the period May 28, 2012 through July 30, 2012. Our review focused on the general and application controls of the University of Iowa Hospitals and Clinics' GE Centricity System as they relate to our audit of the financial statements. The review was more limited than would be necessary to give an opinion on internal controls. Accordingly, we do not express an opinion on internal controls or ensure all deficiencies in internal controls are disclosed.

In conducting our review, we became aware of certain aspects concerning information technology controls for which we believe corrective action is necessary. As a result, we have developed a recommendation which is reported on the following pages. We believe you should be aware of this recommendation which pertains to the University of Iowa Hospitals and Clinics' general controls over the GE Centricity System. This recommendation has been discussed with Hospital personnel and their response to this recommendation is included in this report. While we have expressed our conclusion on the Hospital's response, we did not audit the Hospital's response and, accordingly, we express no opinion on it.

This report, a public record by law, is intended solely for the information and use of the officials and employees of the University of Iowa, citizens of the State of Iowa and other parties to whom the University of Iowa may report. This report is not intended to be and should not be used by anyone other than these specified parties.

We would like to acknowledge the many courtesies and assistance extended to us by personnel of the Hospital during the course of our review. Should you have questions concerning any of the above matters, we shall be pleased to discuss them with you at your convenience. Individuals who participated in our review of the GE Centricity System are listed on page 6 and they are available to discuss these matters with you.

David A. Vaudt	Warren Jenkins
DAVID A. VAUDT, CPA Auditor of State	WARREN G. JENKINS, CPA Chief Deputy Auditor of State

cc: Honorable Terry E. Branstad, Governor
David Roederer, Director, Department of Management
Glen P. Dickinson, Director, Legislative Services Agency

GE Centricity System Controls

A. Background

The GE Centricity System at the University of Iowa Hospitals and Clinics (Hospital or UIHC) is a commercial application which is used for patient registrations, scheduling and the collection of information from a number of clinical systems to process billings and receivables for patients and insurance providers.

B. Scope and Methodology

In conjunction with our audit of the financial statements of the University, we reviewed selected aspects of the general and application controls in place over the Hospital's GE Centricity System for the period May 28, 2012 through July 30, 2012. Specifically, we reviewed the general controls: security management and segregation of duties and the application controls: interface controls and business process controls, including input, processing and output. We interviewed Hospital staff and we reviewed Hospital policies and procedures. To assess the level of compliance with identified controls, we performed selected tests.

We planned and performed our review to adequately assess those Hospital operations within the scope of our review. We developed an understanding of the Hospital's internal controls relevant to the operations included in the scope of our review. We believe our review provides a reasonable basis for our recommendations.

We used a risk-based approach when selecting activities to be reviewed. We focused our review efforts on those activities we identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, we use our finite review resources to identify where and how improvements can be made. Thus, we devote little effort to reviewing operations which may be relatively efficient or effective. As a result, we prepare our review reports on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address activities which may be functioning properly.

C. Results of the Review

As a result of our review, we found certain controls can be strengthened to further ensure the reliability of financial information. Our recommendation, along with the Hospital's response, is detailed in the remainder of this report.

General Controls

(1) Encryption of Laptops – Encryption helps protect sensitive information stored on portable devices by rendering data unintelligible to unauthorized users. The Hospital has established a policy requiring sensitive institutional data stored on portable devices to be encrypted when technically possible and is currently working to install encryption software on laptop computers. Encryption software has not yet been installed on all laptops which could store sensitive data. Also, the policy could be strengthened to require the encryption of all devices before any sensitive data is stored on the device, not just when it is technically possible.

Recommendation – The Hospital should strengthen the policy to require the encryption of any portable device before any sensitive data is stored on it and take steps to ensure all laptops are properly encrypted.

Response - University of Iowa Hospitals and Clinics has an existing policy requiring sensitive institutional data stored on a portable computing device or portable storage device must be encrypted when technically possible using an institutionally approved encryption product to protect data from unauthorized access in the event the device is lost or stolen. This policy was initially approved on June 17, 2007 and was revised and re-approved on September 12, 2011. In an effort to ensure all staff are familiar with this policy, Health Care Information Systems (HCIS) has been delivering a presentation on data secure and data loss prevention, which includes detailed information regarding this and other related policies. To date, this presentation has been delivered to UIHC administrative and clinical leaders, as well as clinical department administrators. HCIS is scheduled to deliver the same presentation to most of the clinical department before the end of the 2012 calendar year. In addition, senior leadership of UIHC has directed HCIS to direct any incidents of failure to comply with this policy to senior leaders for follow-up. HCIS is initiating an extensive external data security assessment which will include a review of compliance with this security policy and is expected to be completed by April 2013.

Conclusion – Response acknowledged. Portable devices and laptop computers present a risk until encrypted.

Application Controls

No recommendations were noted in our review of application controls for the Hospital's GE Centricity System.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Daniel L. Grady, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated in this review include:

Eric Rath, Assistant Auditor
Daniel Mikels, Assistant Auditor