SAN DIEGO: AUDIT & MANAGEMENT ADVISORY SERVICES
0919

July 17, 2015

ANDY LAMB
Director, Supply Chain Management Services
8870

Subject: ***Vendor Hosted Application Review***
Project 2015-21

The final audit report for Vendor Hosted Application Review, Audit Report 2015-21, is attached. We would like to thank all members of the department for their cooperation and assistance during the audit.

Because we were able to reach agreement regarding corrective actions to be taken in response to the audit recommendations, a formal response to the report is not requested.

The findings included in this report will be added to our follow-up system. We will contact you to schedule a review of the corrective actions, at the appropriate time.

UC wide policy requires that all draft audit reports, both printed (copied on tan paper for ease of identification) and electronic, be destroyed after the final report is issued. Please destroy draft reports at this time. Thank you.

David A. Meier

David Meier
Director
Audit & Management Advisory Services

Attachment

cc: E. Babakanian
M. Baggett
D. Brenner
J. Bruner
A. Bustamante
M. Harrison
P. Maysent
T. Moore
B. Ouellet
S. Vacca
K. Wottge

UC San Diego

AUDIT & MANAGEMENT ADVISORY SERVICES

Vendor Hosted Application Review
July 2015

Performed By:

Nai Hwang, Auditor
Jennifer McDonald, Manager

Approved By:

David Meier, Director

Project Number: 2015-21

Vendor Hosted Application Review
Project 2015-21

Table of Contents

I. Background

Audit & Management Advisory Services (AMAS) has completed a review of vendor hosted applications as part of the approved audit plan for Fiscal Year 2014-15. This report summarizes the results of our review.

The University of California San Diego Health System (UCSDHS) contracts with application service providers (ASP) to take advantage of state of the art software functions at a lower cost than what UCSDHS can provide internally. ASP vendors provide computer-based services to customers over a network communication path using a standard protocol. ASP vendors are responsible for providing updated versions of the software, storing data in a secure environment and meeting other contract terms and conditions. At times an ASP may transmit and store personal health information (PHI) as part of the application service provision. In these cases, the Health Information Portability and Accountability Act (HIPAA)[1] requires a business associate agreement (BAA) between UCSDHS, a HIPAA covered entity, and a HIPAA business associate (BA). This contract addresses security for personal health information (PHI) in accordance with HIPAA guidelines.

UCSDHS Procurement Services (Procurement), a division of Supply Chain Management, works with departments for ASP requisitions and contract negotiation. UCSDHS Purchasing Guidelines state that additional Health System Information Security (HSIS) approval is required for computer software and hardware purchases. Once approvals are obtained, UCSDHS Procurement proceeds with the acquisition process from requisition to contract execution.

HSIS performs security assessments on systems for compliance with UCSDHS security policies. HSIS had previously developed an Information Services System Questionnaire (ISSQ) to gather the information related to a particular project, such as: vendor, application data elements, system type, interface configuration, database description, policy compliance, web hosting, and back up and disaster recovery as part of the initial review process for new systems. They currently use an ASP Security Information Questionnaire with added elements of the UCSD Policy and Procedure Manual (PPM 135-3, *Computing Services: Network Security*), for areas regarding physical and network security, vendor staff management, and regulatory compliance.

The Data Security and Privacy Appendix (Appendix-DSP) is designed to address protection for the University of California's (UC) Protected Information and UC networks. In October 2014, UC updated Appendix-DSP to include the data security and privacy obligations of all third parties (including individuals and entities) that connect to UC networks and/or gain access to protected information. Appendix-DSP is a requirement as part of the purchasing contract legal documents, when third parties create, receive, maintain or transmit confidential information on behalf of the University. Appendix-DSP also contains specific language

[1] Guidelines for data privacy and security provisions designed to safeguard medical information.

regarding the need for an information security plan, examination of records (audit clause), and detailed computer system security requirements.

As of March 2015, the HSIS Vendor Application List contained a total of 342 systems/applications. Among these, 17 were categorized as approved virtual external ASP, and 14 of the 17 were in production.

II. Audit Objective, Scope, and Procedures

The objective of our review was to assess the risks associated with the ASP model and specific ASP vendors, on a sample basis, in providing security for UCSDHS data.

In order to achieve our objectives we completed the following:

- Interviewed the Procurement Director and Manager to obtain information on purchasing processes and ASP vendor management;
- Reviewed applicable federal requirements and University policies and procedures including, but not limited to:
  - ➢ UC Business and Finance Bulletin, IS-3 *Electronic Information Security*,
  - ➢ UCSD PPM 135-3, *Computer Services*,
  - ➢ UCSD MCP 703.1, *Centralized Purchasing*,
  - ➢ UCSDHS Purchasing Guidelines, December 2013,
  - ➢ UCOP Procurement Services - Quick Reference Guide to Legal Documents,
  - ➢ UCOP Procurement Appendix-DSP,
  - ➢ HIPAA, section 164.308 (b) (1): *Business associate contracts and other arrangements*;
- Interviewed the HSIS Chief Information Security Officer and staff to obtain information regarding ASP vendor security review processes and management;
- Reviewed the HSIS New Technology Assessment Process Flow and System Implementation Process and Roles, and Information Security Application Review Procedures (draft Jan 2015);
- Reviewed ASP vendors from the HS Application List and extracted a small sample for detailed testing;
- Reviewed the ISSQ and ASP Vendor Questionnaire for selected ASP vendors;
- Reviewed communication and documentation among relevant parties (department, HSIS, Procurement) for security review and contract terms;
- Inquired whether a process was in place to ensure contracts or agreements included a current BAA and other updates as part of privacy and security protection;
- Contacted one department for their business continuity plan related to the ASP software;
- Contacted one vendor for a third party audit report, certification, and security plan;
- Evaluated the appropriateness of continuous monitoring efforts for application security environments; and
- Performed a detailed security assessment for three virtual external ASP vendors to include fire wall control, inclusion of a BAA, Purchase Order, and vendor invoices.

III. Conclusion

We concluded that UCSDHS ASP vendor management processes were generally adequate and provided reasonable assurance that data was secure. Procurement processes ensured that HSIS review and approval was obtained prior to executing new contracts. We observed that secure communication protocols were used between the departments and ASP vendors for accessing and transmitting PHI data. However, we noted that ASP security assessments could be enhanced by requesting third party audit reports and/or certifications in addition to other supporting security documents. In addition, activities related to continuous monitoring[2], such as internal communication, periodic assessments, and contract enhancements, would further mitigate risks associated with ASP vendor security.

IV. Observations and Management Corrective Actions

A. ASP Security Assessment

ASP security assessments could be enhanced by requesting third party audit reports and/or certifications.

During our review of the sampled contracts, we noted that HSIS coordinated with the departments and vendors to complete the ISSQ and ASP System Vendor Questionnaire and performed a security assessment of the information prior to the department submitting the purchase requisition to Procurement.

In addition to the questionnaires, it appeared that some vendors provided additional documentation such as process/data flows, security policies, International Standards Organization certificates, disaster recovery plans, and/or application manuals. It was also noted that vendors may sometimes have a third party audit report (i.e. SAS 70) and/or certifications (i.e.SSAE16 SOC 2 Type 2 report) available for review as part of the initial HSIS security assessment. However, these items were not requested as part of the supporting documents for the security review. These types of reports/certificates should be consistently requested to provide an additional assurance of the vendor's security processes.

Management Corrective Action:

HSIS will request third party audit reports and/or certifications in addition to other security documentation to support a more thorough security review.

[2] The process and technology used to detect compliance and risk issues associated with an organization's operational environment.

B. Continuous Monitoring

A formal communication plan, including protocols for vendor updates or changes and periodic assessments of ASP security environments was not in place. In addition, a security audit clause was not available in the current contracting documents. These elements would allow for the ability to provide continuous monitoring to detect compliance and risk issues with ASP security.

Continuous monitoring is a process in which key business process transactions and controls are assessed on a regular, recurring basis. This permits ongoing insight into the effectiveness of controls and the integrity of transactions running within them. By monitoring business process systems and focusing on controls and transactions, errors, fraud, abuse and system inefficiencies can be detected on a timely basis.

Communication and Periodic Assessment Processes

During our review, we noted that the three ASP contracts selected for testing were merged or acquired by another company. However, there was no formal communication or information exchange between Procurement and HSIS regarding the vendor changes which would indicate the need for an assessment of potential changes in the ASP security environment. A current and new ASP Communication Flow is provided as ***Attachment A***.

In addition, we noted that a periodic security assessment process was not in place to proactively identify any changes in the vendor’s security. The absence of timely communication and periodic assessments increases the risks of having insufficient security which may result in compromised or lost data.

Management Corrective Actions:

Procurement and HSIS will develop a process to communicate ASP vendor updates and changes. In addition HSIS will include a process for periodic assessments as part of a continuous security monitoring plan.

Audit Clause

During our review we noted that the BAA included in ASP contracting documents did not contain an audit clause allowing a security audit to occur outside of a security incident. Section 3.9.1 of the BAA specifies the Universities right to request an audit of the vendor’s uses and disclosures of PHI only in the event of a breach or security incident. In addition, the vendor contract terms and conditions contained an audit clause that was specific to financial reports and other documentation related to financial activities. Therefore, UCSDHS was not entitled by contract to request security documentation or review security practices outside of the initial assessment performed during the requisition process, impacting the ability to perform continuous monitoring of ASP security.

Appendix-DSP Article 8 – "*Information Security Plan, D*, requires the vendor to review its Information Security Plan, update and revise if needed, and submit it to UC upon request; and Article 11 – *Examination of Records,* provides the right to examine and request security documentation and examine all records related to the Appendix-DSP. To ensure continuous monitoring and audit capabilities, Appendix-DSP should be included as part of all ASP contracts.

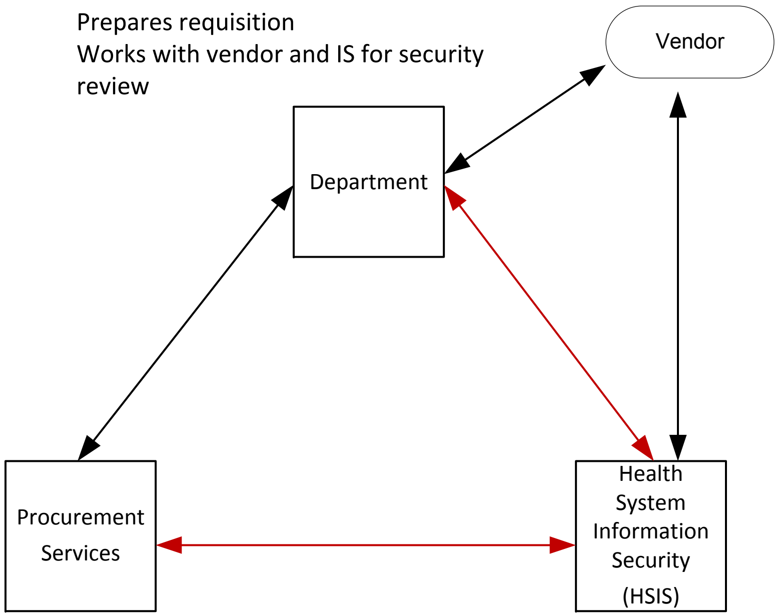
Management Corrective Action:

Procurement is now including Appendix–DSP with ASP contracts in addition to the standard BAA.

Vendor Hosted Application Review
Project 2015-21

Attachment A – ASP Communication Flow

New Contracts - ASP Communication Flow



Prepares requisition
Works with vendor and IS for security review

Vendor

Department

Procurement Services

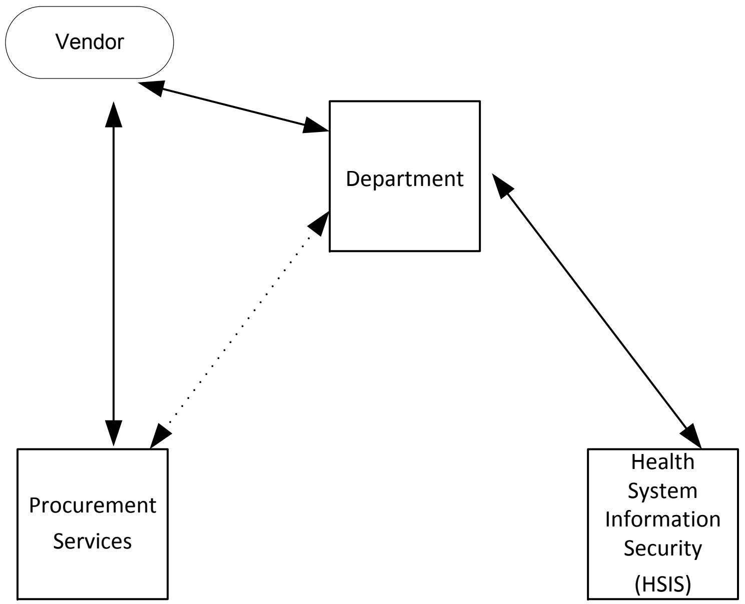
Health System Information Security (HSIS)

Reviews requisition
Reviews IS approval for vendor security
Prepares purchase order
Includes BAA and Appendix-DSP as part of contract

Performs security review
Works with vendor for security issues
Obtains related security documents

↔ A formal communication process for vendor information and security assessments among department, HSIS, and Procurement Services.

Existing Contracts - ASP Communication Flow



Vendor

Department

Procurement Services

Health System Information Security (HSIS)

○ HSIS was not aware of ASP contract or vendor changes.
As a result, a follow up security assessment was not conducted timely

○ weaknesses