UCIrvine | Internal Audit Services

School of Medicine Portable Computing and Electronic Storage Device Inventory

Internal Audit Report No. I2019-210

April 8, 2019

Prepared By
Julie Chung, Senior Auditor
Approved By
Mike Bathke, Director

UNIVERSITY OF CALIFORNIA, IRVINE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

INTERNAL AUDIT SERVICES
IRVINE, CALIFORNIA 92697-3625

April 8, 2019

VALERIE DIXON
INTERIM CHIEF COMPLIANCE & PRIVACY OFFICER
SCHOOL OF MEDICINE

SRI BHARADWAJ
DIRECTOR OF INFORMATION SERVICES AND CISO
UC IRVINE HEALTH

Re: School of Medicine Portable Computing and Electronic Storage Device Inventory
No. I2019-210

Internal Audit Services has completed the review of the School of Medicine (SOM) Portable Computing and Electronic Storage Devices inventory 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.

Mike Bathke
Director
UC Irvine Internal Audit Services

Attachment

C: Audit Committee
Francine Jeffrey, Associate Dean of Administration, SOM

I. MANAGEMENT SUMMARY

In accordance with the fiscal year (FY) 2018-2019 audit plan, Internal Audit Services (IAS) reviewed the UC Irvine Health (UCIH) policy, Controls on Portable Computing and Electronic Storage Devices, and SOM's procedures and processes for the inventory and asset management of portable computing and electronic storage devices. The review identified that procedures, processes, and internal controls were not established and implemented to minimize business risks, promote best business practices, or ensure compliance with University policies. The following observations were noted.

Policy Review – IAS reviewed the UCIH policy and determined that the policy procedures were not established with defined processes or steps and communicated to all appropriate SOM faculty and staff to ensure proper implementation. In addition, training, monitoring and oversight were not addressed in the policy. Further details related to this observation is provided in section V.1.

Inventory Review – IAS review also disclosed that portable computing and electronic storage devices purchased with SOM funds and used to receive, store, create, or transmit confidential or restricted information were not tracked, maintained, and updated in an inventory management system which is necessary to manage the life cycle of the University-owned devices. IAS found that only certain laptops purchased by Information Services or its designees were inventoried and that all other SOM purchases of electronic devices, including laptops, tablets, cellphones, were not inventoried. Details related to this observation is provided in section V.2**.**

II. BACKGROUND

UCI Health Sciences (UCIHS) encompasses the Susan and Henry Samueli College of Health Sciences (COHS), which includes the SOM, School of Nursing, the Department of Pharmaceutical Sciences, and the Program in Public Health, and UCIH, which includes the UCI Medical Center and affiliated healthcare offices.

At UCIH, both University-owned portable computing and electronic storage devices purchased by clinical departments in the SOM and personally-owned devices (laptops, tablets, smart phones, etc.) are allowed to access, process, store, and transmit confidential and restricted information. Information Services (IS) is responsible for addressing the information technology needs of UCIH and provides Client Services to the SOM, which operates clinical departments in UCI Medical Center. IS analysts serve as liaisons in the SOM dean's office and IS has also delegated four or five designated Health Sciences staff access to the IS database that is used to inventory certain laptop purchases.

Due to the inherent risks with portable electronic devices, such as unauthorized access, data breach, theft, or loss, the UCIH policy, Controls on Portable Computing and Electronic Storage Devices, was established to safeguard and protect confidential and restricted information such as protected health information on University or personal portable electronic devices.

III. PURPOSE, SCOPE AND OBJECTIVES

The purpose of this audit was to review SOM practices and processes related to UCIH policy on portable computing and electronic storage devices to assess the internal controls that have been implemented to minimize risks to the University. For testing purposes, the following objectives and scope were established.

1. Review the UCIH policy, Controls on Portable Computing and Electronic Storage Devices, to determine if the policy is complete, current, and up to date and assess whether the appropriate procedures and processes have been established and implemented to minimize business risks and promote best business practices. Assess if procedures exist to properly manage the life cycle of the University-owned portable computing and electronic storage devices (from procurement to decommissioning, or if necessary upon loss or theft).

2. Determine whether an inventory of portable computing and electronic storage devices purchased by the SOM is maintained and monitored. Review and assess current inventorying, monitoring and oversight processes that ensures that portable computing and electronic storage devices are accounted for, safeguarded, and secured from theft, loss, or damage. Determine if a device

inventory log is suitable and complete including audit logs and procedures to review them.

3. Perform sample inventory review to determine if all devices are safeguarded, secured, and accounted for loss, theft, or damage. During inventory review, determine if the employee agreement concerning the use of electronic communications resources (Appendix A of BFB-G-46) is completed and maintained for each employee that has been assigned a portable electronic device as required by University policy.

IV. CONCLUSION

The review found that the policy and SOM portable electronic device management practices and security procedures were not fully established and implemented as intended. Opportunities for improvement were noted in the areas of (a) establishing and implementing portable electronic device security policy procedures and processes, and (b) inventory and asset management of portable computing and electronic storage devices.

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

V. OBSERVATIONS AND MANAGEMENT ACTION PLANS

1. Policy Review

Background

In September 2017, as the policyholder, the Compliance & Privacy Office revised, approved, and issued the UCIH policy, Controls on Portable Computing and Electronic Storage Devices, which was last revised in May 2014. This policy was established to ensure that confidential and restricted information is protected on University issued as well as personal portable electronic devices, such as laptops, tablets, smart phones, etc., that are subject to loss, theft, damage, or data breach.

Observation

IAS reviewed this UCIH policy to determine if the policy was complete, current, and up to date and noted the following observations.

- Although the policy contained responsibilities and outlined security requirements, procedures with defined processes or steps were not established to ensure policy implementation.

- Policy requirements were not communicated to all appropriate SOM employees for proper implementation.

- Also, the procedures were not established for staff training, monitoring and oversight upon policy implementation.

- The Compliance & Privacy Office, the policyholder as far back as May 2014, does not have expertise in electronic information security.

In addition, IAS noted the work group organized to compose, review, and approve this policy was comprised of three offices, Risk Management, Compliance & Privacy, and Medical Staff Administration. Also, this policy addressed several policy stakeholders, including the Purchasing department, IS, UCIH/SOM department administrators, and all UCIH/SOM employees, medical staff, and other health care personnel, students and interns who use portable electronic devices to create, receive, or transmit confidential or restricted information within or outside of UCIH.

However, key policy stakeholders with a vested interest in the policy's implementation, IS, the Purchasing department and UCIH/SOM department administrators whose departments are most affected by the policy, did not participate in the work group to examine existing and related policies and practices; advise on whether conflicts exist with any other University policies or procedures; research critical issues connected to the topic; as well as on the feasibility, completeness, clarity, consistency, style, and format of the policy.

In addition, after reconciling any competing points of view, a draft of the proposed policy was not reviewed by a wider group of senior managers and administrators, along with legal review by the Office of Campus Counsel.

Management Action Plan

By December 31, 2019, UCI Health will work with Dean of SOM to implement the policy as outlined above. As part of the policy implementation, an inventory will be performed on SOM devices and hardware.

2. Inventory Review

Background

The UCIH policy, Controls on Portable Computing and Electronic Storage Devices, requires the installation of appropriate encryption and if compatible with mobile device management (MDM), which allows for remote data destruction, on mobile devices that receives, stores, creates, or transmits confidential or restricted information such as patient information in the event of loss, theft, damage, or data breach. In addition, the policy also requires proper disposal of the portable electronic devices at the end of its life cycle as well as retrieval of portable electronic devices from separating University employees.

Observation

IAS conducted a review of SOM practices to determine if an inventory or log was complete, current, and up to date to properly manage the life cycle of the University-owned portable electronic devices and protect from unauthorized access as noted above before a device was issued to a user.

IAS noted that a complete and accurate inventory of all SOM portable electronic devices is not maintained to track and monitor each devices' progression through inventory: acquisition, issuance, return, disposal as well as accounting for lost or stolen devices. IAS determined that only laptops purchased by IS or its designees were inventoried and that all other laptops, tablets, cellphones, etc. purchased by the SOM were not inventoried. As a

result, SOM is not able to determine if all portable electronic devices are adequately protected and accounted for and adhered to the policy requirements.

Internal controls, such as a proper, complete, and accurate inventory and asset management system should be maintained to ensure policy compliance.

Management Action Plan

By December 31, 2019, UCI Health will work with Dean of SOM to implement the policy as outlined above. As part of the policy implementation, an inventory will be performed on SOM devices and hardware.