UNIVERSITY OF VIRGINIA

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2019

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of the University of Virginia as of and for the year ended June 30, 2019, and issued our report thereon, dated November 22, 2019. Our report is included in the University's basic financial statements that it anticipates releasing on or around December 5, 2019. Our audit found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- instances of noncompliance or other matters required to be reported under Government Auditing Standards.

–TABLE OF CONTENTS–

STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

Improve Security Awareness Training Program
Applicable to: Academic Division
Responsible Department: Information Technology Services
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2016, with satisfactory progress in this area)

The University of Virginia Academic Division (Academic Division) is making progress to address an information security weakness communicated in our prior year audit report regarding improving the security awareness training program; however, corrective action remains in progress.

The Academic Division's Information Technology Services (ITS) established a process to track whether faculty and staff complete their annual security awareness training. Additionally, ITS established a procedure that requires employees to complete security awareness training in order to receive access to the Academic Division's highly sensitive network.

However, the process does not include security awareness training requirements for faculty and staff with access to other parts of the Academic Division's networks. Despite these network segments residing outside the highly sensitive network, they are used daily by the University's faculty and staff community to conduct business and to connect to web portals that connect to systems within the highly sensitive network. It is, therefore, imperative that these users receive security awareness training before, or as soon as practicable after, receiving their access. During calendar year 2018, 2,318 out of 7,093 faculty and staff (33%) that do not have direct access to the highly sensitive network did not complete their assigned training.

The Academic Division's adopted information security standard, ISO 27002 (Academic Division Security Standard), section 7.2.2, states that organizations should train all users on a regular basis and that organizations provide initial security awareness training to employees transferring to new positions, as well as to new hires, before the role becomes active. Additionally, the Academic Division's Data Protection Standards require that faculty, staff, and other affiliates granted access to the Academic Division's data must complete information and security awareness training annually. Ineffective security awareness training increases the risk of security incidents related to untrained users falling victim to common cyber-attacks, such as phishing or social engineering.

The Academic Division plans to continue to incorporate annual security awareness training into its recently implemented learning management system (LMS). ITS should develop a strategy to comply with the Academic Division Security Standard and Data Protection Standards, and provide a sufficient level of security awareness training to all sectors of its faculty and staff who have access to Academic Division networks. The fiscal year 2020 audit will include an evaluation of the Academic Division's completed corrective action and determine whether it satisfactorily resolved the weakness.

Improve Patient Accounting, Billing, and Management System Segregation of Duties

Applicable to: Medical Center
Responsible Department: Patient Financial Services
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in 2018, with satisfactory progress made in this area)

The University of Virginia Medical Center (Medical Center) continues to address the deficiency communicated in our prior year audit report to gain assurance that user access to the patient accounting, billing, and management system complies with the principle of least privilege. During fiscal year 2018, the University of Virginia (University) Audit Department (Audit Department) issued a segregation of duties audit report, which focused on access within the Medical Center's patient accounting, billing, and management system. The primary concerns noted by the Audit Department included insufficient consideration or analysis of potential segregation of duties conflicts when changing user access templates, along with a lack of documented approval when making changes to templates.

The Medical Center Security Standard, section AC-5 Separation of Duties, requires that the organization separate the duties of individuals, document the separation of the duties of individuals, and define information system access authorizations to support separation of duties. The Medical Center has documented an analysis over sensitive security points and roles in the patient accounting, billing, and management system, and has been designing a plan to address concerns over segregation of duties. As of fiscal year end 2019, the Medical Center has not implemented this plan, and; therefore, the Medical Center has limited assurance that the access assigned complies with the principle of least privilege. Improper access to the patient accounting, billing, and management system increases the risk of improper activity within the system, which could subsequently affect the Medical Center's financial statements.

The Medical Center should continue to address the recommendations made by the University Audit Department related to segregation of duties in the patient accounting, billing, and management system. By implementing its plan to limit access in compliance with the principle of least privilege, the Medical Center will be able to better monitor and avoid improper segregation of duties within the system.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Segregation of Duties Controls over the Payroll and Human Resources System

Applicable to: All Divisions
Responsible Department: University Human Resources Office
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University implemented a new payroll and human resources system (System) in fiscal year 2019, and unintentionally assigned employees conflicting roles creating segregation of duties risks. The University hired a consultant with proprietary access analysis tools to perform a segregation of duties analysis over the new System and provide a detailed report identifying potential concerns. The University began to research and address concerns in August 2019 and will continue to address additional concerns during the remainder of fiscal year 2020.

As outlined in the University's policy FIN-021: Internal Control, individuals responsible for administering University funds and resources must grant or delegate financial authority carefully, with consideration for proper segregation of duties. The University's adopted information security standard, ISO 27002, section 9.2.2, states, "the provisioning process for assigning or revoking access rights granted to user IDs should include verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties." Inadequate segregation of duties increases the risk for fraudulent transactions and errors in financial reporting and heightens reliance on compensating detective controls. The improper segregation of duties occurred as a result of the University not identifying business processes and prioritizing potential conflicts prior to System implementation. The University should develop a resource that details conflicting business processes and their respective roles for use in establishing and monitoring future access to the system and resolve remaining segregation of duties conflicts identified in the consultant's report.

Ensure Completion of the Commonwealth's Retirement Benefits System Reconciliation Process

Applicable to: All Divisions
Responsible Department: University Human Resources Office
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

The University Human Resources Office (HR) is not completing a reconciliation of the University's payroll and human resources system to the Commonwealth's retirement benefits system (benefits system). HR did not perform a reconciliation for ten out of 12 months in fiscal year 2019 (83%), and performed its last full reconciliation during August 2018. For 26 employees tested for pay rate changes, 20 (77%) had incorrect pay date changes in the Commonwealth's retirement benefits system, which an effective reconciliation may have detected and corrected.

Commonwealth Accounting Policy and Procedure Manual Topic 50410, Virginia Retirement System and Optional Retirement Plans, states that agencies should submit their snapshot confirmation to the Virginia Retirement System (VRS) that confirms their retirement benefits information is accurate in the benefits system by the 10th of the month following the snapshot month. The VRS Employer Manual states that before confirming the snapshot, the employer must review and reconcile the snapshot to ensure the employer reports the most accurate data. Not performing the required reconciliations prior to confirming the snapshot can lead to incorrect information in the benefits system that determines pension liability calculations for the Commonwealth. Since the VRS actuary uses benefits system data to calculate the Commonwealth's pension and other postemployment benefit liabilities, inaccurate data could result in a misstatement in the Commonwealth's financial statements, and consequently the portion of the collective liability VRS allocates to the University.

The University implemented a new payroll and human resources system in January 2019, which required significant personnel resources to implement. Due to the allocation of these resources to development of the new system, HR deferred performing the required reconciliations. With the completion of the new system implementation, HR should allocate sufficient resources to ensure the proper and timely completion of the reconciliation of the University's human resources information to the benefits system managed by VRS.

Improve Process for Terminating Access to the Commonwealth's Retirement Benefits System
Applicable to: All Divisions
Responsible Department: University Human Resources Office
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

University HR did not terminate employees' access to the benefits system timely upon termination of employment. During fiscal year 2019, six individuals with access to the benefits system separated from the University. For three individuals, HR did not remove system access for more than 30 days after each employee's last day of employment.

The University's policy IRM-003: Data Protection of University Information, classifies personal information that if exposed can lead to identity theft, as highly sensitive data. The University Use of Highly Sensitive Data Standard reads that access, generation, collection, storage, and transmission of highly sensitive data will only be allowed when essential and approved for business processes. Additionally, the University's adopted information security standard, ISO 27002, sections 9.2.1 and 9.2.2, state the University should immediately disable or remove access rights of users who have left the institution. Not removing system access in a timely manner increases the risk of unauthorized access to highly sensitive data by individuals no longer employed by the University.

Currently, on a bi-weekly basis, the HR Benefits department uploads a batch file into the benefits system, which prompts the termination of access. This process could result in an individual retaining access to the benefits system for up to two weeks after their last day of employment. In addition, the HR Benefits department noted that the untimely termination of access for two employees was the result

of a delay in the batch upload. For the third employee, the untimely termination was the result of an error in the batch file. The individual was marked as "inactive" rather than "terminated," which did not prompt system access termination.

The HR Benefits department of the University should develop a process to terminate user access to the benefits system when the employee separates from the University or as soon as the employee no longer needs access to the benefits system to perform assigned job duties. Only 18 employees currently have access to the benefits system, all of whom are centrally located in the HR Benefits or Payroll departments. Therefore, due to the centralized nature of human resources and payroll operations and the small number of users with access, it is reasonable to manually terminate the access as soon as practicable, but not later than the employee's separation date. This improvement in the University's process would greatly increase the security over the highly sensitive data contained in the benefits system.

Develop Policies and Procedures to Ensure Compliance with Conflict of Interest Act Requirements

Applicable to: All Divisions
Responsible Department: Department of Policy, Risk Management, and Compliance
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University's Department of Policy, Risk Management, and Compliance (Policy, Risk Management, and Compliance) does not properly ensure that all individuals in positions of trust file Statement of Economic Interest (SOEI) forms as a condition of assuming employment, and does not maintain adequate internal records to monitor and ensure employees have completed the ethics and conflict of interest training within each rolling two-year period as required by the Code of Virginia. Policy, Risk Management, and Compliance identifies and instructs filers to file only during the annual filing period, regardless of their hire date. Additionally, 313 of 567 filers (55%) have not completed training in the past two years. Policy, Risk Management, and Compliance reviews compliance with training requirements on an annual basis and relies solely on the training records provided and maintained by the Virginia Conflict of Interest and Ethics Advisory Council (the Council), which may be an incomplete listing of training taken by University filers due to the other acceptable trainings that a filer may complete outside of the Council's training process.

Pursuant to the Code of Virginia § 2.2-3114A and § 2.2-3118.2, persons occupying positions of trust within state government shall file with the Council, as a condition to assuming office or employment, a disclosure statement of their personal interests and such other information as is required on the form, on or before the day such office or position of employment is assumed, and thereafter shall file such a statement annually on or before February 1. The Governor of Virginia's Executive Order Number Eight (2018) indicates positions of trust for institutions of higher education include Presidents, Vice Presidents, Provosts, Deans, and any other person as designated by the institution including those persons with approval authority over contracts or audits. Additionally, Code of Virginia § 2.2-3129 and § 2.2-3130 require employees in a position of trust to complete an ethics and conflict of interest course, initially within two months of hire, and thereafter on a biennial basis. Code of Virginia § 2.2-3129,

requires agencies to maintain the training records for a period of not less than five years to confirm that employees have completed the course as required.

Policy, Risk Management, and Compliance does not have adequate policies and procedures in place to ensure compliance with the Act. By not ensuring that individuals in positions of trust file SOEI forms as a condition of assuming employment, the University could be susceptible to actual or perceived conflicts of interest that would impair or appear to impair the objectivity of certain programmatic or fiscal decisions made by employees in designated positions of trust. While not a cost to the University itself, employees in a position of trust who do not complete the required Statement of Economic Interest form may, as allowed by the Code of Virginia § 2.2-3124, be assessed a civil penalty in an amount equal to $250.

Policy, Risk Management, and Compliance should develop, implement, and maintain written policies and procedures to meet the Code of Virginia requirements for the SOEI. These updated policies should assist in identifying positions of trust and develop processes to ensure that the appropriate individuals submit SOEI forms as a condition of assuming their employment and each January thereafter. In addition, Policy, Risk Management, and Compliance is responsible for developing and maintaining a filer listing with training records for no less than the preceding five years. Using this internal record, Policy, Risk Management, and Compliance should ensure that filers are informed of their initial training requirement and their biennial training thereafter, and should update the record upon the filer's completion of training.

Improve Timesheet Approval Process
Applicable to: Academic Division
Responsible Department: Payroll Department
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

The Academic Division does not have adequate timesheet controls to support the reasonableness of hourly employee pay. Currently, the Payroll department instructs supervisors to approve timesheets for their direct report employees prior to each payroll run. However, if supervisors do not approve timesheets by the deadline, an automated payroll system process completes the approval of all unapproved timesheets. The Payroll department then notifies the supervisors of the mass approval of timesheets for their direct report employees and gives them 30 days to make corrections to time. The Academic Division does not require supervisors to review the time or to provide positive confirmation that the submitted time is accurate.

When supervisors rely on the mass approval process, the risk of employees charging fraudulent or erroneous time increases. Supervisor reliance on the mass approval process is a result of the absence of policies and procedures surrounding supervisor approvals and a lack of accountability on behalf of department supervisors.

The Academic Division should develop and implement a formal policy to emphasize timely timesheet approval prior to each pay run to ensure reasonableness and accuracy of hourly employee payroll. In instances where the approving supervisor cannot approve a timesheet in a timely manner, the Academic Division should designate a backup approver. When neither approver is available to approve timesheets prior to the Payroll department's processing of payroll, the Payroll department should require each supervisor to provide subsequent positive confirmation of the reasonableness of the hours paid. Finally, management should develop a mechanism for monitoring those supervisors consistently relying on the mass approval process and implement a system of follow up to ensure the supervisors understand their responsibility for timely approval of timesheets.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 22, 2019

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
University of Virginia

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of the University of Virginia as of and for the year ended June 30, 2019, and the related notes to the financial statements, which collectively comprise the University of Virginia's basic financial statements and have issued our report thereon dated November 22, 2019. Our report includes a reference to other auditors. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of the University, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. We did identify certain deficiencies in internal control over financial reporting entitled "Improve Security Awareness Training Program," "Improve Patient Accounting, Billing, and Management System Segregation of Duties," "Improve Segregation of Duties Controls over the Payroll and Human Resources System," "Ensure Completion of the Commonwealth's Retirement Benefits System Reconciliation Process," "Improve Process for Terminating Access to the Commonwealth's Retirement Benefits System," "Develop Policies and Procedures to Ensure Compliance with Conflict of Interest Act Requirements," and "Improve Timesheet Approval Process," which are described in the sections titled "Status of Prior Year Findings and Recommendations" and "Internal Control and Compliance Findings and Recommendations" that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the sections titled "Status of Prior Year Findings and Recommendations" and "Internal Control and Compliance Findings and Recommendations" in the findings entitled "Improve Security Awareness Training Program," "Improve Patient Accounting, Billing, and Management System Segregation of Duties," "Improve Segregation of Duties Controls over the Payroll and Human Resources System," "Improve Process for Terminating Access to the Commonwealth's Retirement Benefits System," and "Develop Policies and Procedures to Ensure Compliance with Conflict of Interest Act Requirements."

The University's Response to Findings

We discussed this report with management at an exit conference held on November 8, 2019. The University's response to the findings identified in our audit is described in the accompanying section titled "University Response." The University's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings

The University has not completed adequate corrective action with respect to the previously reported findings "Improve Security Awareness Training Program" and "Improve Patient Accounting, Billing, and Management System Segregation of Duties." Accordingly, we included these findings in the section entitled "Status of Prior Year Findings and Recommendations." The University has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

EMS/vks

UNIVERSITY of VIRGINIA

November 26, 2019

Martha Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2019 audit related to the University of Virginia (UVA) Academic Division (University). Below are management's responses to the findings:

Improve Security Awareness Training (prior year finding)

Management Response: The UVA Academic Division concurs with the APA's finding.

Responsible for Corrective Action: Jason Belford, Chief Information Security Officer

Anticipated Completion Date: June 1, 2020

Corrective Action to be taken by the University Management:
Annual security awareness training, which has been fairly successful[1], is not the only form of training that University of Virginia users receive. At least twice per year, UVA Information Security initiates a phishing simulation exercise for all employees. Any employee who would fall victim to this exercise is given immediate, on-screen training. Face-to-face training is arranged for units with high response rates.
While the University feels information security education and awareness is important, it is only one piece of the security strategy of the University. We deploy a defense-in-depth strategy in which risk is mitigated at different points of the attack chain. For example, the University implements firewalls, an intrusion prevention system, email anti-spam/anti-phishing technologies, a DNS firewall, end-point posture checking (for HSD access), and multi-factor authentication.
University policy currently requires all employes to "successfully complete either the University's or Health System's online security awareness training at least annually." ISO 27002, the industry standard which the University follows, states that employees of the organization "should receive appropriate awareness education." According to ISO, "should" indicates a "recommendation"[2], as opposed to "must", which indicates a requirement. So, as described in the APA's finding, the

[1] As discussed with the APA, the University identified 12,378 employees (as of 10/3/2019). Of this total population, most employees (82%) successfully completed annual security awareness training. Of the 2,318 employees who did not take the training, only 474 users actually logged into the UVa network within the last 60 days. In summary, of the "active" employees, 96% have taken the training. Of employees who have access to highly sensitive data, 100% completed the annual security training.
[2] https://www.iso.org/foreword-supplementary-information.html

University's policy requiring training is more stringent than that of the industry standard which the University follows.
Given this, as well as the mitigating factors described above (other training, defense-in-depth strategies), the University will follow its risk-based approach to information security and will be revising its policies, standards, and guidelines concerning general security awareness training to be more in-line with ISO 27002. The University will change its requirements to "recommend" general security training for all employees and will continue to encourage all employees to successfully complete the general security training. Employees accessing Highly Sensitive Data (HSD) will continue to be required to complete the general security training.

Improve Segregation of Duties Controls over the Payroll and Human Resources System

Management Response: The UVA Academic Division concurs with the APA's finding.

Responsible for Corrective Action: Augie Maurelli, AVP for Financial Operations

Anticipated Completion Date: June 30, 2020

Corrective Action to be taken by the University Management:
As noted, the University has proactively engaged an external consultant for a post-implementation review of segregation of duties associated with our HCM implementation. UVAFinance, ITS, HR, and Internal Audit have begun to evaluate and address the recommendations received in the report and will continue to do so through FY2020. UVAFinance will take the lead in addressing segregation of duties conflicts and creating an ongoing process in accordance with FIN-021 and ISO 27002, for evaluating, granting, and monitoring future access to the system, as well as resolving conflicts.

Ensure Completion of the Commonwealth's Retirement Benefits System Reconciliation Process

Management Response: The UVA Academic Division concurs with the APA's finding.

Responsible for Corrective Action: Mary Carter, Retirement Plan Administration Associate
Erica Wheat, HR Manager Benefits, Leave, and Payroll
David King, Senior HR Specialist for Benefits

Anticipated Completion Date: June 30, 2020

Corrective Action to be taken by the University Management:
The University implemented a new Human Resources and Payroll System during the fiscal year and the integration with the Commonwealth's Retirement Benefits System was one of the most complex integration in its tenant. Accordingly, a significant amount of resources and testing was

required to ensure a clean, production quality dataset prior to reconciliation. The University has hired a full-time dedicated resource to handle reconciliations and work is underway to catch up past due reconciliations.

Improve Process for Terminating Access to the Commonwealth's Retirement Benefits System

Management Response: The UVA Academic Division concurs with the APA's finding.

Responsible for Corrective Action: David King, Senior HR Specialist for Benefits

Anticipated Completion Date: January 1, 2020

Corrective Action to be taken by the University Management:
The University is developing an internal protocol with managers of the respective teams across Human Resources and Payroll to ensure the security administrator is notified in writing of a termination of anyone with current access to the system. Furthermore, the University will check the access list regularly and compare against active termination records to ensure that access is terminated timely.

Develop Policies and Procedures to Ensure Compliance with Conflict of Interest Act Requirements

Management Response: The UVA Academic Division concurs with the APA's finding that we are not requiring new employees to complete training and to file a Statement of Economic Interest (SOEI) as part of employee on-boarding and that a process for continuous monitoring of completion will help ensure compliance with the Conflict of Interest Act requirements.

Responsible for Corrective Action: Tom Kim, Manager of HR Business Operations

Anticipated Completion Date: March 31, 2020

Corrective Action to be taken by the University Management:
The University of Virginia will make the following corrective actions:

- By January 10, 2020 , notify employees to complete SOEI training.
- By January 10, 2020 , notify employees to file their SOEI.
- By March 31, 2020, implement a process that would require SOEI training for SOEI identified positions, and implement a process for continuous monitoring of completion.
- By March 31, 2020, implement a process through which new employees will file the SOEI and complete training as they are hired.

Improve Timesheet Approval Process

Management Response: The UVA Academic Division concurs with the APA's finding.

Responsible for Corrective Action: Paul Grisdale, Payroll Director

Anticipated Completion Date: June 30, 2020

Corrective Action to be taken by the University Management:
The University will will review the timesheet approval process and take the necessary steps to create adequate timesheet controls.

Sincerely,

Melody Bianchetto
Vice President of Finance

cc: J.J. Davis
Augie Maurelli
Virginia Evans
Kelly Stuck

Office of the Chief Financial Officer

UVA Health

November 26, 2019

Martha Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2019 audit related to the University of Virginia (UVA) Medical Center. Below are management's responses to the findings:

Improve Patient Accounting, Billing, and Management System Segregation of Duties (prior year finding)

Management Response: The UVA Medical Center concurs with the APA's finding.

Responsible for Corrective Action: Erin Trost, Information Security Manager

Anticipated Completion Date: June 30, 2020

Corrective Action to be taken by the University Management:
During FY2019, the Medical Center has developed a remediation plan and developed a model of functional roles. The model is broken out by key area and refers to key teams and their respective responsibilities. Developing this model goes beyond the APA's recommendation but is necessary for implementation. Furthermore, key compensating controls have been identified in instances were a function cannot be segregated. The Medical Center continues to assess the riskiest security points and to develop, implement, and monitor processes within the system to further mitigate risk.

Sincerely,

Douglas E. Lischke
Health System Chief Financial Officer

cc: J.J. Davis
Chris A. Ghaemmaghami, MD
Pamela Sutton-Wallace
Kim Holdren
Erin Trost

PO Box 800813 | Charlottesville, VA 22908-0813
P 434.924.5426 | F 434.244.7522 | uvahealth.com

UNIVERSITY OF VIRGINIA

As of June 30, 2019

BOARD OF VISITORS

Frank M. Conner, III
Rector

James B. Murray, Jr.
Vice Rector

Robert M. Blue
Mark T. Bowles
L.D. Britt
Whittington W. Clement
Elizabeth M. Cranwell
Thomas A. DePasquale
Barbara J. Fried
John A. Griffin
Robert D. Hardie
Maurice A. Jones
Babur B. Lateef
Tammy S. Murphy
C. Evans Poston, Jr.
James V. Reyes
Jeffrey C. Walker

Derrick Wang
Student Representative

Margaret F. Riley
Faculty Representative

Susan G. Harris
Secretary to the Board of Visitors

ADMINISTRATIVE OFFICERS

James E. Ryan
President

Jennifer Wagner Davis
Executive Vice President and Chief Operating Officer