UNIVERSITY OF VIRGINIA

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2024

Auditor of Public Accounts
Staci A. Henshaw, 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, 2024, and issued our report thereon, dated December 13, 2024. Our report, included in the University's Financial Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.virginia.edu. Our audit found:

- the financial statements are presented fairly, in all material respects;
- one deficiency related to governance structure and resources surrounding the financial reporting process that we consider to be a material weakness in internal control;
- additional internal control findings requiring management's attention; however, we do not consider them to be material weaknesses;
- instances of noncompliance or other matters required to be reported under Government Auditing Standards; and
- adequate corrective action with respect to prior audit findings and recommendations identified as complete in the Findings Summary included in the Appendix.

Our audit also included testing over the major federal program of the Student Financial Assistance Programs Cluster for the Commonwealth's Single Audit, as described in the U.S. Office of Management and Budget Compliance Supplement, and found one internal control finding requiring management's attention and an instance of noncompliance in relation to this testing.

In the section titled "Internal Control and Compliance Findings and Recommendations," we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

The University is one of several entities cited in a risk alert in the Department of Accounts fiscal year 2024 audit report. The "Financial Reporting" risk alert identifies the increased risk that the Commonwealth may not meet the deadline for the Annual Comprehensive Financial Report, which could jeopardize the Commonwealth's bond rating, because multiple entities have increasingly submitted inaccurate and late financial information to the Department of Accounts over the past several fiscal years. As an entity that is contributing to this increased risk for the Commonwealth, the University's corrective action to correct the issues in the finding "Improve Governance Structure and Resources Surrounding Financial Reporting Process" is essential to reducing the risk to the Commonwealth.

–TABLE OF CONTENTS–

	Pages
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-9
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	10-12
APPENDIX – FINDINGS SUMMARY	13
UNIVERSITY RESPONSE	14-18

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Governance Structure and Resources Surrounding Financial Reporting Process
Applicable: University-wide
Responsible Department: Executive Vice President and Chief Operating Officer, Chief Executive Officer UVA Health, UVA Finance, and Medical Center Controller's Office
Type: Internal Control
Severity: Material Weakness
First Reported: 2021 – Significant Deficiency, 2022 – Material Weakness

The University of Virginia (University) continues to implement corrective actions to improve internal controls and governance over the University's consolidated financial statements which include the Academic Division and University of Virginia Medical Center (Medical Center). The University realigned the Medical Center's and Academic Division's financial reporting functions under the University's Chief Financial Officer to improve coordination, define roles and responsibilities, and establish timelines for financial reporting deliverables. The Medical Center financial management team experienced significant turnover during the fiscal year. Under the new management structure, the University engaged consultants to assist in performing a comprehensive review of Medical Center operations and internal controls. The consultants identified a lack of stable processes and controls which increased the risk of not producing reliable and accurate financial data for reporting. The consultants assisted the Medical Center in developing and providing sufficient appropriate evidence to support the control environment and the financial data used in the University's financial statements.

Although the University continues to allocate additional resources and implement new processes and controls over financial reporting, these processes and controls require time to mature. In assessing the maturity of the changes made to the University's financial reporting process, we identified the following significant issues in our review of the financial statements and related control environment.

Financial Reporting

The University did not adequately coordinate and communicate a strategy for consolidation and implementing several accounting pronouncements including, Governmental Accounting Standards Board (GASB) Implementation Guide 2021-1, Q5.1 and GASB Statement No. 94. Specifically, the University did not develop a cross-divisional process to identify and capitalize purchases of groups of assets or identify public-public partnerships, public-private partnerships, or availability payment arrangements. Based on our review, the lack of a unified approach resulted in a $7.3 million adjustment to capitalize groups of assets previously excluded from the financial statements, including a $3.4 million restatement to beginning net position. Additionally, the Medical Center incorrectly entered three subscription-based information technology arrangements (GASB Statement No. 96), resulting in a $10.1 million adjustment impacting capital assets, prepaid expenses, and long-term liabilities. Also, during the financial statement consolidation process, the University did not adequately review intercompany transactions relating to the University's health plan. The oversight resulted in a $9.1 million overstatement of payables and the elimination of intercompany transactions. The lack of a unified

approach to consolidation and implementation of new or existing accounting standards increases the risk of materially misstated financial statements.

Journal Entries

Journal entries are foundational to the integrity and transparency of financial reporting and are used for monthly accruals, contractual adjustments, intercompany activity, patient service revenue, and other financial transactions. The Medical Center posted seven out of 36 (19%) journal entries sampled with a lack of supporting documentation and 12 out of 36 (33%) journal entries sampled with no evidence of the employees who entered and approved the entry. In October 2023, former Medical Center management posted a journal entry of $55 million (statement of net position impact) without a detailed review and formal approval. This entry, related to a significant accounting transaction in 2024, was subsequently reviewed and corrected as part of year-end review procedures conducted by the new Medical Center management team during last quarter of fiscal year 2024. These findings highlight management override of controls as a significant risk to the overall financial reporting and internal control environment. Such risks could result in errors, fraud, and materially misstated financial statements.

Although improved controls were implemented in May 2024, to ensure segregation of duties and formal review of journal entries, issues remain. For instance, an audit adjustment of $7.6 million was required for other postemployment benefit liability accounts and related expense due to human error in a journal entry. This error was not detected by the journal entry control in place. To strengthen the financial reporting process, management must continue evaluating and enhancing controls to address these gaps effectively.

The University implemented new lease tracking procedures moving from its accounting system to manually tracking leases. However, the University did not make the correct journal entries to account for the system transition resulting in a $6.5 million reclassification between operating and nonoperating expenses. Management oversight is a key control when making significant changes to procedures and highlights the importance of accurate recordkeeping for financial reporting.

Accounts Payable

During our review of unrecorded liabilities, for seven out of 80 (7.5%) Medical Center expense vouchers sampled and three out of 30 (10%) Academic Division expense vouchers sampled, the University did not accrue expenses payable in the correct fiscal year. Both divisions used incomplete query logic, and the Medical Center used a minimum analysis threshold, which left approximately $55 million in payables unanalyzed. Management performed a subsequent evaluation resulting in a $9.1 million adjustment to accounts payable and expenses.

Cash Management

The Medical Center did not perform a monthly reconciliation for nine out of 12 (75%) months to identify and timely remediate reconciling items between bank statements and its accounting system. The year-end bank reconciliation was not completed until four months after fiscal year end which led to:

- The discovery of a $34.8 million overpayment to a discretely presently component unit and $58.8 million of unrecorded cash collected by the Medical Center on behalf of a discretely presented component unit;

- The discovery of $62.4 million in unrecorded wire transfers to a discretely presented component unit dating back to August 2023; and

- Unresolved reconciling differences of approximately $1.5 million.

Reconciliations ensure the accuracy and completeness of financial statements by identifying and resolving discrepancies between bank accounts and the accounting system. By not completing reconciliations and addressing reconciling items timely, the Medical Center increases the risk of recording inaccurate information in the University's financial statements and mismanaging cash resources.

University management is responsible for designing and maintaining a system of internal controls relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement in accordance with generally accepted accounting principles. The lack of adequate internal control processes over financial reporting, journal entries, account payable, and cash management and corresponding financial statement misstatements increase the risk that users of financial statements may draw improper conclusions about the University's financial activities. As the combination of deficiencies and adjustments depict, the University's existing internal control processes present a reasonable possibility that a material misstatement will not be prevented or detected and corrected on a timely basis.

These deficiencies are attributable to certain inadequately designed controls and insufficiently documented policies and procedures compounded by significant turnover within the Medical Center's financial management team, which required new personnel to seek external consulting resources to evaluate areas for improvement and assist in the preparation of accurate financial information for consolidation into the University's financial statements. The University should continue to develop effective controls over financial data and processes to produce accurate and complete financial statements. The University should develop policies and procedures over key business process areas including financial reporting, journal entries, accounts payable, and cash management. The policies and procedures should include but are not limited to error correction, bank reconciliation, intercompany account reconciliation, accounts payable cut-off, and appropriate segregation of duties and approval processes.

Improve Firewall Security
Applicable: Academic Division
Responsible Department: Information Technology Services
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Academic Division does not secure a firewall that safeguards a portion of its secure internal network in accordance with the Academic Division's adopted Information Security Standard, the International Organization for Standardization and the International Electrotechnical Commission Standard ISO/IEC 27002 (ISO Standard), as well as Academic Division policy.

We communicated four weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The ISO Standard requires organizations to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the Academic Division information systems and data.

Management oversight resulted in the four identified weaknesses. The Academic Division should improve its processes to administer the firewall and remediate the identified weaknesses to align with the Academic Division's policy and ISO Standard. These improvements will help to safeguard the confidentiality, integrity, and availability of the Academic Division's sensitive networks and mission-critical data.

Improve IT Service Provider Oversight
Applicable: Medical Center
Responsible Department: Health System Technology Services
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Medical Center does not appropriately monitor the effectiveness of the security controls of information technology (IT) service providers (providers) in accordance with the Medical Center's adopted Information Security Standard, the National Institute of Standards and Technology Standard, 800-53 (NIST Standard), as well as the Medical Center's Risk Management Standard (Risk Standard). Specifically, the following four weaknesses exist:

- The Medical Center does not have a policy that requires the Medical Center to maintain an updated list of providers and does not have a procedure to facilitate maintaining an updated list of providers, including roles and responsibilities for Medical Center staff tasked with oversight. Due to the lack of a requirement and process for maintaining a comprehensive and up-to-date list of providers, we were unable to determine an accurate total number of providers the Medical Center uses for IT services. The NIST Standard states that the Medical Center should develop, document, and disseminate a policy that addresses purpose, scope, roles, responsibilities, management commitment, and compliance and is consistent with applicable laws, regulations, policies, standards, and guidelines. Without a policy that

requires the Medical Center to maintain an updated list of providers and a procedure in place to facilitate the policy requirement, the Medical Center cannot ensure that it has an accurate list of providers to review, which could lead to providers with risks that are not reviewed and accepted or mitigated in accordance with the Risk Standard.

- The Medical Center does not obtain and review an independent audit assurance report (such as a System and Organization Controls (SOC) 2 Type II or equivalent report) to validate the operating effectiveness of security controls every three years for each provider with a risk rating of "Moderate" or "High" that contain highly sensitive information, as required by the Risk Standard. The Medical Center has a process in place to obtain and review independent audit assurance reports for existing providers with a risk rating of "Moderate" or "High" during its three-year risk assessment re-review process. The Medical Center provided a list of 12 providers that have a risk rating of "Moderate" or "High" due for a three-year assessment. During calendar year 2024, the Medical Center obtained an independent audit assurance report for ten of the 12 providers and documented its review of the report in each provider's corresponding risk assessment. However, the Medical Center has not obtained and reviewed an independent audit assurance report for the remaining two providers on the list. Additionally, we were unable to determine whether these 12 providers are the only providers that require assessment. The Risk Standard requires that the Medical Center conduct re-reviews for any "Moderate" or "High" risk third-party systems every three years and document the results in a risk assessment report. The NIST Standard requires that the Medical Center employ processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis. Without reviewing independent audit assurance that validates the operating effectiveness of security controls on a regular, ongoing basis, the Medical Center cannot identify possible control deficiencies and follow up with the provider timely, which could result in unauthorized use or disclosure of the Medical Center's sensitive information.

- The Medical Center does not include a requirement in agreements with its providers to provide an independent audit assurance report to the Medical Center every three years to align with the Risk Standard. This Risk Standard states that all provider platforms supported by a vendor that contain sensitive information have an additional requirement of a SOC 2 Type II or equivalent independent audit assurance, and review of their security controls. The NIST Standard requires that the Medical Center employ processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis. Not requiring providers to provide independent audit assurance, such as a SOC 2 Type II or equivalent, on a regular basis could result in an inability for the Medical Center to gain an adequate understanding of the provider's control environment.

- The Medical Center does not identify, evaluate, and determine which subservice providers are significant to the Medical Center's operations. The Medical Center also does not obtain assurance over the relevant controls for significant subservice providers. Subservice providers are supporting providers that deliver or assist in the delivery of a service relied upon to support a provider's environment. The NIST Standard requires that the Medical Center

employ processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis. Not obtaining and reviewing independent audit assurance reports for subservice providers precludes the Medical Center from gaining assurance over the controls excluded from the provider's assurance report due to the subservice provider implementing those controls, which could open the Medical Center to a risk of unauthorized modification or disclosure of sensitive Medical Center data and information.

The Medical Center is currently in the process of completing a project to centralize parts of its contract and risk assessment process and plans to implement a centralized solution for third-party vendor management to manage its contract and risk assessment processes. The Medical Center prioritized completion of this project, which delayed its provider oversight activities. Additionally, the Risk Standard details the Medical Center's process for assessing the risk of systems but does not detail the necessary requirements and processes that the Medical Center should follow for ongoing oversight of its providers, which contributed to the process lacking additional elements.

The Medical Center should develop a policy that requires maintaining an updated list of providers, and receiving and reviewing independent audit assurance reports, such as a SOC 2 Type II or equivalent reports, from all providers on a regular basis. The Medical Center should then develop a procedure to facilitate the implementation of the policy. The Medical Center should also develop a policy or update the Risk Standard to define the requirements and process the Medical Center follows for appropriate provider oversight, including receiving and reviewing independent audit assurance. The Medical Center should then adhere to the Risk Standard and obtain and review independent audit assurance that validates the operating effectiveness of the security controls for all IT providers as part of the required risk assessment re-review process. Additionally, the Medical Center should ensure it has a contract requirement in place requiring providers to supply the Medical Center with independent audit assurance, such as a SOC 2 Type II or equivalent. Finally, the Medical Center should evaluate and determine which subservice providers are significant to the Medical Center's operations. For all significant subservice providers, the Medical Center should determine the best way to obtain assurance over the relevant controls at the subservice provider and document the results of the procedures performed. This assurance could include obtaining and reviewing independent audit assurance reports for the subservice providers. These control enhancements will help to safeguard the confidentiality, integrity, and availability of the Medical Center's sensitive and mission-critical data.

Improve Oversight of Administrative Service Providers
Applicable: Medical Center
Responsible Department: Controller's Office
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Medical Center does not have sufficient internal controls over SOC reports of administrative service providers. The Medical Center outsources certain business tasks and functions to service providers who transmit, process, or store sensitive Medical Center data. SOC reports, specifically SOC 1 Type II reports, provide an independent description and evaluation of the operating effectiveness of a

service providers' internal controls over financial processes and are a key tool in gaining an understanding of a service provider's internal control environment and maintaining oversight of outsourced operations. However, the Medical Center does not have a formal process to identify service providers. Consequently, during fiscal year 2024, the Medical Center did not obtain, review, or document its review of service provider SOC reports to identify deficiencies or determine whether the reports provided adequate coverage over operations.

The Commonwealth Accounting Policies and Procedures Manual (CAPP Manual) Topic 10305 requires agencies to have adequate interaction with service providers to appropriately understand the service provider's internal control environment. Universities must also maintain oversight of service providers to gain assurance over outsourced operations in accordance with Agency Risk Management and Internal Control Standards (ARMICS). In addition, the NIST Standard requires that organizations define and employ processes to monitor security control compliance by external service providers on an ongoing basis.

Without adequate policies and procedures over service providers' operations, the Medical Center is unable to properly identify service providers and ensure the Medical Center's complementary user entity controls are sufficient to support its reliance on the service providers' control design, implementation, and operating effectiveness. Additionally, Medical Center is unable to address any internal control deficiencies and/or exceptions identified in the SOC reports. The Medical Center is increasing the risk that it will not detect a weakness in a service provider's environment by not obtaining the necessary SOC reports timely or properly documenting its review of the reports, and any corrective actions necessary to mitigate the risk to the Medical Center until the service provider corrects the deficiency. The Medical Center should develop and implement a process to identify service providers and obtain, review, and document SOC 1 Type II reports for its service providers that significantly affect its financial activity.

Improve Reporting to National Student Loan Data System

Applicable: Academic Division
Responsible Department: Student Financial Services
Type: Internal Control and Compliance
Severity: Significant Deficiency

University Student Financial Services personnel did not report accurate and/or timely enrollment data to the National Student Loan Data System (NSLDS) for students that withdrew or had an enrollment level change other than graduated or withdrawn. The underlying causes were due to data entry errors and batch processing issues. Specifically, a student's social security number was inaccurately recorded in the Student Information System. Additionally, batch enrollment updates caused new data submissions to overwrite previous data, which resulted in inaccurate enrollment records. While reviewing student records for 40 students, we noted:

- For four students (10%), the effective date in NSLDS did not agree to the Student Information System;

- For five students (13%), Student Financial Services personnel did not report the student enrollment change within the required time frame; and

- For four students (10%), NSLDS included inaccurate campus and/or program level information for at least one critical field.

In accordance with Title 34 U.S. Code of Federal Regulations (CFR) § 685.309 and further outlined in the NSLDS Enrollment Guide published by the Department of Education, enrollment changes must be reported to NSLDS within 30 days when attendance changes, unless a roster file will be submitted within 60 days. The accuracy of Title IV enrollment data depends heavily on information reported by institutions. Untimely and inaccurate data submitted to NSLDS can affect the reliance placed on the system by the Department of Education for monitoring purposes. Noncompliance may also have implications for an institution's participation in Title IV programs and can potentially impact students' loan repayment grace periods and/or loan subsidies. University management should implement additional controls, such as a quality control process to review student status change batches, to ensure the accuracy and timeliness of enrolment data reported to NSLDS.

Strengthen Interdepartmental Communications Related to Terminated Employees
Applicable: Medical Center
Responsible Department: Health System Technology Services and Human Resources
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Medical Center does not have adequate internal controls over the removal of access for terminated employees. We identified the following instances where the Medical Center did not remove an employee's system access within six business days of termination for the following systems:

- Twenty-two out of 173 (13%) terminated users retained access to the Medical Center's medical record system for seven to 65 business days;

- Fourteen out of 125 (11%) terminated users retained access to the Medical Center's timekeeping system for seven to 42 business days; and

- Two out of 58 (3%) terminated users retained access to the Medical Center's financial and accounting system for eight to 14 business days.

The Medical Center's Electronic Information and Systems Use Policy states within forty-eight (48) hours of a manager's/supervisors' receipt of notification of a user's change of job duties, termination of employment, or termination of trainee status, the manager/supervisor shall notify the appropriate Human Resources office and the Human Resources office shall, within three (3) business days of such notification, alert the Health IT Information Security Office (Security Office) to ensure the user's access is consistent with user's change in status. If immediate termination of access is required, the manager/supervisor shall immediately (i.e., within 24 hours) notify the Security Office. The Medical Center's Access Termination Standard states UVA Human Resources will provide a daily report of all UVA

Health daily terminations to the Security Office and the Security Office will disable all network, email, and access to information systems within 24 hours. Not removing system access timely increases the risk of unauthorized transactions and access to highly sensitive data by individuals no longer employed by the Medical Center.

Supervisors and/or Human Resources did not communicate terminations timely to the Security Office resulting in untimely removal of system access. The Medical Center should strengthen communication between supervisors, Human Resources, and the Security Office to ensure timely removal of system access. The Medical Center should ensure all departments are aware of the policy and develop mechanisms to ensure departmental supervisors follow established policies and procedures.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 13, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
University of Virginia

James E. Ryan
President, 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** (University) as of and for the year ended June 30, 2024, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated December 13, 2024. Our report includes a reference to other auditors who audited the financial statements of the component units of the University, as described in our report on the University's financial statements. The other auditors did not audit the financial statements of the component units of the University in accordance with Government Auditing Standards, and accordingly, this report does not include reporting on internal control over financial reporting or compliance and other matters associated with the component units of the University.

Report on 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 (internal control) as a basis for designing 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. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as described in the section titled “Internal Control and Compliance Findings and Recommendations,” we identified certain deficiencies in internal control that we consider to be a material weakness and significant deficiencies.

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. We consider the deficiencies titled “Improve Governance Structure and Resources Surrounding Financial Reporting Process,” which is in the section titled “Internal Control and Compliance Findings and Recommendations,” to be a material weakness.

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. We consider the deficiencies titled "Improve Firewall Security," "Improve IT Service Provider Oversight," "Improve Oversight of Administrative Service Providers," "Improve Reporting to National Student Loan Data System," and "Strengthen Interdepartmental Communications Related to Terminated Employees," which are described in the section titled “Internal Control and Compliance Findings and Recommendations,” 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 financial statements. 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 section titled “Internal Control and Compliance Findings and Recommendations,” in the findings and recommendations titled "Improve Firewall Security," "Improve IT Service Provider Oversight," "Improve Oversight of Administrative Service Providers," "Improve Reporting to National Student Loan Data System," and "Strengthen Interdepartmental Communications Related to Terminated Employees."

The University’s Response to Findings

We discussed this report with management at an exit conference held on January 14, 2025. Government Auditing Standards require the auditor to perform limited procedures on the University’s response to the findings identified in our audit, which is included in the accompanying section titled “University Response.” The University’s response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

The University has not completed corrective action with respect to the prior reported finding identified as ongoing in the Findings Summary included in the Appendix. The University has taken adequate corrective action with respect to prior audit findings identified as complete in the Findings Summary included in the Appendix.

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 Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

DLR/vks

FINDINGS SUMMARY

Finding Title	Applicable Division	Status of Corrective Action*	First Reported for Fiscal Year
Improve Processes over Employment Eligibility Verification	University-wide	Complete	2020
Complete Annual Review over User Access to University Information Systems	Academic	Complete	2021
Complete Annual User Access Reviews	Medical Center	Complete	2022
Complete a System Security Plan for Each Sensitive System	Medical Center	Complete	2022
Improve Accounts Payable Controls	Medical Center	Complete	2023
Improve Database Security	Academic	Complete	2023
Improve Timekeeping Controls	Medical Center	Complete	2023
Perform Complete Physical Inventory	Academic	Complete	2023
Improve Governance Structure and Resources Surrounding Financial Reporting Process	University-wide	Ongoing	2021
Improve Firewall Security	Academic	Ongoing	2024
Improve IT Service Provider Oversight	Medical Center	Ongoing	2024
Improve Oversight of Administrative Service Providers	Medical Center	Ongoing	2024
Improve Reporting to the National Student Loan Data System	Academic	Ongoing	2024
Strengthen Interdepartmental Communications Related to Terminated Employees	Medical Center	Ongoing	2024

* A status of **Complete** indicates management has taken adequate corrective action. A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

UNIVERSITY of VIRGINIA | UVAFinance

December 18, 2024

Ms. Staci Henshaw
Commonwealth of Virginia Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw,

We have reviewed the audit findings and recommendations resulting from the fiscal year 2024 audit related to the University of Virginia (UVA) Academic Division (University) and Medical Center. Below are management's responses to those findings.

Improve Governance Structure and Resources Surrounding Financial Reporting Process
Management Response: The University concurs with the APA's finding.
Responsible for Corrective Action: Financial Reporting
Executive Vice President and Chief Operating Officer, and Chief Executive Officer, UVA Health
Anticipated Completion Date: June 30, 2025

The University of Virginia greatly appreciates the opportunity to address the management point and will continue to work on its remediation. UVA also appreciates the acknowledgement of all the efforts put forth to date regarding resources, bolstered governance, and overall communication and coordination between Academic and Medical Center's finance teams.

In FY 2024, the University implemented a number of changes important to strengthening the internal control environment. These changes include:

- Aligned Academic and University accounting teams, implemented a unified remediation effort and improved communications at all levels including monthly engagement with the APA.UVA will maintain its current audit governance, organizational structures, and single audit coordinator, as well as continuing to increase resources and skill sets.
- Revamped Financial Statements, consolidating them into a unified audited statement with a segmented format for the Medical Center and the Academic Division with single opinion.
- Changed Medical Center financial leadership and added additional resources including third party expertise.

The University and Medical Center have initiated planning to update and integrate its ERP financial module which will further enhance internal controls and efficiencies.

Regarding the specific issues identified by the APA's review of the financial statements,

UVAFinance is the valued and trusted financial partner that the University community turns to first.
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | F 434.982.2315 | vpfinance@virginia.edu

management's response is as follows:

The University agrees with the need for a unified approach to the preparation of its consolidated financial statements; however, also believes that the consolidation process was effectively communicated and agreed to by both divisions early in the year. This is evidenced by the successful redesign of the financial statements, meeting required deadlines, and eliminating the need for a separate set of audited statements for the Medical Center.

The University also agrees with the need to review new GASB accounting pronouncements and ensure accuracy and consistency between Academic and Medical Center divisions. To provide additional context and evidence the work done, GASB 2021-1 was reviewed with the Medical Center team in April 2024, and it was determined that they had begun capitalizing under that guidance in prior years. Based on the thresholds and process being subject to audit in prior years, additional review was not deemed necessary at the time. Ultimately the total adjustments of $4 million, which are less than one one-hundredth of a percent of total capital assets, found were from inconsistent application of the procedures not the procedures themselves that are coordinated across teams in the current reporting structure. Finally, it is important to highlight where there was successful coordination between the teams during FY24 for accounting pronouncements and high impact transactions. The Academic and Medical Center divisions worked together to align capitalization thresholds on equipment at the Medical Center, and completed the technical paper, which was presented jointly to APA, on the proper accounting for the Riverside Health equity interest.

The University conducts monthly reconciliations of all Health Plan activity. The FY24 adjustment was caused by two manual journal entry accruals from prior periods that were not accurately reflected in the manual process used to allocate the Health Plan balance between the University and the Medical Center. To prevent similar issues in the future, the Academic and Medical Center teams will enhance the review process in FY25, ensuring greater accuracy and alignment.

Strong controls over manual journal entries are essential for an effective financial reporting process. The Medical Center has taken steps to implement proper segregation of duties, documentation, and approval processes for both manual entries and intercompany transactions. Additionally, as a mitigating control the Medical Center conducted both manual and analytical reviews of FY24 journal entries.

The Academic Division plans to implement a new lease software to track leases and eliminate manual entries by June 30, 2025. While the balance sheet accounts and total expenses were accurately recorded in the journal entry, classification of expenses was incorrect. The University will include an additional review step to ensure proper expense classification when the new lease accounting system is implemented.

UVAFinance is the valued and trusted financial partner that the University community turns to first.
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | **F** 434.982.2315 | vpfinance@virginia.edu

The University will continue implementation of effective controls over financial reporting of Accounts Payable and will revise its directive and extend its allotted time to identify and evaluate unrecorded liabilities from 31 days after the fiscal year end close to 60+ days.

The University is focused on providing consistent accounting and reconciliation process for Medical Center cash and cash equivalents. The Medical Center team will continue with monthly bank reconciliations to ensure timely and accurate view of cash position at UVA Health. All adjustments noted by the APA above were discovered and corrected by Medical Center management, which indicates that the new reconciliation procedures in place are operating effectively. A Treasury optimization project has begun in November 2024 that will provide for a simplified and transparent mapping of General Ledger Accounts for cash transactions. Medical Center is committed to providing an improved transaction monitoring, segregation of duties, and audit trail clarity for cash and cash equivalents.

The University is committed to continuing to implement robust external reporting processes to ensure accuracy, transparency and compliance in financial disclosures. Through unified financial reporting team, clear ownership of reporting tasks, rigorous review and reconciliations, refinement of reporting frameworks for Academic and Medical center teams, and leveraging technology to automate consolidation process, the University will continue to create a resilient and transparent external reporting process. Finally, the team will ensure enhanced engagement and coordination for all component units and consolidating entities as well.

Improve Firewall Security
Management Response: UVA concurs with the APA's finding.
Responsible for Corrective Action: Information Technology Services
Anticipated Completion Date: June 30, 2025

The University has begun corrective action since the conclusion of the 2024 audit and those steps have been communicated in a separate memo marked Freedom of Information Exempt, due to the sensitivity of the information.

Improve Service Provider Oversight
Management Response: The Medical Center concurs with the APA's finding.
Responsible for Corrective Action: Health System Technology Services
Anticipated Completion Date: June 30, 2025

UVA Health will create a policy-level statement as part of our third-party service provider project that will define the process for maintaining and updating a list of providers.

UVA Medical Center did complete re-evaluations of all its third-party service providers that had

received a "moderate" or "high" risk in FY21 and FY22. In two cases mentioned, the Medical Center received HIPAA third-party assessment report and a SOC 2 Type I as assurance reports. In both those cases the risk level stayed as a moderate risk. While UVA Medical Center had assurance that security controls were reviewed by a third-party we did not obtain a SOC 2 Type II report as those organizations did not have a SOC 2 Type II report to provide at the time of request. UVA Health will update the Risk Management standard to require SOC 2 Type II report review for all UVA Health third-party IT and finance service providers and add HITRUST and ISO as formally accepted report types for IT providers. In addition, UVA Health will create an exception process when a vendor is unable to provide one of assurance reports required per the standard.

UVA Health will update the risk assessment questionnaire to include a question about the use of sub-service providers such as AWS, Google, etc., and will request copies of those sub-service provider SOC 2 Type II or HITRUST or ISO reports on a triennial basis will perform the same level of review as the third-party service provider.

In addition, the UVA Health will work with Contracting & Procurement to strengthen the contract language to include a clause that requires the vendors to provide a copy of their SOC 2 Type II report, or alternatively HITRUST or ISO report for IT providers, upon request and / or at the time of the triennial re-assessment.

Improve Oversight of Third-Party Service Providers
Management Response: The Medical Center concurs with the APA's finding.
Responsible for Corrective Action: Medical Center Controller's Office
Anticipated Completion Date: June 30, 2025

UVA Health will update the Risk Management standard and align with the HIT third-party service provider assessment process to require SOC 2 Type II report review for all UVA Health third-party IT and finance service providers and will add HITRUST and ISO as formally accepted report types for IT providers. In addition, UVA Health will create an exception process when a vendor is unable to provide one of assurance reports required per the standard.

Improve Reporting to National Student Loan Data System
Management Response: The UVA academic division concurs with the APA's finding.
Responsible for Corrective Action: Associate Vice Provost for Enrollment and University Registrar
Anticipated Completion Date: June 30, 2025

The University will implement additional controls to ensure the accuracy and timeliness of enrollment data reported to NSLDS. This includes working collaboratively with Student Financial Services and Information Technology Services to monitor and report late withdrawals, review and update the SIS process for creating enrollment files, and implement a quality control review to

UVAFinance is the valued and trusted financial partner that the University community turns to first.
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | F 434.982.2315 | vpfinance@virginia.edu

check student status change batches for accuracy and timeliness.

Strengthen Interdepartmental Communications Related to Terminated Employees
Management Response: The Medical Center concurs with the APA's finding.
Responsible for Corrective Action: Health System Technology Services, Human Resources
Anticipated Completion Date: June 30, 2025

Delayed notification to HR and HIT Security has occurred in instances where managers did not enter termination dates into Workday in a timely manner, as per MC HR Policy 'Separation From Employment'. Medical Center leadership, in partnership with HR and IT, has already come together and is committed to addressing this issue. The Medical Center will re-educate managers and emphasize the critical need for timely communication regarding terminations and the consequences of non-compliance. Additionally, we will implement monitoring and reporting mechanisms to reduce instances in which the time between employee termination and removal of system access exceeds six business days. Workday administrators will explore ways to automatically notify managers and managers' managers of non-compliance with the requirement for timely termination entries.

Sincerely,

Augie Maurelli
Vice President for Finance, Chief Financial Officer

Erik Shannon
Interim Chief Financial Officer, UVA Medical Center, CEO Community Health

cc: Jennifer "J.J." Davis
Olga Weider
Kelly Doney
Michael Grinnell
Brad Sanford
Laura Hawthorne
John Kosky
Sami Kaur
Wendy Horton
Erin Trost
Robin Parkin
Mike Marquardt

UVAFinance is the valued and trusted financial partner that the University community turns to first.
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | **F** 434.982.2315 | vpfinance@virginia.edu