**The University of Texas Health Science Center at Houston (UTHealth)
Internal Audit Annual Report for 2018**

Purpose of the Annual Report: To provide information on the benefits and effectiveness of the internal audit function. In addition, the annual report assists central oversight agencies in their planning and coordination efforts.

Table of Contents

Purpose of the Annual Internal Audit Report: To provide information on the assurance services, consulting services, and other activities of the internal audit function. In addition, the annual internal audit report assists oversight agencies in their planning and coordination efforts.

I.   **Compliance with Texas Government Code, Section 2102.015: Posting the Internal Audit Plan, Internal Audit Report, and Other Audit Information on Internet Web site**

The Internal Audit plan and Internal Annual Report is contained within the Reports to the State section of UTHealth's web site as required by Texas Government Code, Section 2102.015. An updated report is provided to the web developer in the Office of Institutional Advancement via email. The web developer then posts the information no later than one day prior to the due date for submission to the appropriate reporting state agencies.

II.   **Internal Audit Plan for Fiscal Year 2018**

Audit Number	FY 2018 Audit Plan Audit/Project	Description	Status	Report Date
	Financial Audits	*Description*	Complete	
18-101	Financial Statements FY 2017 Assurance Work	Control and transaction testing, analytical review, and other procedures assigned as part of the financial statements assurance audit	Complete	Report issued by D&T at UT System level
18-102	Financial Statements FY 2018 Assurance Work	Interim work for FY2017 financial statement audit	Complete	Report issued by D&T at UT System level
18-103	Assist State Auditor's Office and other state and/or federal auditors	Provide assistance to the State Auditor's Office and other external audit functions	Complete	No Report Issued
18-115	Review and Validation	Review for compliance with UTS 142.1, Section 6 requiring audits of the monitoring plan to validate the assertions on segregation of duties and account reconciliations	Complete	10/26/2017
	Operational Audits			
18-108	Executive Travel and Entertainment	Review of official function, and travel and entertainment expenses	Complete	11/7/2017
18-114	Purchasing	Review of controls over purchasing processes including purchase coding and use of blanket POs	In Progress	
18-116	Benefits Proportionality	Determine whether proportional benefits by funds are accurately calculated and applied as set forth	Complete	05/30/2018

		in Article IX Section 6.08 of the General Appropriation Act for FY 2015,2016 & 2017		
	Carryforward Audits			
17-117	Core Labs	Operational review of efficiency and effectiveness	Complete	Report Submitted
17-118	SoD General Practice	Review operations at the University Dental Center	Complete	Report Submitted
17-104D	Recommendation Follow up	Follow up on open recommendations	Complete	Report Submitted
	Compliance Audits			
18-106	Joint Admission Medical Program (JAMP)	Provide opinion on the appropriateness of the expenditures for the Program for FY 2017	Complete	10/31/2017
18-107	Texas Higher Education Coordinating Board Residency Program	Provide opinion on revenue and expenditure reporting on annual financial report	Complete	12/18/2017
18-109	Americans with Disabilities	Review of disability and accommodation process to determine compliance with federal guidelines	Complete	07/31/2018
18-110	Medical School Practice Plan (MSRDP)	Assess compliance with MSRDP process or bylaws. Will be performed based on risk	Cancelled	
18-111	Dental School Practice Plan (DSRDP)	DSRDP audit to assess efficiency and effectiveness of operations of biopsy services	In Progress	
18-112	Subrecipient Monitoring	Review of subrecipient monitoring efforts to determine compliance with federal guidelines	Complete	08/16/2018
18-113	MACRA	Review to determine compliance with Medicare Access and CHIP Reauthorization Act	In Progress	
	Carryforward Audits			
17-110	Medical School Practice Plan (MSRDP)	Assess compliance with MSRDP process or bylaws. Will be performed based on risk	Complete	Report Submitted
17-111	Dental School Practice Plan (DSRDP)	DSRDP audit to assess efficiency and effectiveness of operations of biopsy services	Complete	Report Submitted
	Information Technology Audits			
18-201	Security Policy Workflow Agreements	Determine whether controls over security policy workflow agreements are adequate and functioning as intended	Complete	04/05/2018

18-203	Telemedicine	Determine whether controls around telemedicine are adequate and functioning as intended	In Progress	
18-204	Office 365	Determine whether controls around subscription-based application that includes access to Office applications plus other productivity services enabled for the internet (cloud services) are adequate and functioning as intended	Cancelled	
18-205	Google Apps for Education	Determine whether the controls around Google Apps for Education are appropriate and functioning as intended	In Progress	
18-206	System Access Reviews	Determine whether controls around system access reviews are appropriate and functioning as intended	Complete	07/10/2018
18-207	Timeshares	Determine whether controls around patient privacy and the Time Share equipment are adequate and functioning as intended	Cancelled	
18-208	SunNet (CLI Contract)	Determine whether payments and work performed are in compliance with the SunNet Contract terms	In Progress	
18-209	Practice Partner (SON)	Determine whether controls around patient privacy and the Practice Partner application are adequate and functioning as intended	Cancelled	
18-210	Citrix	Determine whether controls around the Citrix application are adequate and functioning as intended	In Progress	
	Carryforward IT Audits			
17-203	New Innovations	Determine whether controls over New Innovations/resident management are adequate and functioning as intended	Complete	10/09/2017
17-204	Hemophilia - Integrated	Review of the billing and collections process as well as system controls for user access, charge capture, billing, collections and accounts receivables	Cancelled	
17-206	Sunrise Clinical Manager	Determine whether controls over the Sunrise Clinical Manager application are adequate and functioning as intended.	Complete	12/12/2017
17-207	Digital Loss prevention (Digital Guardian)	Determine whether controls around data loss prevention and the Digital Guardian application are adequate and functioning as intended	Complete	12/20/2017

17-208	Clinical Data Usage	Determine whether controls around clinical data usage are adequate and functioning as intended	Complete	05/18/2018
17-211	Patient Privacy System (Fair Warning)	Determine whether controls around patient privacy and the Fair Warning application are adequate and functioning as intended	Complete	05/21/2018
	Follow-up Audits			
18-104	Follow-up on Open Recommendations		Complete	09/11/2018

The Hemophilia-integrated audit #17-204 was included in the FY2017 audit plan as the area had not been audited in some time and due to increasing operating revenue, and the implementation of a new billing system. Based on a reassessment, we subsequently determined that other carry-forward audits have a higher relative risk and the 500 budgeted hours planned for the Hemophilia audit would be better allocated to those projects.

Audit 18-209 Practice Partner (500 hours) is an audit of the School of Nursing electronic medical record system. The school discontinued using Practice Partner and now uses Allscripts, which is the same EMR used by the school of medicine. The second audit is 18-204 Office 365 (450 hours). Office 365 is a cloud-based software that, among other things, allows for online collaboration and information sharing. During the performance of the FY2018 risk assessment, we anticipated that Office 365 would be widely used by UTHealth employees. However, only limited functionality is available to UTHealth employees and the software is not widely used.

Three hundred (300) budgeted hours from these audits will be allocated to the Benefits Proportionality audit, which is a requirement in the General Appropriations Act of the 85th Legislature. This audit will cover appropriation years 2015, 2016 and 2017, which coincides with our fiscal years. The balance of the hours from the cancelled audits will cover the current position vacancy and temporary assignment of audit personnel to UTPhysicians.

Audit 18-207 (364 hours remaining) is an audit of clinical timeshares. As we were performing our risk assessment for this audit, we identified the true risk lies in timeshare personnel accessing electronic health records/PHI through remote access. Two other audits, one on the FY2018 audit plan (Citrix) and one on the FY2019 audit plan (Two-Factor Authentication), address remote access risks. We discussed this modification to key stake holders who agree with our assessment. We performed an assessment of available hours remaining in FY2018, including anticpated position vacancies that will occur in the remainder of the fiscal year, and therefore determine this audit can be cancelled without replacement.

Audit 18-110 Medical Service Research and Development Plan (300 budgeted hours) is an audit of compliance with bylaws and processes. Audit 18-113 Medicare Access and Chip

Reauthorization Act (400 hours) is a compliance, which falls under the MSRDP. Thefore, the MSRDP audit was cancelled without replacement.

Compliance with the Benefits Proportionality Audit Requirements for Higher Education Institutions

Rider 8, page III-45, the General Appropriations Act (85th Legislature, Conference Committee Report), requires higher education institutions conduct an internal audit during fiscal year 2018 of benefits proportionality by fund, using a methodology prescribed by the State Auditor's Office. The audit is required to examine appropriation years (AY) 2015 through 2017, and be completed no later than August 31, 2018. To comply with this requirement, a Benefits Proportionality audit (#18-116) was included in UTHealth's 2018 annual audit plan and the audit results have been submitted.

Compliance with the Texas Education Code §51.9337

Senate Bill 20 (84th Legislative Session) made several modifications and additions to Texas Government Code (TGC) and Texas Education Code (TEC) related to purchasing and contracting. Effective September 1, 2015, TEC §51.9337 requires that, *"The chief auditor of an institution of higher education shall annually assess whether the institution has adopted the rules and policies required by this section and shall submit a report of findings to the state auditor."* UTHealth's Auditing and Advisory Services conducted this required assessment for fiscal year 2016, and found the following:

Based on review of current institutional policy and the UT System Board of Regents' *Rules and Regulations*, UTHealth has generally adopted all of the rules and policies required by TEC §51.9337. Review and revision of institutional and System policy is an ongoing process. These rules and policies will continue to be assessed annually to ensure continued compliance with TEC §51.9337.

III. Consulting Services and Non-audit Services Completed

Report No.	Report Date	Name of Project	High-Level Consulting Engagement/Non-audit Service Objective(s)	Observations/ Results and Recommendations
18-501	N/A	SPH Inventory	Review internal controls surrounding inventory	Results communicated to the department.
18-502	N/A	International Travel	Review of internal controls regarding international travel	Results communicated to the department.

IV. External Quality Assurance Review (Peer Review)

BAKER TILLY

Candor. Insight. Results.

June 28, 2017

Mr. Daniel Sherman, Chief Audit Executive
The University of Texas Health Sciences Center at Houston

In May 2017, The University of Texas Health Sciences Center at Houston (UT Health) Auditing & Advisory Services (A&AS or IA) completed a self-assessment of internal audit activities in accordance with guidelines published by the Institute of Internal Auditors (IIA) for the performance of a quality assessment review (QAR). UT Health A&AS engaged an independent review team consisting of three internal audit professionals with extensive higher education and healthcare experience to perform an independent validation of A&AS' QAR self-assessment. The primary objective of the validation was to verify the assertions made in the QAR report concerning IA's conformity to the Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing* (the IIA *Standards*) and Code of Ethics, Generally Accepted Government Auditing Standards (GAGAS), and the relevant requirements of the Texas Internal Auditing Act (TIAA).

The IIA's *Quality Assessment Manual* suggests a scale of three ratings, "generally conforms," "partially conforms," and "does not conform." "Generally conforms" is the top rating and means that an internal audit activity has a charter, policies, and processes that are judged to be in conformance with the *Standards*. "Partially conforms" means deficiencies in practice are noted that are judged to deviate from the *Standards*, but these deficiencies did not preclude the IA activity from performing its responsibilities in an acceptable manner. "Does not conform" means deficiencies are judged to be so significant as to seriously impair or preclude the IA activity from performing adequately in all or in significant areas of its responsibilities.

Based on our independent validation of the QAR performed by A&AS, we agree with A&AS' overall conclusion that the internal audit function **"Generally Conforms"** with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and Code of Ethics, as well as with A&AS' conclusions regarding GAGAS and TIAA requirements. Our review noted strengths as well as opportunities for enhancing the internal audit function.

This information has been prepared pursuant to a client relationship exclusively with, and solely for the use and benefit of, The University of Texas System Administration and UT Health and is subject to the terms and conditions of our related contract. Baker Tilly disclaims any contractual or other responsibility to others based on its use and, accordingly, this information may not be relied upon by anyone other than The University of Texas System Administration and UT Health.

The review team appreciates the cooperation, time, and candid feedback of executive leadership, stakeholders, and A&AS personnel.

Very truly yours,

Baker Tilly Virchow Krause, LLP

an independent member of
BAKER TILLY

V. Internal Audit Plan for Fiscal Year 2019

FY 2019 Audit Plan	Budgeted	
Audit/Project	Hours	Description
Risk Based Audits		
CrowdStrike	500	UTHealth's Endpoint Protection Platform.
Guest Account System	450	Application for sponsoring and monitoring guest accounts.
Office 365	500	Subscription-based application that includes access to Office applications plus other productivity services enabled for the internet (cloud services).
REDCap (2 instances: SBMI + SPH)	500	Web-based application for building and managing online surveys and databases.
SBMI DSRIP Registry	500	Database housing Delivery System Reform Incentive. Payment (DSRIP) Projects, part of the Texas healthcare Transformation and Quality Improvement Program.
TAC 202	300	Texas Administrative Code 202 – Information Security Standards.
Two-Factor Authentication	350	Review of rollout of two-factor authentication.
C*Cure Badging System	450	Photo badging system.
Call Center	350	Review of patient call center processes.
Contract Audit (To be determined)	450	Will be performed based on risk.
DSRDP	300	Review to assess efficiency and effectiveness of operations of the Greenspoint Clinic.
IRB Process	500	Institutional Review Board (IRB) approvals of research involving human subjects.
MSRDP	300	Review compliance with MSRDP process or bylaws. Will be performed based on assessed risk.
Payroll	500	Review to assess efficiency and effectiveness of payroll processes.
Student Status	350	Review to assess efficiency and effectiveness of processes.
Carryforward	500	Carryforward of 2018 Audits.
Review and Validation	50	Review for compliance with UTS 142.1, Section 6 requiring audits of the monitoring plan to validate the assertions on segregation of duties and account reconciliations
Risk Based Audits Subtotal	**6,850**	

Required Audits (Externally and Internally)		
Financial Statements FY 2018	100	Controls over transaction testing, analytical review, and other procedures assigned as part of the financial assurance audit.
Financial Statements FY 2019	80	Interim work for FY 2019 financial statement audit
Assist State Auditor's Office and other external auditors	150	Provide assistance to the State Auditor's Office and other external audit functions
THECB	50	Provide an opinion on revenue and expenditure reporting of program funds
TEA Compliance (CLI)	100	Report on controls over te security of TEA data.
Executive Travel and Entertainment	100	Review of official function. And travel and entertainment expenditures
Required Audits Subtotal	**580**	
Risk-Based Consulting Projects		
Institutional Committees	284	Participation by A&AS in various internal committees.
Training/Assistance Provided by A&AS	100	Train/educate clients on risk and internal audit concepts, including IDEA.
Consulting Projects Reserve	300	Performance of consulting projects requested by management.
Finance & Business Services Consulting	650	*Provide reports to Payroll to identify bank account irregularities. *Provide reports to Procurement to identify duplicate payments, suspicious transactions, BuyCard irregularities, etc. *Analysis of Vendor Master File for irregularities (annual). *Periodic verification of lockbox portal (purge of old scanned check copies). *Review of Taleo (by Dec 2018). *Verification procedures around supplemental pay. *GECB user account review assistance. *Review of sole source/blanket POs.
IT Consulting	300	*Review of medical devices for compliance with Security Policy Workflow Agreements. [semi-annual] *Comparison of network access listing with active employee list. [semi-annual] *Review of Tiger Text adoption/usage. *Splunk alerting for high-risk applications.H32.
Intellectual Property Consulting	200	Review in conjunction with UT System initiative to review and develop

		methodologies to protect UTHealth's intellectual property.
Revenue Cycle Consulting	500	*High dollar inventory process review. *Develop DA around missing charges/patient refunds/denials/bad debt/credit balances.
School Consulting	300	*SOD: Inventory verificati+H25on of SD cards (surprise). *SOD: High dollar inventory process review. *Med School: Telemedicine use & reimbursement/licensing.
Sponsored Projects Consulting	150	*High dollar grant review (direct vs. indirect cost allocation).
Consulting Subtotal	**2,784**	
Risk-Based Reserve		
Management Requests/Emerging Risks	700	Hours to allow flexibility to add audits as additional risks are identified or to address rapidly changing areas.
Risk-Based Reserve Subtotal	**700**	
Investigations		
Investigations	300	These hours are allocated to perform work related to potential thefts or assist other risk mitigating functions.
Investigations Subtotal	**300**	
Follow-up		
Follow-up on Open Recommendations	600	Hours designated to perform periodic follow-up to validate the status of outstanding recommendations.
Follow-up Subtotal	**600**	
Development - Operations		
Data Analytics Development	250	Review of UTHealth generated reports and A&AS reports as part of the ongoing risk assessment process.
FY 2020 Audit Plan	250	Development of annual audit plan using risk assessment techniques as required by GC 2102
Internal Audit Annual Report	50	Preparation and posting of the Internal Audit Plan, Internal Audit Report, and other information as required by HB 16
Internal Audit Committee	500	Preparation of documents and reports presented at the quarterly meetings and related post meeting documentation.
Internal Process Improvement	200	Periodic review and updating of audit processes by management and staff.
Internal Staff Meetings	250	Bi-monthly departmental staff meetings.
TeamMate/IDEA Development & Maintenance	200	Maintenance and development of TeamMate database and IDEA.

UT System/External Requests	150	Time devoted to various external reporting requirements, information requests and other types of assistance provided to external agencies.
Development - Operations Subtotal	**1,850**	
Development – Initiatives and Education		
Continuing Professional Education	550	Professional trainings and CPE courses to keep certifications active.
Quality Assessment Review	100	Departmental process evaluation in preparation for next year's external quality assessment. Yellow Book standards require a QAR every three years.
Professional Activities (writing, publication, external presentations and participation in professional organizations).	200	Writing, publication, external presentations, and participation in professional organizations.
UT System Initiatives (committees, workgroups, etc.)	200	Participation in UT System initiatives including committees, workgroups, etc.
Development – Initiatives and Education Subtotal	**1,050**	
Total Budgeted Hours	**14,714**	

High Risks Not Included in FY 2019 Audit Plan	Explanation/Mitigation	Internal Audit Action
Memorial Hermann affiliation may be delayed, creating operation and budgeting uncertainties.	Monitor Developments	Risk will be re-evaluated and will continue to monitor developments.
Items may inadvertently be omitted from each of the respective MHH specific services contracts.	Monitor Developments	Risk will be re-evaluated and will continue to monitor developments.
Identifying Conflict of Interest and developing management plans may not be performed according to policy.	Covered under audit #16-119 Conflict of Interest Audit.	Report Submitted
Title IX issues may still occur	Covered under 15-114 Title IX Compliance audit	Report Submitted
New contract management system (Jagger) may not be employed consistently throughout the institution.	A&AS sits on the Contract Management System Steering Committee	Monitor developments
Purchasing processes in UTP may not take advantage of premier agreements or other procurement pricing advantages.	Covered under audit #18-114	Audit currently in progress
Harrassment by professors of Ph.D., residents and grad students may occur.	Covered under audit #15-114 Title IX Compliance audit	Monitor developments
Lack of mandatory training program for Title IX/Title VII may leave the university vulnerable to risk of litigation.	Covered under audit #15-114 Title IX Compliance audit	Risk will be re-evaluated and will continue to monitor developments.
Sponsor may not be billed at closeout.	Monitor Developments	Risk will be re-evaluated and will continue to monitor developments.
Current policy allows consensual relationship, which may put university at risk.	Covered under audit #15-114 Title IX Compliance audit	Report Submitted
Policy/structure and oversight may not be adequate for UTP procurement processes.	Covered under audit #18-114	Report Submitted

Physicians may be able to access their own medical record.	Covered by audit #17-211 FairWarning	Report Submitted
Relationships with hospital partners may be at risk.	Monitor Developments	Monitor Developments
Ability to maintain clinical programs may be difficult w/declining reimbursement rates.	Monitor Developments	Monitor Developments
Ability to grow research programs may be hindered with limited resources	Monitor Developments	Monitor Developments
Increase spending by CLI with Sun Net	Covered by audit #18-201 Security Policy Workflow Areements	Report Submitted
A user inadvertently introduces malware while in the Citrix environment.	Covered by audit #18-210 Citrix	Audit currently in progress
Internet of Things (IoT) is not tightly controlled.	There is currently an IoT policy	Will be covered in future NAC audit once solution/controls are built out.
Telemedicine communications are not properly secured.	Covered by audit #18-203 Telemedicine	Audit currently in progress
No defined policies and procedures regarding IoT	There is currently an IoT policy	Will be covered in future NAC audit once solution/controls are built out.
System owners are not performing quarterly (critical applications) or yearly (non-critical applications) access reviews	Covered by audit #18-206 System Access Reviews	Report Submitted
Students/residents create private Facebook groups and share PHI with each other	Difficult to detect without access to personal Facebook accounts.	Monitor Developments
USBs or laptops go missing	Encryption required for USBs and laptops.	Monitor Developments
Timeshares (rented facilities with IT equipment provided to our doctors) using equipment that has not been evaluated by IT Security. Doctors	Covered by audit #18-210 Citrix and the Two-Factor	Citrix audit currently in progress

are using Citrix to enter data into our E.H.R.	Authentication audit on the FY2019 audit plan	
Clinical data is sold without an informed consent being obtained from the patient.	UTHealth not currently selling data.	Monitor Developments

Our risk assessment methodology included interviews and questionnaires to update the annual risk assessment. The identified risks were organized into institution-wide areas such as financial management, human resources management, and purchasing/warehousing. We developed detailed risk assessments of high-risk areas of research, information technology, and patient care. For each identified risk, probability and impact were determine using three to seven factors such as regulatory environment and frequency of identification in responses for the financial/operational risks and scope of process and age of system for IT risks.

VI. External Audit Services Procured in Fiscal Year 2018

Service	Provider
Opinion on financial statements of UT Physicians (501a Corporation supporting UTHealth)	Blazek & Vetterling LLP Certified Public Accountants
Opinion on financial statements of UT System Medical Foundation (a Corporation supporting UTHealth)	Blazek & Vetterling LLP Certified Public Accountants
Opinion on financial statements of Harris County Psychiatric Clinic (HCPC)	BKD Certified Public Accountants
2017 External Audit – Status Report	Deloitte and Touche LLP (Deloitte) Certified Public Accountants
Audit of the Ryan White Program	Harris County
Review to determine UThealth's Center on Aging level of contract compliance	City of Houston Health Department
Audit for federal compliance of the Student Financial Aid Cluster	State Auditor's Office

VII. Reporting Suspected Fraud and Abuse

UTHealth's home page contains a link to information on how to report suspected fraud, waste, and abuse. The information has a link to the State Auditor's fraud reporting website and its hotline number, as well as information on the various ways to report suspected fraud internally. Institutional policies and procedures address the requirement to report fraud and the Standard of Conduct Guide, applicable to all employees addresses the reporting of fraud. The intranet sites of the departments of Institutional Compliance and Auditing & Advisory Services contain information and links for reporting suspected fraud.