Office of Internal Audit

UT Southwestern Medical Center

Research Data Protection and Integrity Audit

Internal Audit Report 19:11

September 25, 2019

Table of Contents

Executive Summary

Background

The UT Southwestern Medical Center (UT Southwestern) mission statement highlights research as a key initiative in *"Research that solves for unmet needs by finding better treatments, cures, and prevention with a commitment to ensuring real world application."* Research activity is carried out in over 200 labs including basic science departments (12), clinical departments (21), and research centers (15), contributing to investigations ranging from the microscopic level to the whole patient. Research studies performed by investigators range from basic and applied sciences to pre-clinical and clinical studies. Funding from federal and state agencies, commercial sponsors, foundations and other sponsors total $470 million per year in support of ongoing research studies.

The Vice Provost and Dean of Research has oversight for research operations, including compliance with laws and regulations. The Research Integrity Officer reports to the Dean of Research and has responsibility for handling allegations of scientific misconduct involving biomedical or behavioral research or research training. In addition, various offices support the research mission and provide guidance, administrative support and training services for the investigators and their teams.

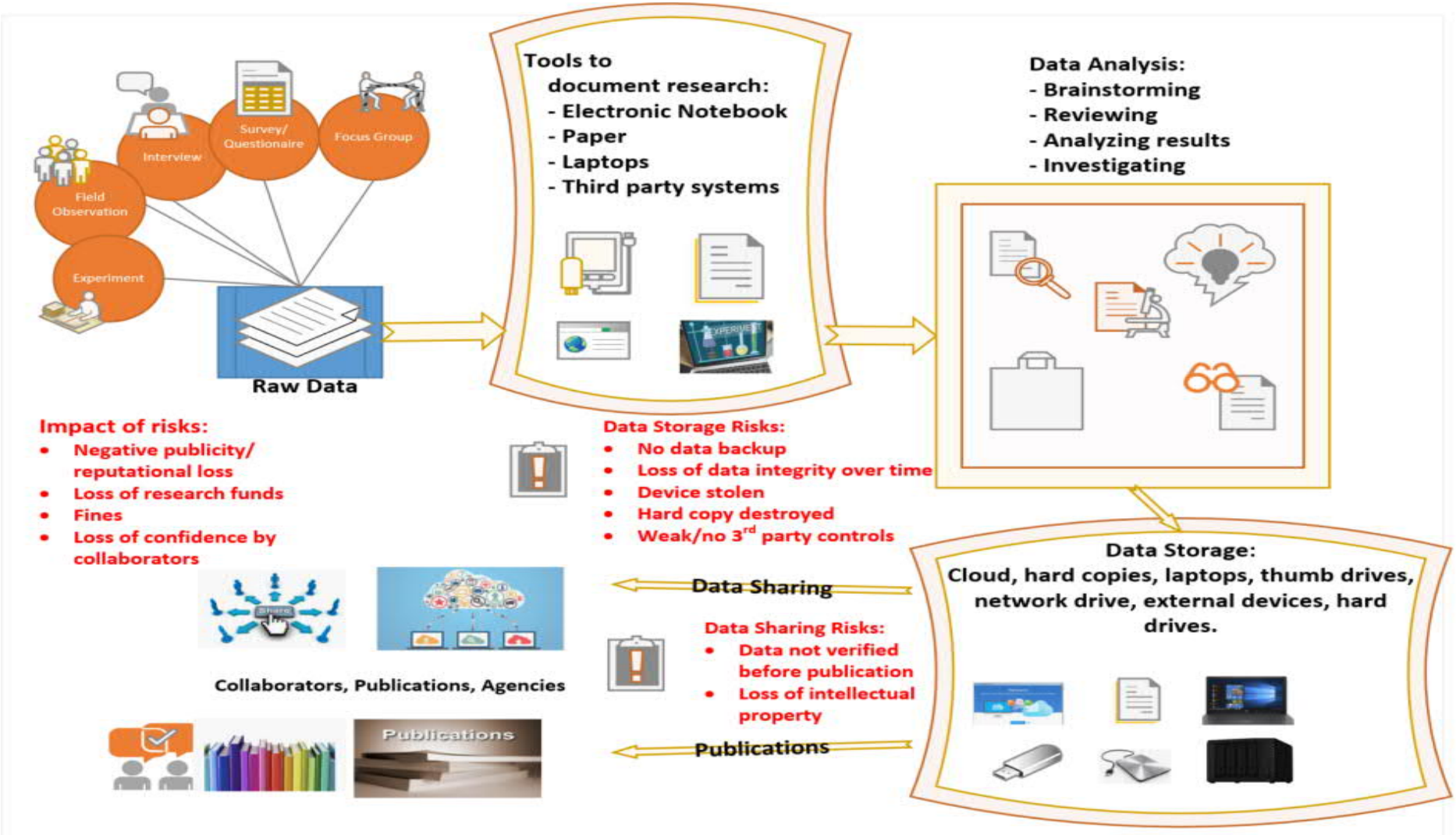
Research data is defined as recorded factual materials commonly accepted as necessary to document and support research findings. The data represents scientific information collected during the course of a research study that is organized into summary statistics and tables. Investigators document research procedures performed and results using a variety of methods or tools including; electronic or paper form lab notebooks, research-specific equipment, spreadsheets and other database programs.

UT Southwestern offers tools to support the compilation of research data, however researchers are allowed to use the tools that they feel best support their needs. Available software tools include Core LIMS (Lab Information Management System) for managing research data associated with pre-clinical drug discovery research; Electronic Lab Notebook (ELN) used for keeping track of individual research, collaborating with other investigators, or sharing resources; and REDCap, used primarily for research surveying.

As part of this review, a survey was conducted in coordination with the Vice Provost and Dean of Research to identify tools used by researchers across UT Southwestern. Survey results revealed that research data is managed or backed up in various ways and each lab has their own procedures for determining storage and retention methods.

Executive Summary

The following graphic provides an overall illustration of the use of research data and related data protection and storage risks.



Executive Summary

Scope and Objective

The Office of Internal Audit has completed its Research Data Protection and Integrity audit. This was a risk based audit and part of the fiscal year 2019 Audit Plan. Audit procedures included interviews with stakeholders; review of policies, procedures, and other relevant documents; researcher survey tools; and data analytics. The audit scope included research data activities from January 2018 to April 2019. The audit objectives were to review and assess the effectiveness and efficiency of processes and controls that ensure achievement of objectives, including:

- Compliance with key regulations and institutional policies and procedures,
- Safeguarding of research data including personal health information (PHI), proprietary and intellectual property developed in research, as well as,
- Methods and controls for data sharing and publication to protect the integrity of UT Southwestern research data.

We conducted our examination according to guidelines set forth by the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

Conclusion

Due to the scope and breadth of research activities at UT Southwestern and variability in methods used to track, compile and protect research data, a robust research data governance structure is needed to ensure research activities are conducted in a manner to protect the integrity of the research data, comply with sponsor requirements, policies and procedures, regulations and other requirements. In addition, central oversight would ensure there is effective data management, retention practices and brand protection. The governance structure should also include monitoring of key activities to assist in ensuring expected activities are occurring as intended.

In addition, the current lab guidelines on maintaining research data should be formalized and refresher training provided to investigators and their teams to reinforce standards and best practices for hardware use, data storage, access controls, back up and retention methods. Clarifying research publication standards, reemphasizing data use agreement requirements and implementing quality assurance procedures will improve compliance with data confidentiality requirements and further ensure research data integrity.

Executive Summary

Included in the table below is a summary of the observations, along with the respective disposition of these observations within the Medical Center internal audit risk definition and classification process. See Appendix A for Risk Rating Classifications and Definitions.

Priority (0)	High (1)	Medium (2)	Low (0)	Total (3)

Below are risk-ranked improvement opportunities:

1. **Strengthen Institutional Research Data Governance Structure & Oversight** – A defined research data governance structure is not in place to provide oversight and monitoring of effective data management and brand protection, increasing non-compliance with grantor requirements, policies and regulations, and potential reputational risk.
2. **Update Research Lab Notebook Policies and Procedures to Increase Data Protection Standards –** Lab research data compilation and storage guidelines need to be disseminated to principal investigators to ensure consistency in data compilation and data protection and storage methods to reduce the risk of loss of data, incomplete or inaccurate data.
3. **Enhance Research Data Sharing and Security Requirements –** Monitoring is not in place to ensure data use agreements are appropriately included in research data sharing contracts, increasing the potential for non-compliant sharing of confidential data and reputational harm.

Management has plans to address the issues identified in the report and in some cases has already implemented corrective actions. These responses, along with additional details for the key improvement opportunities listed above, are in the Detailed Observations and Action Plans Matrix (Matrix) section of this report.

We would like to take the opportunity to thank the department and individuals included in this audit for the courtesies extended to us and for their cooperation during our audit.

Sincerely,

Valla F. Wilson, Vice President for Internal Audit, Chief Audit Executive

Executive Summary

Audit Team:
Elias Dib, Senior Auditor
Robin Irvin, Manager, Internal Audit
Jeff Kromer, Director, IT & Specialty Audit Services
Melinda Lokey, Director, Internal Audit
Van Nguyen, Supervisor, Internal Audit
Gabriel Samuel, Senior IT Auditor

Cc: Claire Aldridge, Associate Vice President, Commercialization and Business Development, Office of Technology Development
Shashea L. Adams-Guess, Assistant Vice President, Planning & Advancement Services
Melody Bell, Assistant Vice President, Academic Information Systems
Arnim E. Dontes, Executive Vice President, Business Affairs
W. P. Andrew Lee, M.D., Executive Vice President for Academic Affairs, Provost and Dean
Megan Marks, Ph.D., Assistant Vice President, Sponsored Programs Administration
Marc E. Milstein, Vice President & Chief Information Officer, Information Resources
Heather Mishra, Associate Vice President, Academic & Administrative Information Resources
Rhonda Oilepo, Director, Human Research Protection Program
Stacy Pritt, D.V.M., Assistant Vice President, Conflict Of Interest and Institutional Animal Care & Use
Russell Rian, Director, Brand Communications and Public Relations, Office of Communications
Nancy Rollins, M.D., Associate Dean, Clinical Research
Elliott Ross, Ph.D., Professor, Pharmacology Department and Institutional Research Integrity Officer
Nathan Routen, Information Security Architect, Interim Chief Information Security Officer
David W. Russell, Ph.D., Vice Provost, Dean of Research
Cameron Slocum, Vice President and Chief Operating Officer, Office of Academic Affairs
Thomas Spencer, Ph.D., Assistant Vice President, IR Operations and Compliance, Academic and Administrative Information Resources

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: High ● **1. <u>Strengthen Institutional Research Data Governance Structure & Oversight</u>** There are Institutional standing committees and Dean's standing committees for clinical and preclinical research studies, lab safety programs and equipment use; however, there is no overarching structure over the management of raw data generated from scientific procedures relative to academic basic research. Insufficient oversight and monitoring of data management increases the risk of data integrity issues and non-compliance going undetected, resulting in a potential loss of funding and reputational damage. Additionally, the Information Systems Acquisition Committee (ISAC), which evaluates and approves system purchases over $25K, does not have an assigned institutional basic research representative to ensure appropriate research related needs are considered. A robust research governance structure ensures consistent data management and protection.	1. Create a formal non-administrative research data governance structure that provides oversight and guidance to the researchers and accountability for Principal Investigators (PIs) to maintain data quality, reliability and integrity. 2. Evaluate appointment of an additional research faculty member to ISAC with the goal of advancing data protection interests and needs of the research community. Coordinate with ISAC leadership to define key research criteria to be considered during evaluation of system purchases.	**<u>Management Action Plans:</u>** 1. Coordinate with the Executive Vice President for Academic Affairs and Provost, Dean of the Medical School and the Dean of the Graduate School of Biomedical Sciences to identify and develop a plan implementing this oversight function. 2. Develop a process to forward the nomination of a faculty member to ISAC for advancing the interest and needs of the research community. This faculty will collaborate with ISAC members on updated criteria for research and bring additional awareness to the Committee on research requirements. **<u>Action Plan Owners:</u>** Vice Provost and Dean of Research Institutional Research Integrity Officer Chief Information Security Officer **<u>Target Completion Dates:</u>** 1. November 30, 2019 2. December 31, 2019 3. January 31, 2020

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium 🟡 **2. <u>Update Research Lab Notebook Policies and Procedures to Increase Data Protection Standards</u>** Currently, there is no formal institutional level policy for research data storage, back up and protection. The Graduate School of Biomedical Sciences checklist provides guidance to departments in developing a research-specific notebook policy, but it has not been codified into a policy or recommended standard procedure. In addition, the checklist references different record retention periods when compared to UT Southwestern official record retention attestation guidelines. Lack of clarity on key research data requirements may lead to inconsistent research data practices. Survey responses received from 212 principal investigators (PIs) across campus, indicated the following: • 49% with no documented lab policies • 33% store data in hard copy • 38% use non-UT Southwestern issued devices as a hardware storing option • 31% use non-UT Southwestern issued devices for data back-ups • 43% back-up data manually	1. Form an interdisciplinary workgroup to assess potential implementation of the research data protection and integrity policy at the institutional and/or school level (e.g., Graduate School of Biomedical Sciences). This includes introducing recommended standards and leading practices for hardware use, data storage, cost models, access controls, back up and retention. 2. Identify a method to categorize research records, including development of an inventory of systems used for research activities. Then implement storage security requirements based on the significance and complexity of research conducted for the different type of records, specifically paper records. 3. Convert the checklist and guidelines to standard operating procedures based on workgroup recommendations to apply as a leading practice across the basic sciences departments and update research record retention requirements accordingly.	**<u>Management Action Plans:</u>** 1. Obtain input from the Executive Vice President, Academic Affairs and Provost to form a workgroup, including faculty researchers and Information Resources personnel, that will assess the potential for implementing a research data protection and integrity policy at the appropriate institutional level. Introduce recommended standards and leading practices for hardware use, data storage, access controls, back up and retention. Because local storage of data on a laptop does not provide for adequate security and backup, designated UT Southwestern network storage locations and devices are needed to ensure appropriate data protection and backup. Evaluate the feasibility of issuing UT Southwestern computing devices (computers, personal devices,etc) to all researchers including post-doctoral personnel and student researchers during their appointment. 2. Identify a method to categorize research records using a risk-based tier method and define data associated with high-risk studies. This will assist in developing a catalog of systems used for research activities to implement storage security requirements based on the significance

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Physical lab notebooks not efficiently maintained require more physical filing space and are subject to increased risk of damage or loss. Use of automated software and robust dissemination of lab notebook requirements, available systems and resources, enhance research data safeguarding, inventory management and record retention compliance.		and complexity of research conducted for the different type of records. This workgroup will also assess the feasibility of placing emphasis for researchers to use the electronic notebook going forward. 3. Convert the current checklist and guidelines, for retaining research notebooks, to standard operating procedures that apply across the basic sciences departments. Also, update research record retention requirements accordingly. **Action Plan Owners:** Vice Provost and Dean of Research Institutional Research Integrity Officer Chief Information Security Officer **Target Completion Dates:** 1. December 31, 2019 2. December 31, 2019 3. December 31, 2019

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium 🟡 **3. <u>Enhance Research Data Sharing and Security Requirements</u>** Research sharing and reporting practices are not consistently in compliance with UT Southwestern policies, guidelines or agreements. For example: • Standards for the use of Data Use Agreements (DUA) have been established; however, monitoring is not in place to ensure compliance with these requirements. • A significant number of PI survey responses indicated collection of protected health information (PHI) as part of the protocol but monitoring is not performed to ensure proper safeguards are in place, increasing the risk of noncompliance with HIPAA privacy rules. • Research data protection guidelines for international travel (e.g., personal and/or non-UT Southwestern sponsored business travel) have not been established. Absence of monitoring to ensure compliance with data use requirements increases the risk of potential inappropriate sharing of research data and non-compliance with agreements.	1. Form an operational workgroup to define research data sharing and collaboration requirements and update relevant policies and procedures. 2. Reemphasize the need to ensure data use agreement requirements are followed and implement monitoring requirements to ensure compliance with data use agreements, sponsor contracts and Privacy rules. 3. Implement research data protection guidelines for international travel (e.g., personal and/or business travel) to include the following: • Advanced disclosure of international travel trips • Encourage the use of UT Southwestern issued equipment with preinstalled malware protection software • Refrain from storing confidential research data on personal computers • Reemphasize VPN and two-way authentication for remote access to the network. Consider additional software to protect downloaded files and images containing PHI.	**<u>Management Action Plans:</u>** Coordinated effort with the Vice Provost and Dean of Research and the Offices of Technology Development, Sponsored Programs Administration, Clinical Research, Export Control Office and Institutional Review Board to implement: 1. A governance process that defines the types of data sharing agreement and relevant provisions, responsible owners, DUA approval and execution, policies and procedures, as well as opportunities for centralized processing. 2. A monitoring plan that ensures compliance with data use agreements, sponsor contracts and privacy rules. 3. Research data protection guidelines that address international travel for personal and/or non-UT Southwestern sponsored business travel. In addition, communicate availability of an Information Resources approved travel packet for researchers traveling outside of the United States.

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
		Action Plan Owners: 1. & 2. Vice Provost and Dean of Research Institutional Research Integrity Officer Associate Vice President, Commercialization and Business Development, Office of Technology Development Assistant Vice President, Sponsored Programs Administration Associate Dean, Clinical Research Chief Information Security Officer Assistant Vice President, Conflict Of Interest and Institutional Animal Care & Use Director, Human Research Protection Program 3. Chief Information Security Officer **Target Completion Dates:** 1. December 31, 2019 2. January 31, 2020 3. December 31, 2019

Appendix A – Risk Classifications and Definitions

As you review each observation within the Detailed Observations and Action Plans Matrix of this report, please note that we have included a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our audit. The following chart is intended to provide information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

	Degree of Risk and Priority of Action	
Risk Definition- The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.	**Priority**	An issue identified by Internal Audit that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.
	High	A finding identified by Internal Audit that is considered to have a high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.
	Medium	A finding identified by Internal Audit that is considered to have a medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level. As such, action is needed by management in order to address the noted concern and reduce the risk to a more desirable level.
	Low	A finding identified by Internal Audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level. As such, action should be taken by management to address the noted concern and reduce risks to the organization.

It is important to note that considerable professional judgment is required in determining the overall ratings presented on the subsequent pages of this report. Accordingly, others could evaluate the results differently and draw different conclusions. It is also important to note that this report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.