UTHealth Houston

Auditing and Advisory Services

22-201 Electronic Medical Record Data Extracts

EXECUTIVE SUMMARY

We have completed our assurance engagement of electronic medical record (EMR) data extracts. This engagement was performed at the request of the UTHealth Houston (UTHealth) Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

Background
Data extracts are requested for analytical (historical, trending, analysis) or operating (current data) purposes. If the requestor is a UTHealth employee, the data extract is delivered to an internal fileshare location where it is retrieved by the requestor. If the requestor is external to UTHealth (e.g., a vendor), the data extract is delivered to a UTHealth Secure File Transfer Protocol (SFTP) site or the vendor's SFTP site where it is retrieved by the requestor. A Business Associate Agreement (BAA) is required to be executed with a vendor prior to the release of data extracts containing protected health information (PHI).

Objectives
We focused exclusively on data extracts from the Epic application. Our objective was to determine whether controls around Epic data extracts are adequate and functioning as intended. Specifically, to determine if:
- An assessment of purpose, business need, and/or minimum use was performed before the data extract was processed.
- A data agreement and/or BAA was executed prior to release of the data extract to vendors.
- User access to the internal fileshare location and UTHealth's SFTP site is appropriate based on job responsibilities.
- Vendor access to the UTHealth's SFTP site is appropriate.
- For selected McGovern Medical School (MMS) departments, PHI is properly stored and protected.

Scope
- All Epic data extracts as of February 4, 2022.
- Users with access to the internal fileshare location as of February 4, 2022.
- Users with access to the UTHealth's SFTP site as of February 8, 2022.
- Vendor users with access to the UTHealth's SFTP site as of February 3, 2022. Management informed us there were none as of this date.
- PHI stored at MMS departments as of January 25, 2021. Management informed us this is the most current listing at the time of review.

Conclusion
Overall, controls around Epic data extracts are adequate and functioning as intended. We noted the following opportunity for improvement:

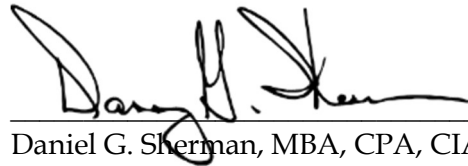| #	Observation Summary	Risk	Risk Rating
1	A formal process for documenting the assessment/quality review of data extract requests has not been established.	Insufficient documentation to support data extract requests.	**Medium**

OBSERVATIONS & MANAGEMENT RESPONSES

#1   Documentation
Cause A formal process for documenting the assessment/quality review of data extract requests has not been established. **Risk** Insufficient documentation to support data extract requests. **Condition** An assessment of purpose, business need, and/or minimum use for each data extract request is not formally documented. Additionally, a quality review of each data extract is informally documented using email. **Criteria** COSO Internal Control – Integrated Frameworks describes control activities as "actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out." Control activities are performed at all levels of the entity and may be preventive or detective in nature. Section 6.2.1 of ITPOL-004 *Access Control Policy* states: "Access to Protected Health Information and other confidential information under the jurisdiction of UTHealth will be assigned to users, programs, processes or other automated mechanisms based on minimum necessary requirements."
Recommendation(s) Develop and implement a process for documenting the assessment/quality review of data extract requests. **Rating** Medium
Management Response We will develop and implement the use of a checklist for the assessment/quality review of data extract requests. The checklist will be reviewed at the upcoming Analytics Steering Group meeting before implementation. **Responsible Party** Miguel Rodriguez, Director of Healthcare IT Analytics **Implementation Date** July 1, 2022

We would like to thank the Epic Operating staff and management who assisted us during the engagement.

Daniel G. Sherman

Daniel G. Sherman, MBA, CPA, CIA
Associate Vice President & Chief Audit Officer

OBSERVATION RATINGS

Priority	An issue that, if not addressed timely, has a high probability to directly impact achievement of a strategic or important operational objective of UTHealth or the UT System as a whole.
High	An issue considered to have a medium to high probability of adverse effects to a significant office or business process or to UTHealth as a whole.
Medium	An issue considered to have a low to medium probability of adverse effects to an office or business process or to UTHealth as a whole.
Low	An issue considered to have minimal probability of adverse effects to an office or business process or to UTHealth as a whole.

NUMBER OF PRIORITY OBSERVATIONS REPORTED TO UT SYSTEM
None

MAPPING TO A&AS FY 2022 RISK ASSESSMENT

Reference	Risk
FIN 170	With the implementation of Epic, there will be a disjointed and inefficient effort to develop data collection and reporting processes. (Medium)
IT 26	Applications/Databases containing sensitive data are not adequately protected. (High)
IT 38	Data requests are not based on business need and/or are processed with sensitive (and unneeded) data fields then not protected in accordance with their classification. (High)
IT 78	Multiple sets of the same data could increase risk while lowering quality of data. (High)

DATA ANALYTICS UTILIZED
None

ENGAGEMENT TEAM
AVP/CAO – Daniel G. Sherman, MBA, CPA, CIA
Manager – Brook Syers, CPA, CIA, CISA, CFE
Staff – Kathy Tran, CIA, CISA, CFE, CGAP

END OF FIELDWORK DATE
April 14, 2022

ISSUE DATE
May 23, 2022

REPORT DISTRIBUTION
Audit Committee
Kristi Bradley
Bassel Choucair
Kevin Dillon
Dr. Babatope Fatuyi
Dr. James Griffiths
Beverly Moore
Miguel Rodriguez
Ana Touchstone
Amar Yousif