THE UNIVERSITY OF TEXAS
MD Anderson ~~Cancer~~ Center

Department of Internal Audit

March 5, 2020

MEMORANDUM

TO: Elizabeth Ninan
Director, Perioperative Services

FROM: Sherri Magnus
Vice President & Chief Audit Officer

SUBJECT: Perioperative Services Division Review
Audit Control Number 19-110CF

Objective and Scope

Internal Audit conducted a review of the Perioperative Services Department in accordance with 2019 work plan. The objective of the review was to provide a general assessment of the financial, administrative, and compliance controls within the department. Work covered processes in place during the period September 1, 2017 to Aug 31, 2019 and any related periods.

Audit Conclusion

Our original project scope was revised to focus on several administrative and financial areas. The Institution was surveyed in 2019 by the Centers for Medicare and Medicaid Services, as well as the Joint Commission. Both of these surveys focused on patient safety and quality, evaluating care processes and technology, in Perioperative Services. We determined that the risks in these areas were adequately assessed as part of these surveys, and were therefore excluded from our scope. Internal Audit will consider the Department for a possible future audit.

In the interim, we wanted to communicate the following opportunities for improvement that were identified as part of our revised procedures.

The courtesy and cooperation extended by the personnel in the Department of Perioperative Services are sincerely appreciated.

Making Cancer History®

1.0 Strengthen Asset Monitoring and Reporting   *RANKING: MEDIUM*

The Department is not adequately monitoring or reporting its assets (totaling 1972). Specifically, the Department has not:

- Submitted the required missing property report forms to Materials Management for six out of 15 missing assets (totaling $219,700).
- Addressed 39 IT assets that have not been connected to the MDACC network for more than a year. Nine of these contain Protected Health Information (PHI) per institutional records.
- Completed offsite authorization and data security agreement forms for four IT assets remotely located.
- Tagged 74 assets as required.

The Information Resources Security Operations Manual (IRSOM) and the Asset Control Manual (ACM) provide requirements for oversight and protection of Institutional assets. Requirements include reporting of missing assets, maintenance of offsite asset authorizations, and property tagging. Without adequate controls over assets, there is an increased risk that theft or losses may occur and not be detected in a timely manner. Furthermore, unused assets and their contents, when not properly decommissioned or retired, may be misused.

Recommendation:
Management should strengthen controls related to assets to ensure that all required reporting occurs, offsite authorizations are completed, and assets are tagged. Management should also evaluate those assets that have not been connected to the network in an extended amount of time.

Management's Action Plan:
Responsible Executive: Elizabeth Ninan
Owner: Tasa Woods
Due Date: April 30, 2020

1. *Leadership in Perioperative Services will continue to partner with the director of clinical engineering and director of facilities to streamline the process for tracking and reconciling assets.*
2. *Perioperative Services will pursue using Aeroscout (RFID or like-technology) to assist in locating devices specifically for units that may connect to the network or contain PHI information. This can be in conjunction with RFID team efforts in relationship to the OR Controls project for existing devices.*
3. *Perioperative Services will also collaborate with the asset management team and asset finance team to help create a method early in the new asset acquisition process to associate new mobile equipment with locating devices.*
4. *Lastly, Perioperative Services will assign dedicated personnel to focus on asset management tasks to ensure timely troubleshooting and asset tracking.*

Making Cancer History®

2.0 Ensure Computers and Mobile Devices Are Protected   *RANKING: MEDIUM*

The Information Resources Security Operations Manual requires the protection of desktops, laptops, and mobile computing devices that view or store confidential information. We identified five mobile devices and iPads that did not contain sufficient protective measures. Without these device management protections, sensitive information could be accessible to unauthorized individuals.

Recommendation:
Management should coordinate with the Information Technology department to ensure all computers and mobile devices are protected.

Management's Action Plan:
Responsible Executive: Elizabeth Ninan
Owner: Tasa Woods
Due Date: April 30, 2020

1.   *Perioperative Services will proceed accordingly with the recommended action to coordinate with the Information Technology Department to develop sound processes to ensure that all computers and mobile devices are protected in accordance with institutional policy.*
2.   *Perioperative leadership will work with the Information Security team to provide education related to device management.*

3.0 Approve Timecards as Required   *RANKING: MEDIUM*

A review of a sample of timecards selected during FY2019 revealed that 99% were not approved in Kronos by department management, increasing the risk that errors or irregularities may not occur and not be detected or corrected. Management indicated that employee time is being monitored, specifically overtime, through reports created from their ancillary system. Institutional Policy requires department managers to review all time and leave captured in Kronos for accuracy and complete approval process in the system by 11:59 p.m. each Tuesday.

Recommendation:
Management should establish processes to ensure that all employee timecards are reviewed and approved in Kronos by management each week in accordance with institutional policy.

Making Cancer History®

Management's Action Plan:
Responsible Executive: Elizabeth Ninan
Owners: Jenise Rice for PACU Nursing
Observer: Ri Dorado for Main and Mays OR Nursing
Due Date for Interim Processes: April 30, 2020
Due Date: August 31, 2020

1. *Perioperative Services will continue to monitor overtime expenditures using overtime reports provided by timekeepers and the Peri-op finance team.*
2. *Perioperative leadership will work with managers to identify and remove barriers to weekly approval of Kronos time cards.*
3. *Perioperative Services supervisors, managers and associate directors will be required to complete Kronos training to include how to review/approve of timecard. This training will be added to orientation for new leaders.*
    a. *Supervisors, managers, associate directors will be given access to Kronos approval/editing tools (This is will be increased access from current access of view only)*
4. *Will ensure Perioperative leadership team complete time card review/approval processes in the new Kronos advanced scheduling (Dimensions) tool.*
5. *In the interim, leadership will continue with strict review process established with overtime approval form, overtime management reports, as well as create a Kronos report to be reviewed by managers/directors to oversee the frequency of Kronos corrections by month.*

Appendix A

Objective, Scope and Methodology:
The objective of the review is to provide a general assessment of the financial, administrative, and compliance controls within the department; however, all selected transactions occurred between September 2017 and August 2019, unless otherwise noted below.

As our scope was revised, our methodology included the following procedures:

- Interviewed key personnel and reviewed relevant organizational policies to understand financial and administrative processes.
- Reviewed physical inventory results and assessed processes and controls over assets.
- Reviewed IT assets reported as non-encrypted and validated current status.
- Tested procurement card transactions and reconciliations for compliance with institutional guidelines. *Note that our procedures did not include a review of non-procurement card expenditures for compliance with procurement/purchasing policies.*
- Reviewed documentation to ensure required monthly certification of selected expenditures, payroll expense reviews, and reconciliation of accounts.
- Reviewed non-grant account activity to determine whether deficit balances were properly resolved.
- Examined timekeeping and leave records to determine if institutional leave management guidelines were followed.

Our internal audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

Number of Priority Findings to be monitored by UT System: None
A Priority Finding is defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*

cc: Martha Salas
        Steven Drone
        Tasa Woods