UTHealth
The University of Texas
Health Science Center at Houston

16-211 Physical Access

We have completed our audit of physical access. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

BACKGROUND

Physical access controls are critical in restricting access to high-risk areas and protecting assets. A variety of physical access controls are employed across UTHealth depending on the location and type of assets. These controls include access control systems, visitor access procedures, periodic reviews of access, and incident response investigations.

OBJECTIVES

The objective of this audit was to determine whether controls over physical access are adequate and functioning as intended.

SCOPE PERIOD

The scope period was September 1, 2015 – August 31, 2016.

METHODOLOGY

The following procedures were performed:

- Obtained a list of high-risk safety areas from Safety, Health, Environment, and Risk Management (SHERM), animal care areas from Center for Laboratory Animal Medicine and Care (CLAMC), and high-value areas from Capital Assets Management (CAM). Judgmentally selected a sample of ten rooms, one with two protected areas, for a total of eleven areas tested. Obtained the list of employees with badge, biometric, and key access to areas, and assessed appropriateness of access given job titles and responsibilities. Analyzed physical access logs and obtained management responses regarding irregularities. Verified access controls followed applicable federal and state regulations and conducted site visits to verify visitor access procedures. Obtained evidence that approver lists are updated on an annual basis.
- Reviewed evidence of access listing subscriptions and verified access listings were approved on a regular basis. Verified physical access logs were reviewed on a regular basis.
- For a subset of the high-risk areas, conducted hold-open door tests and verified UT Police at Houston (UTP-H) received automated alarms. Verified incident response investigations were conducted as needed.
- Selected a sample of publicly-accessible network ports and verified access to the UTHealth network was restricted.
- Assessed the methodology for adding high-risk areas and installing access controls for reasonableness.

713.500.3160 phone 713.500.3170 fax
P.O. Box 20036
Houston, Texas 77225
www.uthouston.edu

- Obtained the list of employees with access to the CCURE and IRIS applications and assessed appropriateness of access given job responsibilities.

AUDIT RESULTS

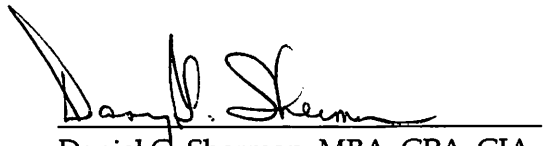
A&AS identified areas of improvement related to lost/stolen keys, badge access reviews, approver list updates, and badge/biometric access:

- For four high-risk areas, inappropriate access was noted for sixteen individuals; however, no evidence of unauthorized entry was identified. Additionally, one badge access listing was not sent to the approver during the most recent monthly review and two approver lists were not confirmed during the annual confirmation process.
- One of the keys for a high-risk area in our sample could not be accounted for and UTP-H was not notified.
- For two high-risk areas requiring biometric/badge access in our sample, five individuals either had biometric access with no badge access or badge access with no biometric access. No individuals were noted who inappropriately had both biometric and badge access, which is required to access these areas.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

None

We would like to thank the staff and management within UTP-H, SHERM, CLAMC, Harris County Psychiatric Clinic (HCPC), and McGovern Medical School who assisted us during our review.



Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

MAPPING TO FY 2016 RISK ASSESSMENT

Risk (Rating)	Not applicable. Audit was added during FY 2016.

DATA ANALYTICS UTILIZED

Data Analytic #1	Utilizing data analytics software, A&AS analyzed physical access logs to identify anomalies for successful and failed badge entry attempts.

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned	Tammy Tran
End of Fieldwork Date	December 12, 2016
Issue Date	January 19, 2017

Copies to:
Audit Committee
William Adcox
Michael Tramonte
Dr. Robert Emery
Amar Yousif
Raymond Gerwitz
Catherine Doughty

Issue #1

BADGE ACCESS REVIEWS

An access badge is a credential used to gain entry to an area having automated access control entry points. Entry points may be doors, turnstiles, parking gates or other barriers. Access badges use various technologies to identify the holder of the badge to an access control system. On an annual basis (more frequently if requested), UTP-H sends badge access listings to the applicable approvers for review. The listings are reviewed for appropriateness and changes are communicated back to UTP-H accordingly.

A&AS selected a judgmental sample of eleven high-risk areas, nine of which have badge access, and obtained the current badge access listings and most recent confirmation communications sent by UTP-H to the applicable approvers. We also inquired about the appropriateness of access with the applicable approvers. We noted the following exceptions for 5 of the 9 (56%) high-risk badge access rooms in our sample:

- For one room (MSE R204E), the access listing was not sent to the approver by UTP-H during the most recent monthly review.
- For four of the rooms in our sample, individuals with inappropriate access were noted as detailed below:

ROOM	# OF PERSONNEL WITH ACCESS	# OF PERSONNEL WITH INAPPROPRIATE ACCESS (% OF TOTAL)
MSB 2.221P	32	1 (3%)
MSB 2.404	14	1 (7%)
HCPC Pharmacy	22	2 (9%)
UCT 2035	643	12 (2%)
TOTALS	**711**	**16 (2%)**

For three of the rooms (MSB 2.221P, MSB 2.404, UCT 2035), the badge access listing was sent to the applicable approver by UTP-H for the annual review; however, the approvers did not respond. Management informed us there are hundreds of badge access listings sent to the applicable approvers by UTP-H and following up on all nonresponses is not possible given the current resources.

For the HCPC Pharmacy, the approver sent a request to remove the two employees with inappropriate access; however, UTP-H did not process the changes until the time of our audit procedures.

During our fieldwork, requests were sent to UTP-H by the applicable approvers and all individuals with inappropriate access were removed from the badge access listings. A&AS verified that the badge access listings were properly updated.

	APPROVER LISTS UTP-H informed us that badge access listings are maintained by approvers, who are at least manager-level employees. UTP-H sends requests to departments on an annual basis to confirm approver lists (names of approvers and contact information). A&AS reviewed the sample of nine high-risk badge access areas and verified that UTP-H obtained confirmation of the approver lists from the applicable departments. For 2 of the 9 (22%) rooms, UTP-H sent the annual confirmation of the approver list; however, it was not returned by the applicable department.
Recommendation #1	We recommend UTHealth management work with UTP-H to develop and implement access control procedures that, at a minimum, address access risk, control levels required, and review/approval requirements.
Rating	Medium
Management Response	The UTP-H Risk Mitigation and Risk Operations teams will review areas where access is restricted by badge access and provide a list of areas where appropriate increased control procedures will be implemented. The new procedure will include an escalation process for the top 10-15 security sensitive areas on campus ensuring the information is properly reviewed and necessary modifications are processed in a timely manner.
Responsible Party	Raymond Gerwitz, Director of Risk Strategy and Operational Excellence - UTP-H
Implementation Date	June 1, 2017

Issue #2	The Key/Card Access Control Policy states that keys are distributed to Key Controllers who are responsible for the authorization and distribution of keys to individuals, as well as maintaining accurate and current records of all keys issued. The policy also states that the individual key holder agrees to protect the key from loss or theft upon acceptance and immediately notify UTP-H if the key is lost or stolen. A&AS judgmentally selected a sample of eleven high-risk areas, seven of which have some combination of key access (five with badge/key/biometric/keypad access and two with key/keypad access), and reviewed the listings of employees that were issued keys by the applicable Key Controller. For one of the rooms (key/keypad access) in our sample, a key could not be accounted for and UTP-H was not notified by the key holder. The room houses high-value MRI machines. A&AS confirmed that, going forward, all missing keys will now be reported to the Director of Management Operations II - Clinical (DMO-C) who will ensure they are reported to UPT-H. Additionally, the DMO-C informed us that the circumstances around the missing key were researched and it was determined that rekeying the door was not necessary.
Recommendation #2	A process should be developed and implemented to ensure key holders notify UTP-H when a key is lost or stolen. Additionally, we recommend that the responsible Key Controller determine the circumstances around the missing key and take appropriate steps to mitigate the risk of unauthorized access.
Rating	Medium
Management Response	We researched the circumstances around the missing key and decided that rekeying the door was not necessary. Going forward, all missing keys will be reported to the DMO-C who will ensure that they are reported to UTP-H.
Responsible Party	Catherine Doughty, Director of Management Operations II - Clinical
Implementation Date	Implemented as of January 4, 2017

Issue #3	A&AS selected a judgmental sample of eleven high-risk areas, two of which require biometric access for entry. The iris of the individual is scanned and sent to UTP-H for upload to the biometric profile system (IRIS). In order to access a room protected by an IRIS scanner, individuals must have both an authorized biometric profile in IRIS and an authorized badge in the badge access system. A&AS reviewed the badge and biometric access listings for the two biometric access rooms in our sample. For one or both rooms, A&AS identified five individuals who incorrectly have either: • Biometric access with no badge access; or • Badge access with no biometric access We reviewed access logs and at no time during this audit was there evidence of unauthorized entry identified. There were no incidences where an individual was identified who inappropriately had both biometric and badge access, which is required to access these rooms.
Recommendation #3	We recommend an access review of these rooms be conducted and all access removed for individuals not requiring entry.
Rating	Low
Management Response	Environmental Health & Safety reviewed the listing of individuals who are authorized to have unescorted access to the designated rooms (e.g. successfully completed both the biometric authorization and badge access). Individuals who had not completed both steps were contacted and either assisted in completing both necessary steps or removed from both rosters (both the iris scanning and badge access rosters). Future routine checks will be performed to reconcile the two lists as part of our regular review of our security control program.
Responsible Party	Dr. Robert Emery, Vice President of Safety, Health, Environment and Risk Management
Implementation Date	Implemented as of January 4, 2017