UTHealth™
The University of Texas
Health Science Center at Houston

Office of Auditing & Advisory Services

18-203 Telemedicine

We have completed our audit of telemedicine. 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

Telemedicine involves the remote transmission of healthcare services and data from one location to another, including over the phone, internet, and video conferencing systems. Six telemedicine applications are currently being utilized by various McGovern Medical School departments across UTHealth, including Pediatrics, Pediatric Surgery, Neurology, Psychiatry and Behavioral Sciences, Cardiothoracic and Vascular Surgery, Physical Medicine and Rehabilitation, and Internal Medicine.

OBJECTIVES

The objective of this audit was to determine whether controls around telemedicine are adequate and functioning as intended.

SCOPE PERIOD

The scope period was all telemedicine initiatives and applications as of April 26, 2018.

METHODOLOGY

The following procedures were performed:

- Verified executed Business Associate Agreements were in place for all telemedicine applications.
- Selected a judgmental sample of telemedicine applications and obtained evidence all users have received proper training. Verified a review/approval was obtained from IT Security prior to implementation, technical controls are in place, encryption is used for transmission, and the application has been updated with current security patches and updates. Obtained access listings and verified appropriateness based on user type and/or job titles; selected a sample of users and verified appropriate access approvals were obtained.
- Obtained a list of all departments utilizing telemedicine, selected a random sample of clinics, interviewed practice managers to verify only approved telemedicine applications are being used, and performed a walkthrough of designated telemedicine patient areas to verify security and privacy controls are in place.

AUDIT RESULTS

A&AS identified the following areas of improvement:

- Formal policies and procedures around telemedicine applications have not been created.
- Service level agreements for telemedicine applications have not been executed.
- Training is not formally documented for two applications.

- Inappropriate access and inadequate documentation of access approvals were noted in some cases.
- One application was not current with security patches and updates.
- An annual reassessment of a high-risk application has not been performed.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM
None.

We would like to thank the staff and management within various McGovern Medical School departments, Medical School Information Technology (MSIT), and IT Security who assisted us during our review.

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

MAPPING TO FY 2018 RISK ASSESSMENT

Risk (Rating)	Telemedicine communications are not properly secured. (High)

DATA ANALYTICS UTILIZED

Data Analytic #1	N/A

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CISA, CFE
Auditor Assigned	Tammy Tran, CISA
End of Fieldwork Date	September 4, 2018
Issue Date	October 19, 2018

Copies to:
Audit Committee
Dr. Barbara Stoll
Dr. Ryan Walsh
Rick Miller
Amar Yousif
Bassel Choucair
Dr. Tzu-Ching Wu
Dr. Matthew Harting

18-203 Telemedicine

Issue #1	Section 164.308(a)(1)(i) Administrative Safeguards of the HIPAA Security Rule requires the implementation of policies and procedures to prevent, detect, contain, and correct security violations. A&AS noted there are no formal policies and procedures currently in place around telemedicine applications. Management informed us that due to the recent implementation of telemedicine, policies and procedures are currently under development but have not yet been implemented.
Recommendation #1	We recommend management develop a timeline around the implementation of telemedicine policies and procedures and track progress on an ongoing basis.
Rating	Medium
Management Response	We agree with the recommendation and will develop a timeline around the implementation of telemedicine policies and procedures and track progress on an ongoing basis.
Responsible Party	Dr. Ryan Walsh, Chief Medical Information Officer
Implementation Date	January 31, 2019

Issue #2	The National Institute of Standards and Technology (NIST) *Special Publication 800-146* recommends service level agreements be implemented to ensure service providers are held accountable for four types of promises: availability, remedies for failure to perform, data preservation, and legal care of consumer information. A&AS noted there are no service level agreements currently in place for telemedicine applications that define availability, remedies for failure to perform, data preservation, and legal care of consumer information.
Recommendation #2	We recommend management conduct a risk assessment of the telemedicine applications currently in use to determine if service level agreements should be executed. The results of the risk assessment, including any related decisions, should be documented.
Rating	Medium
Management Response	We agree with the recommendation and will conduct a risk assessment of the current telemedicine applications to determine if service level agreements should be executed. We will document the results and any related decisions.
Responsible Party	Dr. Ryan Walsh, Chief Medical Information Officer
Implementation Date	January 7, 2019

Issue #3	Control AT-3 of the Control Standards Catalog (a supplement to Texas Administrative Code 202) requires the organization to provide role-based security training to personnel: • Before authorizing access to the information system or performing assigned duties; • When required by information system changes; and • At a defined frequency thereafter. A&AS selected a judgmental sample of five telemedicine applications, obtained user access lists, and verified all users have received proper training. For 2 of the 5 (40%) applications, management informed us training is not formally documented. As a result, A&AS was unable to verify users of these two applications received proper training.
Recommendation #3	We recommend management formally document training conducted for all telemedicine applications.
Rating	Medium

Management Response #3a	We agree with the recommendation and will formally document training conducted for the telemedicine applications under our responsibility.
Responsible Party #3a	Dr. Ryan Walsh, Chief Medical Information Officer
Implementation Date #3a	January 31, 2019

Management Response #3b	For fellows, a log of consultations is kept by the responsible Assistant Professor as a verification of proficiency for fellowship. For new faculty members, one-on-one training is conducted by primary telemedicine faculty and proficiency certified at that time with mock consults. The primary telemedicine faculty will confirm via email that training has been conducted. The emails will be retained to document training has been conducted.
Responsible Party #3b	Dr. Tzu-Ching Wu, Telemedicine Program Director
Implementation Date #3b	August 1, 2018 (to be verified by A&AS)

Issue #4	Control AC-2 of the Control Standards Catalog (a supplement to Texas Administrative Code 202) requires account managers to create, modify, disable, and remove user access when necessary. It also requires a process flow for approval of access requests to information systems. Control AC-5 requires organizations to implement adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity. A&AS selected a judgmental sample of five applications, obtained user access lists, and performed the following: • Verified appropriateness of access given user type and/or job titles. • Selected a sample of users from each access list and verified appropriate access approvals were obtained. We noted the following issues: • For 2 of the 5 (40%) applications, access approvals were not documented. • For one application, 3 of 42 (7%) users had inappropriate access given user type and/or job title. • For one application, we noted an access approver who also had administrative access to create accounts.
Recommendation #4	We recommend management: • Develop and implement a process to ensure all access approvals are documented. • Deactivate the users with inappropriate access. • Remove the administrative access of the access approver.
Rating	Medium

Management Response #4a	We have deactivated the users with inappropriate access. We have developed and implemented the *Telemedicine: User Access for InTouch* procedure to ensure all access approvals are documented.
Responsible Party #4a	Dr. Matthew Harting, Medical Director of Pediatric Surgery Telemedicine Program
Implementation Date #4a	September 1, 2018 (to be verified by A&AS)

Management Response #4b	Access for new users is requested via email by the Program Manager and must be approved by the Telemedicine Program Director. A log is now kept of the username, date of access granted, and signature of the approver. Access has been deactivated for the users with inappropriate access. The Program Manager has retained administrative access and the responsibility for approving access has been transitioned to the Telemedicine Program Director.
Responsible Party #4b	Dr. Tzu-Ching Wu, Telemedicine Program Director
Implementation Date #4b	August 1, 2018 (to be verified by A&AS)

Management Response #4c	We agree with the recommendation and will develop and implement a process to ensure all access approvals are documented.
Responsible Party #4c	Dr. Ryan Walsh, Chief Medical Information Officer
Implementation Date #4c	January 7, 2019

Issue #5	Control MA-2 of the Control Standards Catalog (a supplement to Texas Administrative Code 202) requires the organization to schedule and perform maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. A&AS selected a judgmental sample of five telemedicine applications and verified whether each was current with security patches/updates. One of the applications in our sample was not current with security patches/updates.
Recommendation #5	We recommend management update the application with current security patches/updates, as well as develop and implement a process to ensure the application receives future security patches/updates on a timely basis.
Rating	Medium
Management Response	We agree with the recommendation and will update the application with current security patches/updates. Additionally, we will develop and implement a process to ensure the application receives future patches/updates on a timely basis.
Responsible Party	Dr. Tzu-Ching Wu, Telemedicine Program Director
Implementation Date	November 1, 2018

Issue #6	During third party security risk assessments performed by IT Security, application vendors are assigned a risk rating, which determines the frequency at which a reassessment is required to be conducted. Vendors assigned a high-risk rating are required to be reassessed on an annual basis. A&AS selected a judgmental sample of five telemedicine applications and verified whether a third party security risk assessment was performed by IT security prior to implementation. A third party security risk assessment was performed for all five telemedicine applications prior to implementation; however, we did note one application (rated as high-risk) that had not been reassessed by IT Security since its implementation in 2016.
Recommendation #6	We recommend IT Security perform a reassessment of the application, as well as develop and implement a process to ensure reassessments are performed at the required frequency.
Rating	Medium
Management Response	IT Security will perform a reassessment of the application, as well as develop and implement a process to ensure reassessments are performed at the required frequency.
Responsible Party	Amar Yousif, Associate Vice President of Information Technology Security
Implementation Date	January 31, 2019