UTHealth
The University of Texas
Health Science Center at Houston

16-203 Vendor Access

We have completed our audit of vendor 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

Vendors are granted access to information resources at UTHealth in a variety of ways:

- **SecureLink** – A remote access software utilized by UTHealth that provides complete control over third-party access, including the ability to customize restriction options for each vendor.
- **Virtual Private Network (VPN)** – Uses the internet to provide remote vendors secure access to the UTHealth network. Access can be limited to specific servers, web pages, or files as needed.
- **Guest Accounts** – To be granted access, an individual employed by the vendor must be sponsored by a faculty or administration and professional (A&P) employee at UTHealth. The individual must complete the Information Resources User Acknowledgement and Contractor Confidentiality forms, view the Guest Information Security Awareness training, and present these and identity documents to the Registration Agent (RA) or at one of the University Identity Verification Centers. Remote individuals must present these forms to a notary public.

OBJECTIVES

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

SCOPE PERIOD

The scope period was March 1, 2015 to February 29, 2016.

METHODOLOGY

The following procedures were performed for vendor access via:

SecureLink

- Obtained evidence that policies and procedures for granting access exist.
- Selected a sample of three vendors granted access through SecureLink and obtained evidence that the access was properly approved and configured.
- Verified that email notifications are sent to the SecureLink administrator and/or application steward/custodian when a vendor logs in to SecureLink.
- Verified that vendor activity is recorded in audit logs and historical files and that SecureLink is configured to disable vendor accounts after 60 days of inactivity.

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

16-203 Vendor Access

Virtual Private Network

- Obtained evidence that policies and procedures for granting access exist.
- Selected a sample of three vendors and verified that a Business Associates Agreement (BAA) is in place for those vendors with access to Protected Health Information (PHI).

Guest Accounts

- Obtained evidence that policies and procedures for granting access exist.
- Selected a sample of three applications, obtained a list of vendors granted guest access to each, and selected a sample of 20 vendor guest accounts. For each guest account, A&AS obtained evidence that the access was properly approved and the Information Resources User Agreement and Contractor Acknowledgement forms were completed. A&AS also verified that each guest account was properly renewed during the most recent yearly renewal process.
- For vendors with direct VPN access to the application, A&AS verified that two-factor authentication is required.
- For vendors with access to PHI, A&AS verified that a BAA is in place.
- Obtained the most recent scans for generic system accounts and verified that any default privileges/generic system accounts identified were renamed (to identify the vendor) or disabled.
- Verified that the Director of Practice Management Systems is the only individual with authority to approve guest account access for McKesson employees.

AUDIT RESULTS

A&AS identified areas of improvement related to BAAs, generic service accounts, and the required forms for guest accounts:

- Two vendors were granted access to PHI without an executed BAA in place.
- Generic vendor service accounts were used to log in to SecureLink.
- A number of Information Resources User Agreements and Contractor Acknowledgement forms could not be located at the time of our procedures.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

One. See Issue #1 below.

We would like to thank the staff and management within IT Security, Data Center Operations and Services, Administrative Technology, and Clinical Technology who assisted us during our review.

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

MAPPING TO FY 2016 RISK ASSESSMENT

Risk (Rating)	R.17 A guest account could be used to infiltrate the UTHealth network and plant malware or steal data. R.25 Vendors are inappropriately granted access to our systems.

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned	Lieu Tran
End of Fieldwork Date	May 13, 2016
Issue Date	July 29, 2016

Copies to:
Audit Committee
Andrew Casas
Richard Miller
Amar Yousif
Ryan Walsh
Kevin Granhold
Dr. James Griffiths

Issue #1	*HIPAA Security Rule 164.308* states that written contracts are required from business associates who maintain, create, receive or transmit e-PHI for covered entities. The business associate is required to safeguard this information according to the Security Rule. *Department of Health and Human Services, 45 CFR 164.308 - Administrative Safeguards* states that a covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. *UTS165 Standard 22.3* requires that any contract involving third-party access to, creation, or maintenance of PHI must include a BAA in a form approved by Institutional counsel or OGC. A&AS obtained the application inventory, selected a sample of critical applications, and obtained a list of vendors granted access to each application. We then selected a sample of vendors with access to PHI to verify that a BAA is in place. Of the eight vendors in our sample, two (25%) did not have a BAA in place at the time of our procedures. Management informed us that these two vendors are staffing agencies and the requirement for a BAA was not recognized at the time they were contracted. Additionally, the executed BAA with McKesson (vendor with access to GE Centricity Business) could not be located at the time of our procedures. McKesson also subcontracted with another vendor (Omega) that accesses PHI; therefore a BAA is required between these two entities. An executed copy of this BAA could not be located at the time of our procedures. Both BAAs were in force and subsequently provided by management.
Recommendation #1	We recommend that management: • Execute BAAs with the vendors identified in our testing. • Conduct an analysis to determine if there are any remaining vendors (that have access to PHI) for which a BAA is required. Execute BAAs as appropriate. • Develop and implement a process to ensure that BAAs are executed with vendors before they are allowed to access PHI.

16-203 Vendor Access

Rating	High
Management Response	BAAs were executed (as of April 2016) with the two vendors identified by A&AS. Clinical Technology staff internally audited vendor files and ensured vendors with access to PHI had signed BAAs on file, and instituted a central repository and filing system for maintaining the documents. A policy/procedure ("Authorization of Guest Accounts Approved By Clinical Technology") has been drafted for approving guest accounts as well as approving access to applications administered by Clinical Technology. The policy/procedure requires that a copy of the executed BAA must be on file with Clinical Technology before access to an application containing PHI is approved. The policy/procedure has been submitted to the UTP Policy Committee for approval and will be implemented by October 1, 2016.
Responsible Party	Andrew Casas & Ryan Walsh
Implementation Date	October 1, 2016

Issue #2	*UTS165 Standard 4.2(b) Access Management* requires the creation of uniquely identifiable accounts for all users, including accounts created for use by vendors. A SecureLink account is assigned to each individual vendor, including a generic vendor account with an individual access key. Multiple individuals at the vendor are able to use the generic vendor account, resulting in the inability to track individual user identities. For 3 of the 10 SecureLink sessions (33%) reviewed by A&AS, a generic vendor account was used to log in. The three sessions were undertaken by two different vendors. Of these two vendors, one had their access subsequently terminated.
Recommendation #2	We recommend that the generic vendor accounts be disabled and vendors only be allowed to log in with unique and identifiable credentials.
Rating	Medium
Management Response	We have terminated the access of the remaining vendor. Additionally, we have updated the Vendor Remote Server Access policy/procedures to state: * Each representative performing work on behalf of the approved vendor company must have a company issued email account which contains the representative's name or a unique ID associated to the representative which clearly identifies the representative as an employee of the company. * No generic email accounts may be used for registration in SecureLink.
Responsible Party	Kevin Granhold
Implementation Date	Implemented as of June 2016

Issue #3	*ITSOP-016 Guest Administration Process – Section 5.0 Standards* requires that guest accounts candidates complete and sign both the Information Resource User Acknowledgement and Contractor Confidentiality Agreement forms in the presence of a Registration Agent (RA). For remote guest account candidates, these forms must be signed before a notary public. Original forms are forwarded to Records Management office for storage/archiving. A&AS selected a sample of 20 vendor guest accounts registered in the Guest Administration tool and noted the following: • For 5 out of 20 (25%), the Information Resources User Agreement could not be located. • For 7 out of 20 (35%), the Contractor Confidentiality Acknowledgement Form could not be located.
Recommendation #3	We recommend that an analysis be performed to determine the underlying factors that resulted in the missing documentation, as well as determine if the issue extends beyond the items in our sample. Remediation efforts should be conducted in response to the analysis as deemed appropriate.
Rating	Low
Management Response	Identity and Access Management (IAM) and Records Management will work together to identify the factors that resulted in the missing documentation. We will create new procedures that will ensure the use of current forms that can be linked to the guest user. These changes will be communicated to the RAs that are responsible for the documentation. We will also implement audit controls to ensure the paperwork has been received by Records Management within an acceptable timeframe.
Responsible Party	Richard Miller & Amar Yousif
Implementation Date	January 1, 2017