January 22, 2015

Report on Exemption from Security Policy Audit #15-203

We have completed our audit of the exemption from security policy. 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

According to a recent study conducted by the Ponemon Institute, an organization that conducts independent research on privacy, data protection and information security policy, approximately 90% of health care organizations have exposed patient data - or had it stolen - in 2012 and 2013. The medical industry currently faces more breaches than the military and banking sectors combined. In 2014, Healthcare IT News reported that since the Health Insurance Portability and Accountability Act (HIPAA) breach notification requirement took effect in 2009, nearly 31.4 million people have had their protected health information compromised in privacy and security breaches. The Office for Civil Rights, the Health and Human Services division responsible for enforcing HIPAA, has levied more than $25.1 million in fines against healthcare organizations responsible for violating the privacy and security rules.

The American Health Information Management Association (AHIMA) has reported that stolen health insurance ID numbers can command up to $50 on the black market, compared to $1 for a stolen social security number. Health insurance ID numbers can be used by criminals to fraudulently bill insurance or Medicare, obtain free consultations, or secure prescription medications that can later be sold.

The use of mobile devices combined with the rise in the number of personnel authorized to view patient records has increased the risk of data theft and loss. Data stored on mobile devices should be encrypted where possible in order to prevent unauthorized access. Encryption is the process of converting data into an unreadable format that is reversible with the use of an encryption key or password.

The University of Texas Systemwide Policy 165 (UTS 165)

UTS 165 Security Practice Bulletin #1 (SPB-1) requires encryption in the event that confidential University data are to be stored on a portable computing device or a non-University owned computing device, and that encrypted data remain accessible in the event that the encryption key becomes lost or forgotten.
Report On Exemption From Security Policy

The encryption must use products and/or methods approved by the CISO. SPB-1 also allows for an exemption to the encryption requirement for specific circumstances or business needs relating to an individual program or department, or for broader circumstances that span the institution as a whole. Exemptions must be documented and include the following elements:

- A statement defining the nature and scope of the exemption in terms of the data included and/or the class of devices included.
- The rationale for granting the exemption.
- An expiration date for the exemption.
- A description of any compensating security measures that are to be required.
- The signature of the CISO, and in the case of an exemption resulting from a data owner request, the data owner’s signature.

Encryption

The Disk Encryption Policy (ITPOL-032) requires all UTH health desktops, laptops, and netbook computers to be encrypted with a University-approved whole disk encryption or full disk encryption method. ITPOL-032 outlines technical encryption standards, the exemption process, and penalties for violations. Exemption requests are submitted using the Exemption From Encryption Form (ITP-007) and approved by the Chief Information Security Officer (CISO). Exception requests unrelated to encryption are subject to a different process as described below.

Exceptions

The Information Security Program at UTH establishes policies and procedures that apply to all system and infrastructure owners of information technology resources. As there are situations when the strict application of policies could significantly impair or reduce the functionality of a service, an Information Security Exception Request Policy (ITPOL-016) was created. ITPOL-016 outlines the information that must be submitted with the exception request, the approvals needed, and the appeals process. Exception requests are submitted using the Exception Request Form (ITF-003) and approved by the CISO.

Medical and Scientific Devices

The Medical and Scientific Device Policy (ITPOL-035) outlines the way in which medical and scientific devices that store Protected Health Information (PHI) must be acquired, operated, and decommissioned so that the privacy and security of patient information is upheld. The scope of ITPOL-035 covers all medical, scientific, and other devices operated by UTH health and UTP that store PHI and are not covered by other encryption policies, e.g., the Disk Encryption Policy (ITPOL-032). Devices not owned by UTH health that are provided by vendors or business partners are also governed by ITPOL-035. Medical and scientific devices are assigned to four categories depending on the way in which they handle patient data and interact with computer networks and systems:

Category I - Unable to store PHI. Encryption is not required.

Category II - Ability to store PHI, but unable to connect to the wired or wireless computer network. Encryption is required or the device must be configured so that PHI is unable to accumulate beyond 100 records on the local media if encryption is not permitted by the manufacturer.
Report On Exemption From Security Policy

Category III - Ability to store PHI and connect to the wired or wireless network, but unable to interface with the Electronic Health Record (EHR) system or other patient care systems. Encryption is required or the device must be configured so that PHI is unable to accumulate beyond 100 records on the local media if encryption is not permitted by the manufacturer. Security patches, anti-virus software, or an in-line intrusion prevention system must be applied in order to mitigate the risk of network attacks.

Category IV - Ability to store PHI, connect to the wired or wireless computer network, and interface with the EHR system or other patient care systems. Encryption is required or the device must be configured so that PHI is unable to accumulate beyond 100 records on the local media if encryption is not permitted by the manufacturer. Security patches, anti-virus software, and an in-line intrusion prevention system must be applied in order to mitigate the risk of network attacks.

Unencrypted Devices at UTHealth Clinical Information Technology (CIT) and Medical School Information Technology (MSIT) are currently conducting a project to review all medical/research/scientific (MRS) devices to determine if an exemption from the encryption requirement is needed. As of January 2015, a total of 351 Category II/III/IV devices have been identified ("Project Queue") with the progress detailed below:

<table>
<thead>
<tr>
<th>Status</th>
<th>Number of Devices</th>
<th>Percentage of Total Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exemption Request Approved</td>
<td>50</td>
<td>14%</td>
</tr>
<tr>
<td>Exemption Request Submitted to IT Security &amp; Awaiting CISO Approval</td>
<td>24</td>
<td>7%</td>
</tr>
<tr>
<td>Currently Being Assessed for Encryption Requirement</td>
<td>110</td>
<td>31%</td>
</tr>
<tr>
<td>Not Yet Examined for Encryption Requirement</td>
<td>167</td>
<td>48%</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>351</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

OBJECTIVES

The objective of this audit is to determine whether the controls around exemption requests and compensating controls implemented for exempted equipment are appropriate and functioning as intended.

SCOPE AND METHODOLOGY

Through a review of UTHHealth policies and procedures, interviews with IT personnel and control owners, site visits, and an analysis of project metrics, Auditing and Advisory Services (A&AS) performed an audit of the exemption from security policy.
AUDIT RESULTS

Exceptions and Exemptions
A&AS selected a random sample of approved exception and exemption requests from January 2012 to September 2014 and verified approvals by the Chief Information Security Officer (CISO) and submitting departments, as applicable. We also verified that all requests had a valid expiration date and included all required information. While no issues were noted, going forward, we suggest that an expiration date field be added to the Exception Request Form ITF-003 and expiration dates be documented for all exception and exemption requests.

Compensating Controls
Compensating controls are required to be in place when an exception or exemption request is approved. Examples of compensating controls include not storing PHI on the device, restricting and limiting physical access to the device, limiting the accumulation of PHI records to less than 100, and/or labeling the device to show that it is not encrypted and therefore should not be used to store confidential information.

A&AS selected a sample of 25 requests (16 exceptions and 9 exemptions) during the audit period. We met with the control owners and verified that the compensating controls were being performed as indicated on the requests approved by the CISO. No issues were noted.

Unencrypted Devices
As discussed in the Background section above, CIT and MSIT are currently conducting a project to review all MRS devices to determine if an exemption from the encryption requirement is needed. In order to verify the completeness, A&AS compared the MRS devices currently in the Project Queue with the MRS devices reflected in the Information Technology Asset Management System (ITAMS). We identified 136 unencrypted devices in ITAMS that were not included in the Project Queue, from which we selected a random sample of fifteen.

We met with the device owners and reviewed each device to determine whether it stores or has the capability to store PHI, and if so, whether an exemption request has been submitted for approval. Of the 15 devices in our sample, six were Category I (unable to store PHI/encryption not required) and excluded from our testing. Eight of the nine remaining devices either contained PHI or had the capability to store it, and did not have an exemption request as required by ITPOL-035. The remaining device had an exemption in place; however, more than 100 PHI records were stored on it at the time of our procedures.

While conducting our site visits, we also observed an additional 18 unencrypted medical devices (11 owned by UTHealth and seven not owned by UTHealth) that either contained PHI or had the capability to store it, and did not have an exemption request as required by ITPOL-035. Of the 18, eight were not currently in the Project Queue to be assessed for exemption requirements. Three of the eight were not owned by UTHealth.

Additionally, CIT accompanied A&AS during our site visits and identified additional medical devices that either contained PHI or had the capability to store it, which were also added to the Project Queue.
In summary, unencrypted medical devices were identified by A&AS that: 1) either contain PHI or have the capability to store it; 2) for which an exemption request has not been submitted; and 3) at the time of our procedures, had not been identified by CIT/MSIT and included in the Project Queue. In some cases, system owners and custodians were unaware of the exemption from encryption requirements.

Recommendation 1:
We recommend that CIT and MSIT work together to develop an ongoing process for identifying new devices that may be in need of an exemption from the encryption requirement.

Management's Response 1A: The medical devices identified by both A&AS and CIT during the audit were added to the Project Queue. In regards to the unencrypted medical device with the compliance issue, management was informed and the issue has been rectified and verified. MSIT and CIT will re-inventory all locations and both inventory systems will be updated and reconciled during the project.

Responsible Party: Dr. James Griffiths and Bassel Choucair
Implementation Date: September 1, 2015

Management's Response 1B: Ultimately the CIT inventory system will be rolled into ITAMS, and all new medical devices that are approved via the MSIT purchasing application will be added to ITAMS, designated as a medical device, and tagged upon delivery. In addition, biomedical device tags will be utilized to designate Category II-IV for owned and non-owned devices.

Responsible Party: Dr. James Griffiths and Bassel Choucair
Implementation Date: January 31, 2016

Recommendation 2:
We recommend that periodic training or communications to system owners/custodians should be performed in order to reinforce the exemption from encryption requirement.

Management's Response: The current onsite auditing process includes (when requested) device training for clinical management and technicians, which targets verification of patient data and automated or manual deletion procedures. As of January 2015, we began sending medical device communications (which include encryption requirements) to the Physician Office Administrators, which we will expand to include System Owners. We will also determine the feasibility of creating formal training around encryption requirements, which could possibly be included in new hire orientation.

Responsible Party: Dr. James Griffiths
Implementation Date: August 31, 2015

Project Queue

A&AS met with the project owners and obtained the prior four months of reports associated with the project. We then performed an analysis to determine the projected timeframe for clearing the current Project Queue of MRS devices.
As of January 2015, A&AS determined that based on current staffing levels and monthly progress, it would take up to 13 months (February 2016) to finish reviewing the devices in the Project Queue. This projection is based on the average clearance rate over the prior four months. Given the increased risk associated with unencrypted devices, A&AS believes the progress is not adequate. Additionally, it is expected that additional devices (including those provided by vendors or business partners) will be added to the Project Queue as remaining sites are inventoried and other devices are identified.

Recommendation 3:

We recommend that management assess the need for additional resources in order to clear the Project Queue of unencrypted devices in a more timely manner.

Management’s Response: This has been addressed. In addition to the two full-time employees dedicated to this project, UTP administration approved the hiring of four contractors to assist with clearing the Project Queue and performing re-inventories. As of January 26, 2015, three of the four contractors have been hired. Interviews are currently in progress for the remaining position.

Responsible Party: Dr. James Griffiths
Implementation Date: January 12, 2015

CONCLUSION

Controls around exemption requests and compensating controls implemented for exempted equipment are generally appropriate and functioning as intended. Recommendations were made for identifying unencrypted devices that may need exemptions, increasing training or communications to reinforce the encryption requirements, and clearing the Project Queue of unencrypted devices in a more timely manner.

We would like to thank the IT Security, CIT, and MSIT staff and management who assisted us during our review.

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

DGS: BBS

cc: Audit Committee
Michael Tramonte
Andrew Casas

Rick Miller
Amar Yousif
Bassel Choucair

Dr. James Griffiths
Gene Chandler

Audit Manager: Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned: Lieu Tran

Issue Date: February 17, 2015