FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Information Security Controls Audit of the Mobile Health Center

Report No. 16/17-03

September 13, 2016

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: September 13, 2016

To: John Rock, Dean, FIU Herbert Wertheim College of Medicine and Senior Vice President for Medical Affairs

Pedro J. Greer Jr., Associate Dean for Community Engagement and Chair of Department of Humanities, Health, and Society

From: Allen Vann, Chief Audit Executive *for AV*

Subject: **Information Security Controls Audit of the Mobile Health Center Report No. 16/17-03**

The Mobile Health Center (MHC) is comprised of four mobile vans. MHC1 and MHC3 are used for primary care services, MHC2 is used for mammography services and MHC4 is not currently in use. The mobile vans rely on a dedicated information systems infrastructure, which includes routers, laptops and image servers to maintain the operations while staff members are assisting patients. Pursuant to our approved annual plan, we have completed an information security controls audit of the MHC.

The primary objective of our audit was to determine whether information security controls over the MHC were adequate and effective. Specifically, we evaluated the information security measures for confidentiality, integrity and availability of patient data.

Overall, our audit disclosed that the MHC's information risk is fair, i.e. information system controls are in place but can be improved. The MHC has opportunities to strengthen controls relating to patching laptops, removing dormant firewall connections, monitoring patient data access logs, disabling generic user accounts, and testing comprehensive business continuity. Our audit resulted in 12 recommendations which management agreed to implement.

We would like to take this opportunity to express our appreciation for the cooperation and courtesies extended to us during this audit.

Attachment

C: Claudia Puig, Chair, FIU Board of Trustees
Gerald C. Grant Jr., Chair, FIU Board of Trustees Finance and Audit Committee
FIU Board of Trustees Finance & Audit Committee Members
Mark B. Rosenberg, University President
Kenneth G. Furton, Provost and Executive Vice President
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Javier I. Marques, Chief of Staff, Office of the President
Robert Grillo, Vice President and CIO, Division of Information Technology
Liane Martinez, Executive Associate Dean for HWCOM Finance & Administration

TABLE OF CONTENTS

OBJECTIVE, SCOPE AND METHODOLOGY

We have completed an information security controls audit of the University's Mobile Health Center (MHC). The objective of our audit was to determine whether information security controls were adequate and effective. Specifically, we evaluated information security measures for confidentiality, integrity and availability of patient data.[1]

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* using a risk-based methodology. To accomplish specific Information Technology (IT) control objectives, we applied a governance, risk and compliance framework, which utilizes the *COBIT 5.0 Framework, Special Publication 800-53A Revision 4 Assessing Security and Privacy Control in Federal Information Systems and Organizations*. Audit fieldwork was conducted from January to July 2016.

During the audit, we:

- reviewed FIU's and MHC's policies and procedures, applicable Florida statues and federal laws;
- observed current practices and current patient data flow processes;
- interviewed responsible personnel;
- visited the mobile health vans; and
- tested selected process flow items.

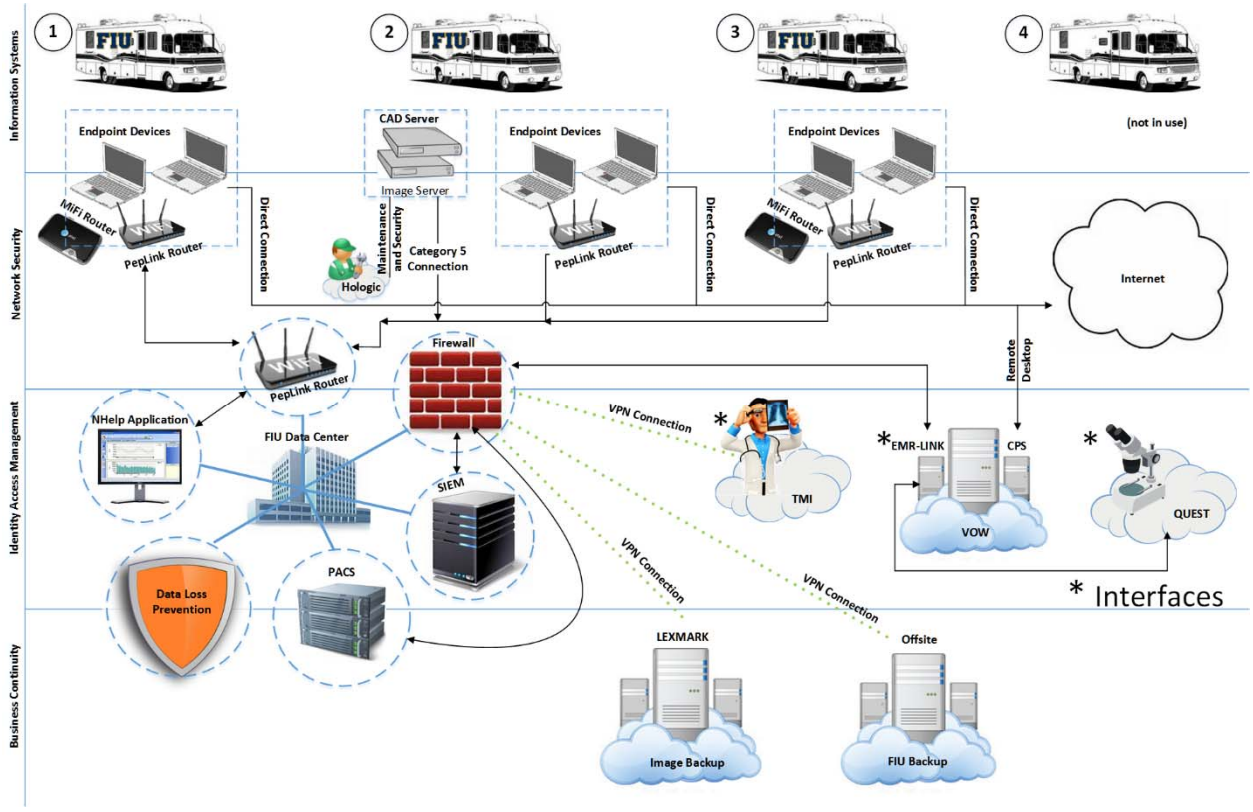
Sample sizes and items selected for testing were determined on a judgmental basis.

Though there were no external audit reports issued during the last three years with any applicable prior recommendations related to the scope and objectives of this audit, there were prior internal audit recommendations related to the scope and objectives of this audit requiring follow-up.

[1] A separate audit report was issued for financial and operational controls related to the MHC.

BACKGROUND

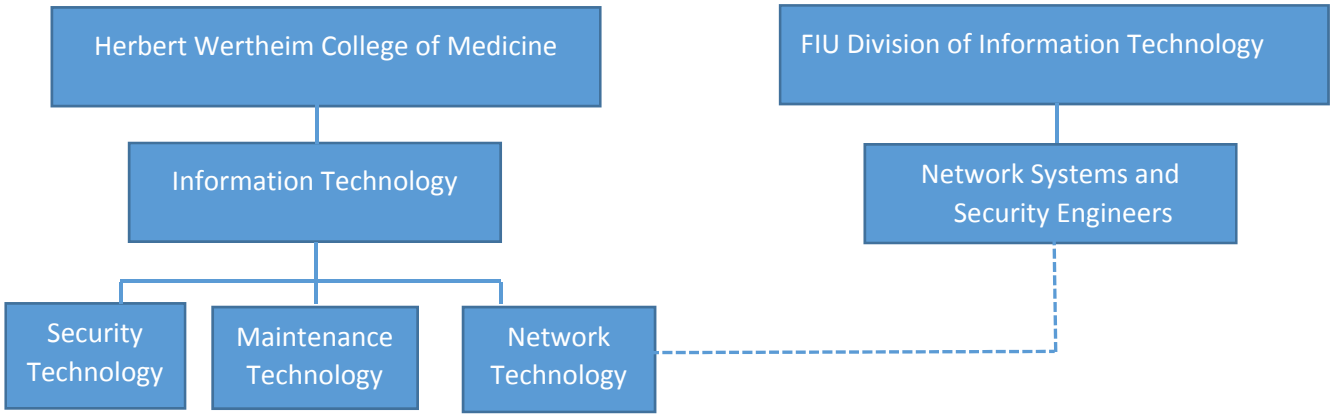
The MHC is comprised of four mobile vans. MHC 1 and MHC 3 are used for primary care services, MHC 2 is used for mammography services and MHC 4 is not currently in use. The mobile vans rely on dedicated information systems, which include routers, laptops and image servers to maintain the operations while they are assisting patients.



Since the mobile vans operate in different locations away from the University's network, each vehicle has a cellular router that is used to transmit data. The laptops that are stationed in each van connect through the cellular router and access the Internet, FIU Data Center and the Electronic Medical Record (EMR) application. The Mammography van has imaging servers that has the ability to transmit data wirelessly and also connect directly to the FIU Data Center when it is parked at the MMC campus parking garage. Additionally, MHC 1 and MHC 3 have a separate MiFi Router that acts as a cellular connection that can also be used outside of the van. Depending on the application, patient data may travel from the mobile van router to the FIU Data Center router, FIU Data Center Firewall, directly to the Internet, VPN or as a remote desktop connection. This includes in-house and vendor applications located in the FIU Data Center and third-party hosting companies that are used to complete the scheduling, imaging, testing and diagnosing of patients. Patient data is backed up at two separate locations.

Personnel

The MHC Information Technology is under the direction of the Associate Dean of Health IT within the Hebert Wertheim College of Medicine (HWCOM or College). The information system operations are managed by the College's IT Director and day to day activities are handled by members of her staff. Network systems are managed by the FIU Division of Information Technology's Network Systems and Security Engineering Department. A collaborative effort between the two departments is vital to maintain the continued operations of the MHC as shown below.



FINDINGS AND RECOMMENDATIONS

Overall, we concluded that the MHC's information risk is fair, i.e. information system controls are in place but can be improved. The MHC has opportunities to strengthen controls relating to patching laptops, removing dormant firewall connections, monitoring patient data access logs, disabling generic user accounts, and testing comprehensive business continuity. Furthermore, there were prior information system related recommendations that have not been fully implemented.

The areas of our observations are detailed below.

1. Information Systems Security Controls

Information Systems Security includes preventive, detective and corrective measures which are implemented and maintained (especially up-to-date security patches and virus definitions) on endpoint devices such as laptop that connect to the MHC network and protects them from malware, brute force attacks and unauthorized access.

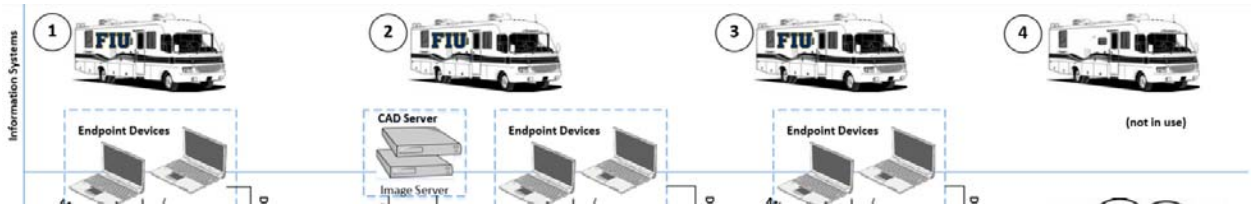


Figure 1: Information Systems Security Areas Tested

a) Asset Management

According to the College's Policy and Procedure, asset management reviews are required to be conducted on an annual basis. However, the reviews have been conducted every year and a half. This increases the risk that missing equipment containing sensitive data could go undetected for a longer period of time as discussed in the next section below.

During the audit, we observed that all of the devices listed in the provided Security Overviews documents were located in their respective areas and were stored behind locked cabinets. When in use, laptops were secured to the premises by a Kensington lock. According to the Clinical Director, the combinations are only known to the residing staff on-board the vans.

b) Security Incident

The HWCOM IT Security Manager discovered that two laptops were missing from MHC 1 during the annual asset management review in November 2015. According to the HWCOM IT Security tracking logs, five months elapsed before one of the devices was identified as missing. One laptop was never recovered. The other device was recovered from the employee responsible for the theft prior to her termination. The missing laptops should have been identified in a timelier manner through their monthly workstation review.

The College reported the incidents to the FIU Police, completed their Security Incident Report and collaborated with FIU Network Security Department. The Security Incident Report reflected that the College's Director of Clinical Applications determined that there were no unusual activities from the user, even though the former employee had access to patient data and there was evidence of printing patients' date of birth.

The College met with their internal team including legal, HR and IT. According to the Associate Dean of Health IT, the FIU HIPAA Security Officer and Compliance Officer were kept abreast and an FIU Legal associate acted as the HWCOM Privacy Officer throughout the security incident. The handling of the security incident follows the FIU Policy 1610.005, *Health Insurance Portability and Accountability Act Compliance,* which states that it is the responsibility of the Business Unit and Privacy and Security Officer of the Business Unit to work together to ensure that operational compliance matters are documented and adequately investigated.

c) Updates and Patches

The College has two employees that maintain the laptops operating system updates and patches. The laptops are used to check patient schedules, update medical test results and prescribe medication. Of the 14 laptops tested, six considered low risk or no risk as it relates to patient data. All 14 devices have encrypted hard drives that reduce the risk of unauthorized access to stored data. This is especially useful if a device is lost or stolen. However, for the other eight laptops:

- Four were missing 10 or more security updates.
- Two MACs did not have DLP installed as it is not available for that operating system. The computers are used to connect to the mammography server to move the images to the PACS server in the FIU Data Center.
- One was operational for over a year prior to installing McAfee antivirus.
- One laptop's McAfee AutoUpdate has not been operational for a year and a half.

In their current configuration, the eight devices have a higher than necessary risk of becoming infected by malicious software.

Additionally, there are two third-party managed devices in MHC 2 that are used to create and store patient medical images. The HWCOM IT does not maintain the devices and therefore cannot determine if the devices are adequately secured.

d) Risk Assessments

Risk assessments began in 2012 and initially concentrated on the physical controls over the vans themselves and not on the overall data process flow. According to the HWCOM IT Security Officer, a consultant was hired in 2014 to help improve the MHC's risk assessment. While there was an increase of applications and devices covered by the assessment, other areas within the data process flow, such as input from FIU Data Center, the Business Associate Agreements and SOC-2 Report for the MHC vendors were not included. After discussion with Division of IT management, we determined that risk assessments were not performed at the FIU Data Center. It is critically important to ensure that MHC data is protected in a HIPAA compliant manner. Additionally, the Security Overview Document did not include a lessons learned to address the improvement of existing controls as a result of the missing/stolen laptops.

Updating risk coverage by incorporating FIU Data Center risk assessments, Business Associate Agreements, SOC-2 Report, and lessons learned will increase the MHC's ability to identify and mitigate high risk areas.

Recommendations

The Mobile Health Center should:	
1.1	Ensure that a monthly workstation review is properly performed.
1.2	Work with the University's Network Systems and Security Engineering Department to ensure that: a) anti-virus products are properly installed and b) all laptops contain tracking application whose logs are periodically reviewed.
1.3	Work with the third-party vendors to ensure that the two managed systems are comprehensively protected.
1.4	Conduct more comprehensive risk assessment.

Management Response/Action Plan:

1.1 MHC staff will conduct weekly account of all workstations through a check-in/check-out process.

Implementation date: March 1, 2017

1.2 MHC staff will connect all workstations to FIU network and allow updates to be applied on a monthly basis. In event HWCOM IT staff must perform this activity, an evaluation to cost of resources will be performed.

HWCOM IT Security conducts periodic review of random set of laptops monthly to ensure antivirus is installed and up to date.

HWCOM IT Client Support Team will get Computrace license for remaining laptops. The checklist to review computrace logs is in place. Computrace alert notification regarding device name change is in place.

Implementation date: March 1, 2017

1.3 We will continue to request and review SOC2 reports and bridge letters from 3rd party vendors.

MHC staff will request regular reporting of system update maintenance conducted on the MHC systems by 3rd party vendors and provide to HWCOM IT.

Implementation date: March 1, 2017

1.4 MHC will include vendor's SOC2 review in risk assessment. In addition, the Division of Information Technology (DoIT) will conduct initial and periodic risk assessments on the FIU Datacenter and disaster recovery datacenter.

Implementation date: March 1, 2017

2. Network Security Controls

Network Security includes defining and protecting internal and external boundaries; limiting access points to the boundaries through the use of firewalls to allow for more comprehensive monitoring of inbound and outbound data traffic; documenting exception to the implemented firewall rules; and protecting the information during transit outside of controlled areas.

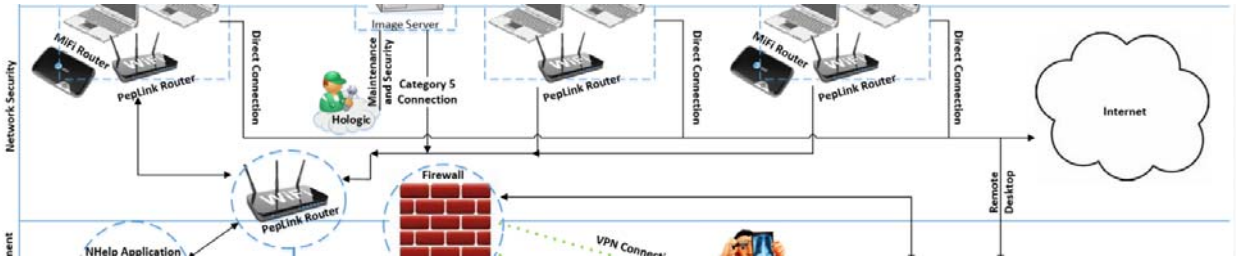


Figure 2: Network Security Controls Areas Tested

a) Monitoring

There are network data flow diagrams that adequately identify the internal and external boundaries for each of the three active MHC vans. Each van has a firewall deployed to protect the inbound and outbound data traffic. The firewall rules mostly lock down the devices to where they can only communicate with the EMR application and FIU information systems. However, there are two outbound rules that allow the endpoints to connect to outside sites. If a device was to become compromised, sensitive patient data could be sent outside the network without being detected. One method to help identify potential attack vectors for endpoint devices is through vulnerability scanning.

According to the College's Audit and Monitoring Control Policy and Procedure, the IT Security unit is responsible for ongoing monitoring of information systems. However, the University's Network Engineering and Telecommunications IT Assistant Director indicated that no vulnerability scans have been performed on the MHC endpoint devices. Vulnerability scans increase awareness of potential areas of compromise by identifying high risk configuration settings. We also noted that the Intrusion Detection and Denial of Service Prevention setting on the mammography van's router had been disabled. The router's Intrusion Detection and DoS Prevention settings protect the MHC data while in-transit and the network's continued operation.

MHC 1 and MHC 3 have MiFi devices that can connect the laptops directly to the Internet on the mobile carrier's network. The use of the MiFi devices bypasses the University's network monitoring mechanisms. According to the Network Engineering and Telecommunication's Network Security Engineer Manager, all MHC information systems that connect to the FIU Data Center's firewall are monitored by the security information and event management (SIEM)[2] system. Six of the 12 MHC information systems

[2] The SIEM monitors connected devices through log management and provides real-time situational awareness to identity malicious activity.

examined were connected to the FIU Data Center firewall. The information systems that were not monitored by the SIEM include the Van's Peplink Router, CPS and NHelp applications. Additionally, the Network Engineering and Telecommunication's Network Security Engineer Manager stated that connecting the MHC vans PepLink system logs to the SIEM would also enhance the monitoring of the MHC devices.

The effectiveness of the MHC monitoring controls are reduced by the lack of vulnerability scans, open HTTP outbound firewall rules, MiFi direct internet connections, and information systems that are not monitored by the SIEM. A non-monitored endpoint device could become compromised and go undetected, thereby increasing the security risk to sensitive patient data.

b) Data Flow Traffic

The College's Technical Security Measures Policy and Procedure Document 1.5 states that it is the HWCOM System Administrators' responsibility to work with the FIU DoIT Network Management Group to determine firewall rules for HWCOM server, storage and equipment to ensure networking and security requirements are met and transmission of sensitive data is secured over encrypted tunnels. In total there are 1,656 firewall rules that limit the ingress and egress data traffic to the devices that are part of the MHC data flow process. Over time the rules become outdated and no longer needed. According to the College's Audit and Monitoring Control Policy and Procedure, the firewall audit should be conducted by the HWCOM IT Security Unit on a monthly basis. We asked the UTS Network Security Department to run a zero hit count on the devices firewall rules to see which ones are no longer actively in use. The results showed that 98% of firewall connections have not been used in the last 12 months. Inactive firewall connections that are no longer needed provide unnecessary potential entry points for network attacks.

Recommendations

The Mobile Health Center should:	
2.1	Work with the University's Technology Network Services Department to: a) conduct vulnerability scans on MHC devices and b) connect the mobile vans' routers system logs and the CPS and NHelp applications to the SIEM.
2.2	Deny, reroute or remove direct internet data traffic, and review firewall rules and their corresponding zero hit results and disable all inactive connections.

Management Response/Action Plan:

2.1 a) HWCOM IT will work with FIU Technology Network Services to conduct a vulnerability scan of the MHC firewall. However, HWCOM IT will not open up firewall rules to allow inbound connection of vulnerability scanning system to access the MHC devices directly as these devices rely on the firewall for protection. As proprietary systems, the MHC devices maintain their own security measures as designed and configured by the vendor and part of this design necessate the need for firewall protection.

Currently, there are zero inbound firewall rules in place in MHC.

b) Feasibility assessment with connecting MHC routers to FIU DoIT SIEM will be conducted by Dec 15 which will result in future plan for central monitoring of router and system logs. MHC uses mobile broadband and sending logs to SIEM would consume bandwidth. Evaluation will include assessment of any impact to performance of the proprietary systems in the MHC which will impede patient care.

CPS and NHelp is not hosted onbroad on MHC.

Implementation date: March 1, 2017

2.2 HWCOM IT will request monthly zero hit reports from DoIT Network Services and take action to deny, reroute and remove rules as necessary.

Implementation date: March 1, 2017

3. Identity Access Management Controls

The Identity Access Management Controls we reviewed included policies, procedures, and the unique identification of user accounts. According to NIST sp800-53A Rev.4 AC 2.1, user identity and logical access should be managed to ensure that all accounts are appropriately established, modified and disabled in a timely manner.

Figure 3: Identity Access Management Areas Tested

a) Policies and Procedures

There are two separate HWCOM documents regarding User Access. The HWCOM Audit and Monitoring Control Policy and Procedure states that IT Security is responsible for checking workforce access on a quarterly basis. Secondly, an HWCOM Application Access Verification Procedure states that the HWCOM IT Security Unit is responsible for providing the data owners with a User Access Report and that they are responsible for reviewing member's access. The IT Security Manager stated that he formally reviewed the CPS, EMR-LINK and N-Help application's access on a yearly basis. However, Hologic, Laptops, Lexmark, Data Center PACS Servers, and FIU Backup did not have an assigned data owner and consequently were not reviewed.

We tested 79 active and 40 deactivated user accounts to determine whether they should be active or if they were deactivated in a timely manner. Our test disclosed that:

- One CPS terminated user's account was reactivated to get temporary access to her data. The account has remained active for a year and a half and should have been deactivated once the data was no longer needed.
- A CPS training account that was created in 2012 to train users in the EMR application's initial launch was still active.
- An assistant professor's CPS user account was still active almost 6 months after his termination.
- A laptop used to move patient image files had an active guest account.

There is an increased risk of unauthorized access to sensitive patient data when temporary accounts are still active after their intended use or are not deactivated in a timely manner.

b) Log Monitoring

FIU Policy No. 1670.015, *Authentication and Audit Controls for EPHI* states that the FIU will continuously perform monitoring, inspection, testing and auditing of such systems and software access logs in order to ensure the confidentiality, integrity, and availability of EPHI. In addition, the HWCOM Audit and Monitoring Controls Policy and Procedure states that applications are to be audited on a quarterly basis. However, we were informed that Audit logs have not been reviewed since the HWCOM Privacy Officer's departure in July 2015. In the absence of these reviews, increases the risk that inappropriate access to sensitive patient information goes undetected.

c) Uniquely Identifiable User Accounts

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. During our testing, we found 22 generically named user accounts with Administrator privileges to information systems including the patient medical records, images, and to the laptops used in the MHC Vans. The generic user accounts on the laptops have not been logged into for 630 days on average. Generic accounts, specifically with administrator privileges, reduces the information systems' ability to track individual user actions. Additionally, the user accounts could be used to bypass existing identity management controls.

d) Least Privileged Access

The COBIT 5.0 DSS06.03.03 control objective of least privileged user access is to only allow authorized user access that is necessary to accomplish assigned tasks in accordance with their business functions. In the ERM-LINK application we noted that the administrator access for the Director of Clinical Applications and the Clinical IT Analyst III was appropriate for their job duties. However, there are four accounts that have the ability to manage users, which includes the IT Assistant Director, a Licensed Practical Nurse, a test account, and a consultant. We also found that the College's IT Director has Administrator access on the FIU Backup process. Typically, senior management positions are consulted on activities but do not perform the actual System Administrator duties. The identified users' privileges should be reduced to align with their job duties and the account's purpose.

Data files that may contain sensitive patient information are flagged through the Data Loss Prevention mechanism and are stored on a separate server in the FIU Data Center. During our examination of the DLP server access, we noted that there were four FIU Network user groups that have access to the MHC DLP data. User accounts include the Associate Director of University Computer Systems, Assistant Director of University Computer System and the IT Manager of Computer Systems. However, only 4 of the 15 FIU Network Services users regularly log onto the Data Loss Prevention server as part of the job duties.

Having the ability to manage user accounts increases the Segregation of Duties risk in that a user could access another user's account and use it for malicious activities. Also based on the FIU Network Department jobs and positions, access to sensitive patient data located on the DLP server is not applied in a least privileged manner.

Recommendations

The Mobile Health Center should:	
3.1	Perform access report reviews as prescribed and assign data owners to the remaining applications and produce access reports for the data owners review.
3.2	Strengthen access controls by: a) Reviewing and deactivating the two temporary user accounts and guest account. b) Deactivating generic user accounts where appropriate. Disabling the four user accounts' administrative privileges.
3.3	Review application audit log files starting from June 2015.
3.4	Review the continuing need for the College's IT Director administrator access privileges to the backup system.
3.5	Work with the University's Network Services Department to ensure that Network Services employees access to DLP data is limited to the necessity of their assignments.

Management Response/Action Plan:

3.1 HWCOM IT will assign the data owners and add them to annual user verification procedure. FIU Backup is a veeam backup application with no user login interface. The Admin group has access to the Server where the application is installed. HWCOM IT Security Unit formally reviews the users that belongs in that group and ensures only appropriate users are in that group.

Implementation date: March 1, 2017

3.2 HWCOM IT Security will work with Clinical Applications Team on regular review of accounts which need deactivation and provide documentation on any exceptions to guest accounts with justification. Generic Admin account passwords are reset each time the laptop is rebooted.

Implementation date: March 1, 2017

3.3 The Privacy and Compliance Office will perform application audit log reviews based on HWCOM policy and procedure.

Implementation date: March 1, 2017

3.4 Access will be revoked by Sept 30, 2016.

Implementation date: September 30, 2016

3.5 In our discussion with the University's Netowrk Service Department, the DLP is managed and maintained by DoIT NSSE group. The DoIT NSSE will implement procedure for minimum necessary access to DLP data within the NSSE staff. The DoIT will conduct periodic audit of minimum necessary access based on established procedure.

Implementation date: March 1, 2017

4. Business Continuity Plan

The purpose of Business Continuity is to establish and maintain a plan to enable the business and IT to respond to incident and disruptions in order to continue operations of critical business processes at a level acceptable to the MHC.

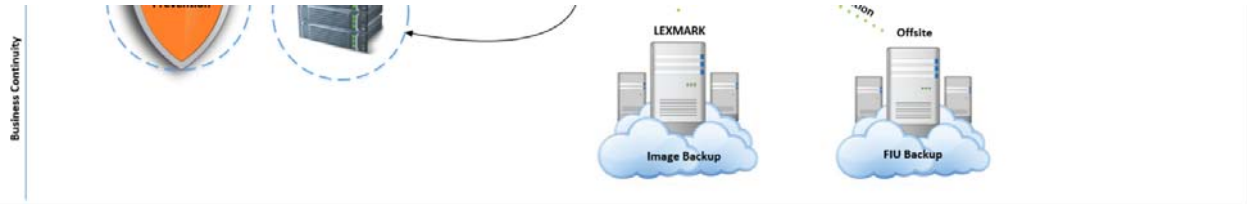


Figure 4: Business Continuity Areas Tested

a) Planning

There is a mix of in-house and third-party applications that are critical to the daily MHC operations. A periodic review of internal and external disaster recovery plans ensures the confidentiality, integrity and availability of the information systems data. The Plan was periodically reviewed and updated between May 19, 2014 through October 2, 2015. However, the Plan only identified four of the nine critical components of the MHC, which increases the risk to its patient data readiness.

b) Testing

According to the HWCOM Disaster Recovery Plan Policy and Procedure, it is the responsibility of the HWCOM Information Security Officer to ensure that the Plan is tested periodically and that it meet HIPAA Security Standards for safeguarding systems containing ePHI. However, only one simulated site test was performed on the PACS system back in August 2013. Table-top tests were performed for the file backup and the Neighborhood Outreach Portal a total of 11 and 13 times, respectively in 2015. The remaining six systems, which include the CPS, EMR-LINK, Lexmark, TMI, Quest, and Hologic were not tested. According to the Associate Dean of Health IT, the EMR-LINK, TMI and Quest application are third-party interfaces that cannot be tested by HWCOM; Lexmark is tested as part of the daily operations of sending and retrieving images from the backup service; and that they have a service level agreement with Hologic to maintain the imaging servers in MHC 2.

We reviewed the hosting companies SOC-2 report for the MHC's EMR application. According to the report, the company offers Backups and Disaster Recovery services and tests their contingency plans on an annual basis. It was not evident from the SOC-2 report whether the College patients' data is adequately protected.

Without the inclusion of the remaining systems into the Disaster Recovery Plan, the adequacy of the internal and external controls that ensure the confidentiality, integrity, and availability of the MHC information systems data is uncertain.

Recommendation

The Mobile Health Center should:	
4.1	Include all third-party applications in the Disaster Recovery Plan and Test sections to ensure their control effectiveness to protect the confidentiality, integrity and availability of sensitive patient data.

Management Response/Action Plan:

4.1 As noted in the background diagram on page 2, Hologic creates the image, stores a copy and sends it to PACS. From PACS, the same image is transferred to TMI, and Lexmark. The archived copy of the image from PACS is backed up in NWRDC Data Center as well.

HWCOM IT will request for regular reporting from 3rd party vendors on Disaster Recovery plan activities.

Implementation date: March 1, 2017

5. Implementation of Prior Audit Recommendations

In prior audit reports, there were six recommendations related to the Health Care Network's Billing, Collections, and Electronic Medical Record Systems reported by management as completely implemented. These same recommendations have applicability to the MHC through their shared systems.

Our examination of six prior recommendations included observation of actual processes, interviews with MHC personnel and testing of selected devices, which revealed that one was implemented and five were not fully implemented.

The test results for each prior recommendation examined are as follows:

University's Office of Internal Audit Report			
#	Recommendation	Implementation	
		Fully	Not Fully
(2013/14-07) Audit of the HCN's Billing, Collections, and Electronic Medical Record Systems			
6.2	Ensure that virus definition files and operating system security updates are updated in a timely manner.		✓
6.4	Ensure that workstation antivirus configuration settings cannot be modified by non-privileged users.	✓	
6.5	Review and remove generically named user accounts where appropriate.		✓
7.1	Review all firewall rule sets to ensure firewall rules are appropriate.		✓
8.3	Establish mitigating access controls, including the regular review of audit logs to ensure the appropriate use of data by multi-cross functional and those identified with specific skills sets.		✓
9.2	Periodically perform tests on the EMR and take corrective actions as necessary.		✓

Listed below are the recommendations determined to be not fully implemented accompanied by the results of our current observations.

1. Recommendation 6.2
   Ensure that virus definition files and operating system security patches are updated in a timely manner.

   Current Observation:
   As previously discussed in Information Systems Security Controls section b) Updates and Patches on page 5, four laptops were missing 10 or more security updates, one laptop was operational for more than a year prior to installing McAfee antivirus, and a laptop's McAfee AutoUpdate has not been operational for a year and a half.

2. Recommendation 6.5
   Review and remove generically named user accounts where appropriate.

   Current Observation:
   As previously discussed in Identity Access Management section c) Uniquely Identifiable User Accounts on page 11, we found 21 generically named user accounts with Administrator privileges to information systems, including the patient medical records, images, and to the laptops used in the MHC vans.

3. Recommendation 7.1
   Review all firewall rule sets to ensure firewall rules are appropriate.

   Current Observation:
   As previously discussed in section b) Data Flow Traffic on page 8, our zero hit count testing showed that 98% of the MHC Firewall connections have not been used to transmit data in the last 12 months.

4. Recommendation 8.3
   Establish mitigating access controls, including the regular review of audit logs to ensure the appropriate use of data by multi-cross functional and those identified with specific skills sets.

   Current Observation:
   As previously discussed in section b) Log Monitoring on page 11, we were informed that audit logs have not been reviewed since the termination of the HWCOM Compliance Officer in July 2015.

5. Recommendation 9.2
   Periodically perform tests on the EMR and take corrective actions as necessary.

   Current Observation:
   As previously discussed in section b) Testing on page 13, the MHC has not reviewed the EMR vendor's SOC-2 Report as part of the Disaster Recovery Process to ensure that the vendor does subscribe to their hosts backup services and that the MHC data is adequately protected.