FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of the HCN's Billing, Collections, and Electronic Medical Record Systems

Report No. 13/14-07

November 13, 2013

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: November 13, 2013

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

Fernando Valverde, Chief Executive Officer, FIU HealthCare Network

From: Allen Vann, Audit Director

Subject: **Audit of the HCN's Billing, Collections and Electronic Medical Record Systems, Report No. 13/14-07**

Pursuant to our annual audit plan, we have completed an audit of the FIU Academic Health Center HealthCare Network Faculty Group Practice, Inc. (the "HCN")'s Billing, Collections, and Electronic Medical Record Systems. The primary objective of our audit was to determine if the HCN's established controls and procedures are adequate to ensure that: 1) medical services are accurately and timely billed, collected, and recorded; 2) electronic health records' sensitive data has proper information security measures for confidentiality, integrity and availability; and 3) HCN's policies and procedures, applicable laws, rules and regulations are complied with.

Overall, our audit disclosed that the HCN's controls and procedures related to billing and collections were mostly adequate. Nevertheless, there were areas where internal controls need strengthening, particularly in patient records keeping and patient accounts review. Also, Information Technology security controls related to electronic health record systems, network and access can be improved. The audit resulted in 30 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: Sukrit Agrawal, Chair, BOT Finance and Audit Committee and Committee Member
Board of Directors, FIU HealthCare Network
Mark B. Rosenberg, University President
Douglas Wartzok, Provost and Executive Vice President
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Yolangel Hernandez Suarez, Chief Medical Officer, FIU HealthCare Network
Mauricio Sirvent, Chief Financial Officer, FIU HealthCare Network
Javier I. Marques, Chief of Staff, Office of the President

TABLE OF CONTENTS

OBJECTIVES, SCOPE AND METHODOLOGY

Pursuant to our approved annual plan, we have completed an audit of The Florida International University Academic Health Center HealthCare Network Faculty Group Practice, Inc. (the "HCN")'s Billing, Collections, and Electronic Medical Record Systems. The primary objective of our audit was to determine if the HCN's established controls and procedures are adequate to ensure that:

- Medical services are accurately and timely billed, collected, and recorded;
- Electronic health records' sensitive data has proper information security measures for confidentiality, integrity and availability; and
- HCN's policies and procedures, applicable laws, rules and regulations are complied with.

Our audit included review of revenue transactions from January 1, 2013 through April 30, 2013. The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing,* and included tests of the accounting records and such other auditing procedures as we considered necessary under the circumstances. For Information Technology (IT) control objectives, we applied a governance, risk and compliance framework, which utilizes the *Control Objectives for Information and related Technology (COBIT) 5.0 Framework and the National Institute of Standards and Technology (NIST) Special Publications 800-53A Revision 1 Guide for Assessing the Security Controls in Federal Information Systems and Organizations*.

During the audit, we reviewed FIU's and HCN's policies and procedures, applicable Florida statutes and federal laws, observed current practices and processing techniques, interviewed responsible personnel, and tested selected transactions. Sample sizes and transactions selected for testing were determined on a judgmental basis. Audit fieldwork was conducted from April to September 2013.

As this was the first internal audit of the HCN, there were no prior internal audit recommendations related to the scope and objectives of this audit requiring follow-up. Similarly, there were no other external audit reports issued during the last three years with any applicable prior recommendations related to the scope and objectives of this audit. The accounting firm Marcum Rachlin performs an annual audit of the financial statements of HCN. For each year audited, the accounting firm issued an unqualified opinion and did not identify any deficiencies in internal controls as it relates to financial reporting.

BACKGROUND

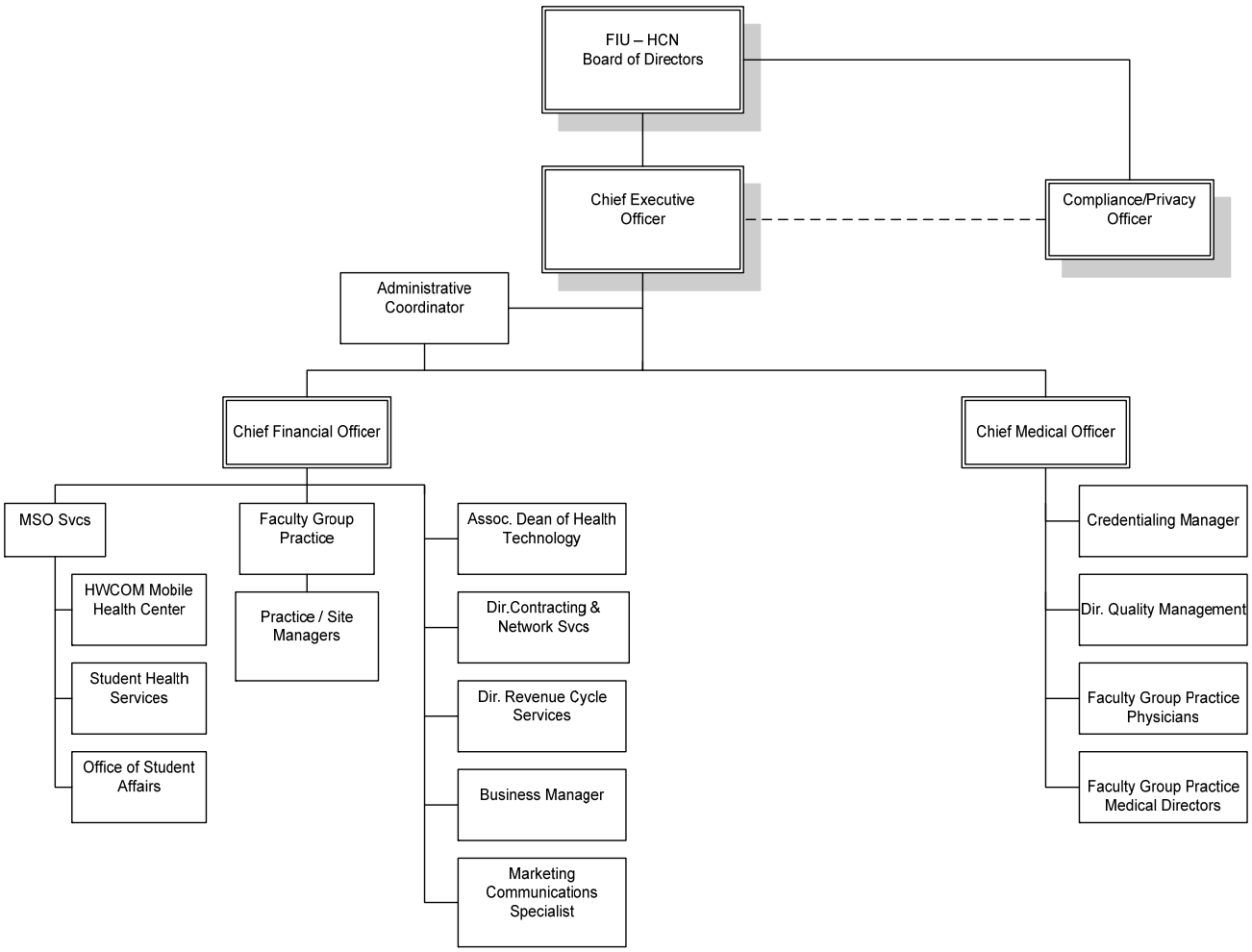
On August 8, 2011, the FIU Herbert Wertheim College of Medicine (HWCOM) opened the first medical facility and Faculty Group Practice in PG5 at the Modesto Maidique campus. Physicians from the HWCOM are able to provide patients with primary care, preventive care and specialty care services. The HCN was established to provide support to the HWCOM as well as other FIU academic health centers including the College of Nursing and Health Sciences, the Robert Stempel College of Public Health and Social Work and the Department of Psychology within the College of Arts and Sciences.

The HCN facilitates the clinical practice of medicine and performs various administrative functions including billing and collections, contract management with vendors and insurance plans, provider credentialing and administration of practice operations.

In late 2012, the HCN transitioned to the use of Electronic Health Records and implemented a new Electronic Medical Record system (EMR). In addition, a second Faculty Group Practice was opened at the Broward Health Medical Center in Fort Lauderdale, Florida.

Personnel

The following organization chart depicts the HCN's structure and employees as of September 2013.



Financial Information

During the fiscal year 2013, the HCN's operating revenues totaled $1.3 million and operating expenses totaled $3.2 million. The operating revenues amount was comprised of primary care and specialty care physician services (approximately $810,000), as well as other operating revenues generated by the HCN relating to non-clinical practice services (approximately $510,000). The following summarizes the HCN's financial activity for fiscal years 2011 through 2013.[1]

Condensed Statement of Revenues, Expenses, and Changes in Net Assets
(In Thousands)

	2013	2012	2011
Operating Revenues	$ 1,329	$ 322	$ 20
Operating Expenses	3,152	2,164	260
Operating Income (Loss)	(1,823)	(1,842)	(240)
Nonoperating Expenses	(78)	(29)	(2)
Nonoperating Income	1,483	--	--
Change in Net Assets	(418)	(1,871)	(242)
Net Assets - Beginning of Year	(2,097)	(226)	16
Net Assets - End of Year	$ (2,515)	$ (2,097)	$ (226)

[1] Source: The HCN's Audited Financial Statements for the Year Ended June 30, 2013

(page intentionally left blank)

FINDINGS AND RECOMMENDATIONS

Overall, our audit disclosed that the HCN's controls and procedures related to billing and collections were mostly adequate. Nevertheless, there were areas where internal controls need strengthening, particularly in patient records keeping and patient accounts review. Also, Information Technology security controls related to electronic health record systems, network and access can be improved. Our overall evaluation of internal controls is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		X	
Policy & Procedures Compliance		X	
Effect		X	
Information Risk		X	
External Risk		X	

INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls	**Effective**	**Opportunities exist to improve effectiveness**	**Do not exist or are not reliable**
Policy & Procedures Compliance	**Non-compliance issues are minor**	**Some instances of non-compliance Issues were evident**	**Non-compliance issues are pervasive, significant, or have severe consequences**
Effect	**Not likely to impact operations or program outcomes**	**Impact on outcomes contained**	**Negative impact on outcomes**
Information Risk	**Information systems are reliable**	**Data systems are mostly accurate but can be improved**	**Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions**
External Risk	**None or low**	**Moderate**	**High**

Details for Financial and Operational Controls area are summarized in Section I of this report. Our evaluation of IT Controls is further summarized and detailed in Section II of the report.

(page intentionally left blank)

SECTION I. FINANCIAL AND OPERATIONAL CONTROLS

1. New Patient Registration Forms

When a new patient comes to a Faculty Group Practice site, they are required to complete several registration forms and sign General Consent to Treatment before seeing a physician. These forms include Patient Demographic Information, Medical History, Notice of Privacy Practices, Notice of Social Security Number Collection and Use and Medical Records Request. In addition, the medical receptionist obtains a second form of identification and a copy of the insurance card from the patient. Prior to implementation of the EMR, these forms were kept in the patients' file. Now, they are scanned and maintained in the EMR for all new patients.

We reviewed 30 patient files and the associated medical records to ensure the forms were properly obtained and on file. Six out of 30 patient files reviewed had exceptions:

- One patient was seen after the implementation of the EMR, but did not complete the patient forms. Consequently her forms were not in the system.
- Two files were missing the provider's signature on the Medical History Form.
- One patient record was missing a copy of the patient's driver license or another form of ID, in addition to missing the provider's signature on the Medical History Form.
- Two patient files were missing a signed copy of the Notice of Collection of Patient Social Security Number form.

Signed forms acknowledge the patient's and/or provider's understanding or receipt of information. In addition, the practice of obtaining patient forms is a "best practice" to reduce the risk of denials and/or non-collection of patient accounts.

Recommendations

The HCN should:	
1.1	Ensure that all patient forms are completed.
1.2	Re-educate physicians and clinical support staff on the importance of obtaining and completing patient forms.

Management Response/Action Plan:

1.1 The policy regarding the patient Medical History Form (Form) will be amended to remove the requirement that the physician manually sign the Form. In the two cited instances within the Audit report, the services coded and subsequently billed met history of present illness requirements and were properly coded by the physicians and then billed.

Implementation date: January 2, 2014

1.2 Re-education of both physicians and clinical staff will be completed with revised policy.

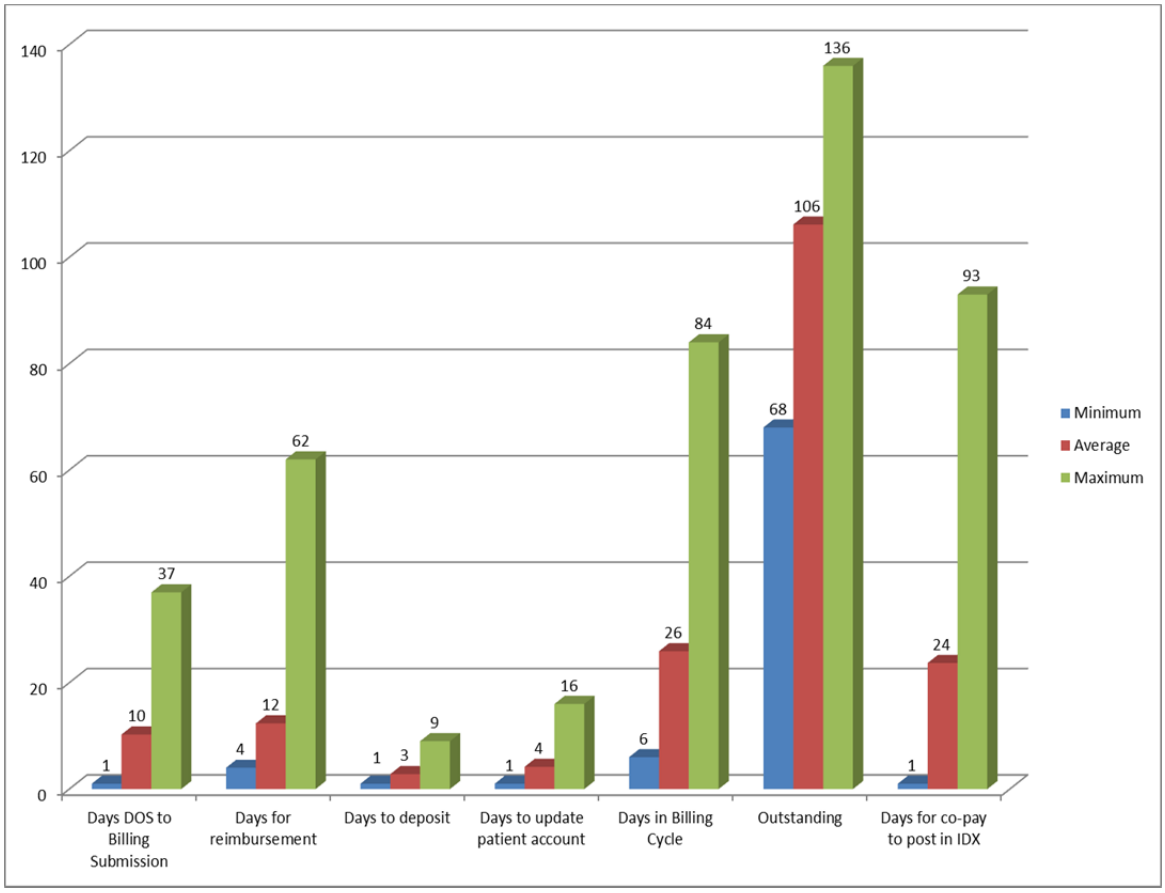
Implementation date: February 3, 2014

2. Billing and Collections

The HCN has a contract with Origins Healthcare Solutions ("Origins"), formerly known as Partners in Practice, to provide the billing and collection services for the practice. These services include direct patient billing and collection, insurance billing and collection, internal delinquency follow-up and collections, and Medicare and Medicaid billing and collection to and on behalf of the medical providers.

The HCN handles the administration of patient accounts for all payments received at each of the practices. In addition, the HCN's Director of Revenue Cycle Services has the responsibility to review claims for the purpose of assessing the accuracy of coding prior to releasing claims into the billing system (IDX) for Origins to submit.

During the audit period of January through April 2013 the HCN had $458,511 in charges and net receipts of $215,564[2]. We selected 30 patient accounts to test. The following chart provides an overview of the Revenue Cycle process for the accounts tested.



[2] Source: FIU April 2013 Financial Report prepared by Origins Healthcare Solutions

Our findings in this area are discussed below.

a) Revenue Cycle

As the HCN has to fulfill certain responsibilities prior to submitting claims to Origins, the revenue cycle process should be timely managed. Currently no policies exist to define acceptable periods to review claims or to update patient accounts, which led to untimely submission of charges and untimely updating of patient accounts.

Three out of 30 patients tested were “self-pay” that paid at the time of service. It took 37 days for two of the three accounts to reflect the payments made and the other account was showing as outstanding, when in fact the payment was received on the day of service.

The HCN utilizes two different systems. Time of service payments (i.e. copays) are initially entered into CPS10 (the EMR system) and then manually distributed and applied to the patient’s account in the IDX (the billing system). However, the Medical Receptionist has to wait until the charges are reviewed and submitted by the Director of Revenue Cycle Services before the patient can be identified and the payment can be applied in the billing system. As a result, these charges are often left in a “hold file” and the Medical Receptionist has to constantly check the system to see if the charges have been submitted.

Defined and appropriate review periods can reduce the time it takes to update patient accounts and ultimately reduce days of accounts outstanding.

b) Review and Follow-up

Per the contract agreement with Origins, the HCN is responsible for working several task manager queues for management of accounts receivable. In addition, per HCN Policy 5.10, once an overpayment paid by a patient is identified and confirmed, the Director of Revenue Cycle Services will initiate a refund request. The refund will be sent to the patient within 20 business days and the patient account will be noted of the impending reimbursement.

Out of the 30 accounts reviewed, we noted the following:

- Six accounts had been outstanding ranging from 68-136 days,
- One account had a credit or refund owed to the patient, and
- One account did not reflect the patient’s co-payment received on the date-of-service.

Timely review and follow-up are essential to avoid potential loss of revenue or patient dissatisfaction.

c) Billed Charges

To ensure that all patient visits and services are documented and all charges billed, HCN Policy 5.21, *Internal Controls,* states that daily audits are conducted that compare patients who arrived for their appointments against billed charges.

In fact, no such audits are being performed. Providers are responsible for updating the patient's medical record and coding the service after the patient is seen. A service form in the EMR system is utilized to code the charge, which initiates the billing of a charge. We found one instance in which the Provider did not code the charge in the system; therefore, the charge had not been submitted to Origins for reimbursement.

Per discussion with the HCN Chief Financial Officer, there is a bucket list in the system that notifies the physician of pending items to be completed. However, our testing revealed a weakness in this process as this list was not timely reviewed by the physician. The date of service for the claim was April 10, 2013 and our testing was performed on August 1, 2013.

Having an effective process in place to ensure that all patients seen are billed is essential to prevent the potential loss of revenue.

d) Payer Contract Compliance

Per HCN Policy 5.17, "payments received from Payers with which FIU has a contract to provide clinical services to insured's will be reviewed utilizing the billing and collections vendor's denial management/contract compliance software to ensure correct payment has been received." Payments determined to be "out of compliance" will be addressed between the billing and collection vendor, Director of Revenue Cycle Services, Director of Network Services and the Payer's provider representative.

During the audit period, we observed that no review was being performed by the HCN to compare contract rates with reimbursed amounts. We were informed that this process is performed by Origins. Two out of 30 claims reviewed appeared to be reimbursed at a lower rate than the contracted amount by approximately $35. Upon audit inquiry, the Director of Revenue Cycle Services followed-up with the payers accordingly. One of the two claims was noted as being reduced as a multiple procedure discount, per the Florida Blue Policy and was correctly reimbursed. The other claim was underpaid, although by a small balance amount. The HCN was not aware of Origins small balance threshold and had not received any exception reports or notifications of payments being out of compliance with contract terms.

Nevertheless, a review of contract rates and reimbursed amounts should also be performed by the HCN to ensure contractual obligations are met and to avoid potential loss of revenue.

e) Deposits

Patient payments received at the HCN should be collected and deposited in a timely manner. The HCN's policies and procedures do not specify an acceptable amount of time for cash and checks to be deposited.

We tested five days of collections at both the MMC and Broward locations. On average, it took 3 days to deposit cash and checks at the MMC locations and 4.5 days at the Broward location.[3] Currently, the Director of Revenue Cycle Services goes to the Broward location to collect payments so the deposits can be made, but there is no formal schedule of collection, which led to the longer number of days to deposit the revenues collected in Broward.

During the audit, we noted that the HCN obtained a scanner at the MMC location that will allow checks to be scanned and instantly deposited into the HCN's account. This new process was implemented in May and will significantly decrease the amount of time to deposit checks. A scanner is also planned to be implemented for use at the Broward location.

Recommendations

The HCN should:	
2.1	Determine and document acceptable periods to review and submit charges and post patient payments.
2.2	Ensure that work queues are timely reviewed and patient accounts with outstanding Accounts Receivable and credit balances are properly followed up.
2.3	Improve current processes to ensure timely billing of all seen patients.
2.4	At a minimum, perform quarterly reviews to ensure that Origins is meeting their requirements to compare contracted rates to reimbursed rates.
2.5	Contact Origins to determine the small balance threshold and if it is acceptable for the HCN.
2.6	Update policies and procedures to include a cash control policy.

[3] Note: Although the HCN is not required to follow FIU policy, FIU policy requires collections to be deposited within two days.

2.7	Define a formal deposit schedule for payments received at the Broward practice, until such time that a check scanner for depositing checks is implemented.

Management Response/Action Plan:

2.1-2.2 For submission of charges and posting of payments, current policy will be revised and updated to the following:

- Charge submission – goal of 2 business days; 100% no later than 7 business days.
- Patient payment posting – goal of 1 business day; 100% no later than 4 business days.

Policy will be updated and then staff will be appropriately trained.

Policies will be updated to meet the following:

1. Physician "bucket" to be reviewed by individual physician and all billing items to be completed within 7 business days.
2. A/R reports to be reviewed monthly.
3. Credit balance reports to be reviewed monthly.

Implementation date: January 2, 2014

2.3 Same policy and procedure implementation as described in response to recommendations 2.1 and 2.2 above.

Implementation date: February 3, 2014

2.4 Although we will be reviewing the accounts receivable reports, we will request evidence from Origins ensuring that this function is being performed. We will also institute a quarterly random sample of 25 claims to ensure that appropriate payment is being received.

Implementation date: March 21, 2014

2.5 Small balance threshold will be documented within our revised policy.

Implementation date: January 2, 2014

2.6 All financial policies will be undergoing review and updating.

Implementation date: March 28, 2014

2.7 Check scanner is currently in place at the HCN office and handles FGP MMC and Broward. Check scanners will be deployed at both MMC and Broward practice sites. Additionally, with this process change, we will establish a formal policy on deposits.

Implementation date: January 2, 2014

3. Policies and Procedures

With the HCN still being a fairly new operation, as well as with the recent implementation of the EMR and the addition of the Broward practice, adequate policies and procedures are important for day-to-day operations.

We noted that policy numbers 5.19, 5.22, and 5.25 pertaining to HCN's Financial Management do not reflect current operations. In addition, Policy 5.11 – "Charge Capture Validation" had not been completed, which is a key process in ensuring that charges are captured, accurate and timely submitted for billing.

Outdated policies and procedures affect an employee's ability to understand their roles and responsibilities.

Recommendation

The HCN should:	
3.1	Review and update all financial management policies and procedures, including policy numbers 5.11, 5.19, 5.22, and 5.25.

Management Response/Action Plan:

3.1 All financial policies will be undergoing review and updating.

Implementation date: March 28, 2014

4. Reporting Tools

Effective reporting tools are required to provide management with quick, reliable and accurate information.

The HCN-MMC Practice Manager stated that there is no report that will quickly provide information on patient visits. Therefore, it is a very manual and timely process to obtain the number of patients that visited the practice during any given period. The Practice Manager counts patients on a weekly basis and provides the information to the HCN CFO; however, documentation is not maintained to support the count.

Due to the lack of supporting documentation, we were unable to determine the accuracy of visits for Q3 of FY 12-13. There were approximately 2,500 patients scheduled and/or seen according to a report provided to us compared to total patient visits of 1,898 reported in the April 2013 Management Report to the HCN's Board of Directors for the MMC location. We were informed that the total patient visits data include lab tests, radiologic exams, flu vaccines, etc., which are not reported in physician/patient encounter information.

The lack of supporting documentation increases the risk of inaccurate information being reported.

Recommendation

The HCN should:	
4.1	Develop automated reporting tools that are fully supportable.

Management Response/Action Plan:

4.1 IT Clinical Informatics Analyst is currently reviewing all standard report availability from GE Centricity and Origins. She will be working with Associate Dean for HIT and HCN CFO and Revenue Cycle Director on standard portfolio of monthly reports, which will include ad-hoc reporting as needed.

Implementation date: April 10, 2014

5. Compliance

Adequate policies and procedures exist to delineate a process to monitor billable health care items and services provided to Faculty Group Practice patients and to ensure compliance with Compliance Standards relating to billing for health care items and services provided to Faculty Group Practice patients.

Employee compliance, education, and billing compliance monitoring activities are performed collaboratively by the HCN's Practice Manager, Director of Quality Management, Director of Revenue Cycle Services and Compliance Officer. During the audit, we observed the following:

a) Education and Training

AHC/HCN Policy 7.08 *Employee Compliance Training and Education for all Staff and Providers* requires individual on-boarding education regarding coding and billing requirements be completed by the HCN Director of Revenue Cycle Services. Additionally, according to AHC/HCN Policy 7.08, education and training covering compliance standards is mandatory for all clinical faculty members, other FIU employees, and independent contractors providing clinical or administrative services on behalf of, or supporting the Faculty Group Practice. The faculty member or employee is required to complete training before work in support of the Faculty Group Practice can be resumed.

The Compliance Officer provided signed compliance training sheets to evidence that 14 of the 15 billing providers tested received training, and corroborating evidence that the 1 provider participated in training, absent a signed sheet that was reportedly misfiled. Training is provided to ensure the provider's knowledge and understanding of their role in FIU's clinical enterprise compliance standards. Collection of sign-in sheets helps to corroborate the training was conducted.

We were informed that the Compliance Officer will obtain new documentation from the provider. In addition, we acknowledge that the on-line Faculty and Staff Learning Environment was implemented during our audit, which will help the Compliance Officer better manage the professional training process.

b) Auditing and Monitoring

AHC/HCN Policy 7.07 Routine Billing Compliance Monitoring requires a random sampling of a statistically reliable number of medical records (if less than all records) by the HCN Director of Revenue Cycle Services for coding review. Additionally, according to AHC/HCN Policy 7.11, the Compliance Officer is responsible for monitoring and reviewing the coding and documentation practices of providers within the Faculty Group Practice, billing on behalf of FIU and Providers employed by FIU. A minimum of twenty services, representing at least ten patients will be reviewed for each new provider annually.

Coding reviews for FY 2013 had not been completed by the Compliance Officer. We were informed that approximately 65-75% of the reviews were completed, but had not been 100% completed for any provider, which was a result of time constraints, i.e., the Compliance Officer was heavily involved in the implementation of the EMR and the development of an online HIPAA/Privacy training module.

The goal of the coding review process is to reduce payer refunds, identify areas of inaccurate coding and to proactively provide education. Without proper monitoring, there is a risk of improper billing, missed submission of charges, and/or denial of claims due to untimely billing.

Recommendations

The HCN's Compliance Officer should:	
5.1	Ensure that the appropriate documentation and evidence of compliance training is properly maintained.
5.2	Complete coding reviews that should have been performed for FY 2013.
5.3	Establish a process that will ensure future reviews are completed in a timely manner.

Management Response/Action Plan:

5.1 The Compliance Office will continue to use manual methods of documentation of 1:1 training sessions and endeavors to strengthen its filing systems. The one missing sign in sheet cannot be located; the provider has terminated his services to FGP patients, effective September 2013.

Implementation date: Completed with on-going maintenance for future training.

5.2 The AHC, FIU HCN Compliance Annual Report has been finalized and will be delivered to the HCN Board on October 29, 2013, and the AHC Compliance Committee on November 13, 2013.

Implementation date: Completed

5.3 a) The Compliance Office is conducting concurrent auditing of completed coding in accordance with policy and procedure; a process made possible with the adoption and experience of use of the electronic medical record system.

Implementation date: Completed

b) The Compliance Office has also requested the addition of personnel, specifically, a coding educator and auditor to undertake education and auditing of claims. As the clinical enterprise grows and medical services complexity increases, additional resources are required

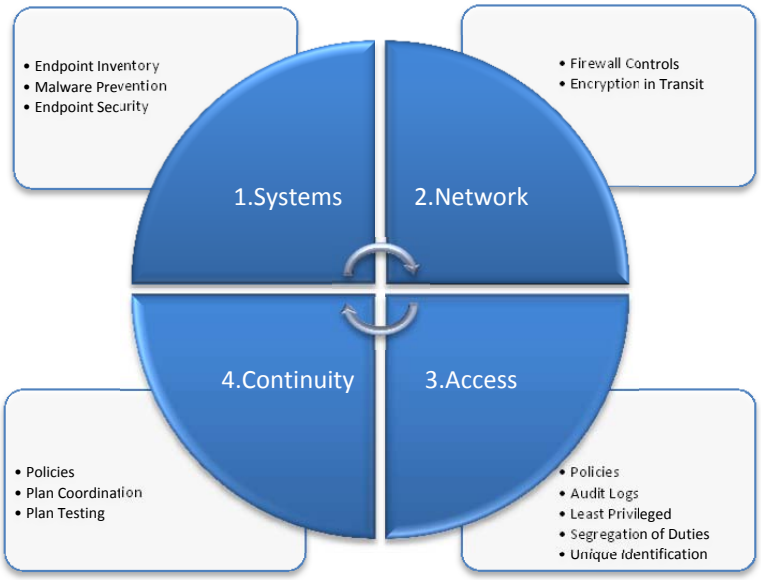
Implementation date: January 31, 2014

SECTION II. INFORMATION TECHNOLOGY CONTROLS

Our review of the Information Technology (IT) controls is divided into four sections:

1) Systems Security;
2) Network Security;
3) Access Controls; and
4) Business Continuity.

To achieve our IT audit objectives, we applied a Governance, Risk and Compliance framework which utilizes the following universally recognized methodologies and guidelines:



- The Control Objectives for Information and related Technology (COBIT) 5.0 Framework; and

- The National Institute of Standards and Technology (NIST) Special Publication 800-53A Revision 1 Guide for Assessing the Security Controls in Federal Information Systems and Organizations.

We also applied applicable FIU and HCN policies and procedures. Details of our findings and recommendations follow:

6. Systems Security

Systems Security includes malware prevention, endpoint security, and information surplus security. Preventive, detective and corrective measures should be implemented and maintained (especially up-to-date security patches and virus controls) on endpoint devices such as laptops and desktops which connect to the electronic medical records data to protect them from malware, brute force attacks, and unauthorized access. Endpoint devices, including servers that store sensitive data are typically encrypted; vulnerability assessments should be performed periodically to ensure the effectiveness of existing information systems security controls; and surplus systems should be properly disposed. Processes relating to systems security were generally achieving their intended purpose. Our observations follow:

a) Endpoint Inventory

As required by FIU Policy No. 1670.030, *Inventory and Software Containing Electronic Protected Health Information*, the HCN adequately maintains an endpoint inventory list for the 30 PG-5, 7 Broward, and 7 Mobile Van endpoint devices. The inventory lists contain the user name, IP or MAC address, host name, serial number and the location.

According to the Associate Dean of Health Information Technology, the inventory lists are updated on a real-time basis by the Manager of Educational and Clinical Technology and the IT Security Officer/Engineer. No exceptions were noted in this area.

b) Malicious Code Protection

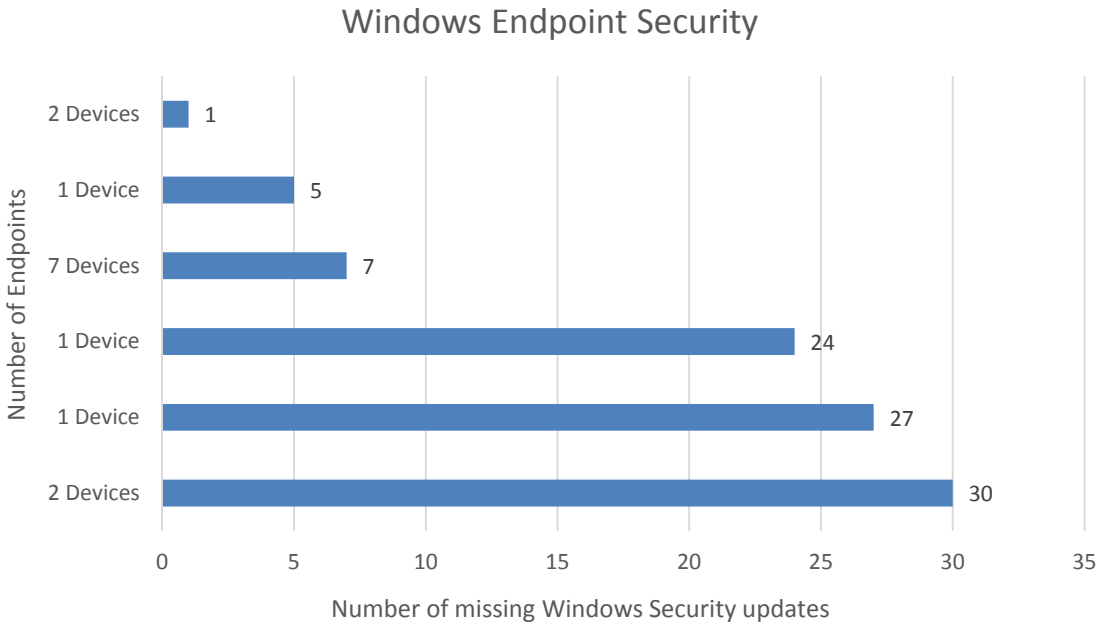
Endpoint devices[4] may be exploited by malicious code through the use of electronic mail attachments, web access, removable media, or other common means. To detect and eradicate these types of endpoint vulnerabilities, the HCN applies a layered security approach utilizing the McAfee On-Access Scanner (OAS) module and Microsoft Malicious Software Removal Tool. McAfee's OAS service scans files prior to the user opening them to ensure they are not infected. The Microsoft Malicious Software Removal Tool is an anti-malware utility that checks computers for infections and helps remove malware and any other infections found. Whereas an antivirus program blocks malicious software from running on a computer, the Microsoft Malicious Software Removal Tool removes malicious software from a workstation already infected. For malicious code prevention mechanisms to remain effective, signature definition files should be automatically updated on a daily or as needed basis.

Our test of 45 endpoint devices (workstations) at PG5, Broward and the Mobile Van disclosed the following:

- 44 were actively running OAS; but 1 device at the PG5 used for registration and insurance authorizations had OAS disabled.
- 14 devices' OAS at PG5 were not updated timely. They included 5 staff, 4 doctors, medication room, front desk, practice manager, administrative station, and registration.
- 2 devices' OAS at Broward, which were used by one of the doctors and an office loaner laptop, were not updated in a timely manner.
- 16 devices did not have their malicious code prevention mechanisms adequately updated. On average, the antivirus signature file updates were 71 days behind on these 16 endpoint devices.

[4] Endpoint devices include laptop and desktop workstations.

We also observed that 14 endpoint devices were missing between 1 and 30 Windows security updates in total as illustrated in the table below.



Missing security updates reduces the effectiveness of antivirus mechanisms in a layered security approach.

In addition to managing the antivirus mechanisms, the University's UTS Network Security Systems Engineering department (NSSE) manages the HCN information systems endpoint devices' host intrusion and hard drive encryption services. An ePO agent needs to be installed on each endpoint device in order to communicate with the NSSE antivirus servers. Once properly connected the ePO agent will automatically install all antivirus, HIPS, and encryption mechanisms. However, there were 5 endpoint devices that did not have an installed ePO agent.

In the event a virus is discovered, HCN information systems are adequately configured to first clean files automatically and then delete if the file cannot be cleaned. All information systems tested automatically delete quarantined files after 28 or 45 days respectively. Also, we determined that 44 endpoint devices were adequately configured to prevent non-privileged users from circumventing malicious code protection mechanisms. But one device was incorrectly configured to allow non-privileged users with the ability to change antivirus properties.

c) Endpoint Security

Administrator user accounts have an inherited risk due to their associated elevated access privileges. By assigning unique identities to administrator user accounts individual users are properly identified and their activities can be tracked. During the audit we noted that a total of 9 generically named administrator user accounts were identified. Upon our inquiry, 4 were promptly deleted by HCN IT Security. Of the 5 remaining generic administrator user accounts, 1 is an application account necessary for the program to work; 1 is used internally; and 3 were created by the hardware vendor to update the system drivers. The use of generically named user accounts increases the risk of unauthorized access.

To minimize the risk of unauthorized access to endpoint devices, the HCN properly set up its endpoint devices, which require users to change their passwords every 180 days and will automatically lock out a user after 5 invalid login attempts over a 15 minute period. The user will remain locked out for 15 minutes until it is automatically reset.

The University's UTS Network Security Engineering department (NSSE) provides hard drive encryption to its managed systems, including HCN. Three of the 45 devices tested did not have the hard drive encrypted including one laptop from the Broward location which is used off-site. The non-encrypted hard drives increase the risk of unauthorized access.

Recommendations

The HCN should:	
6.1	Monitor endpoints OAS module to ensure it is operating at full strength.
6.2	Ensure that virus definition files and operating system security updates are updated in a timely manner.
6.3	Implement the identified devices onto the ePO and ensure all related security services including hard drive encryption are properly functioning.
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.

Management Response/Action Plan:

6.1 The HWCOM Security Engineer has been monitoring end points on a periodic basis.

Implementation date: Completed

6.2 The HWCOM Security Engineer has been monitoring virus definition files via McAfee and Nexpose reports. In addition, operating system updates are monitored by reviewing Nexpose reports.

Implementation date: Completed

6.3 The HWCOM Security Engineer will have current policy revised and updated to the following:

Coordinate with UTS to ensure that applicable devices are synced, updated and reviewed with related security services at a minimum of 90 days.

The HWCOM Security Engineer will work with NSSE to address the five identified devices for EPO.

Implementation date: February 10, 2014

6.4 This policy is in place. HWCOM Security Engineer will coordinate with UTS to ensure that only privileged users have access to configuring anti-virus settings.

Antivirus configuration settings are managed centrally through FIU DoIT NSSE group. By default, the workstation antivirus program is locked down so that configurations cannot be changed by non-privileged users. The HWCOM Security Engineer will work with NSSE to address the identified workstation to ensure it cannot be modified by non- privileged users.

Implementation date: January 2, 2014

6.5 Policy is in place. IT Director or designee is responsible for reviewing all generically named user accounts to ensure that they are only utilized as deemed necessary.

Implementation date: Completed

7. Network Security

Network security includes defining and protecting internal and external boundaries, limiting access points to the boundaries through the use of firewalls and intrusion protection systems. Firewall rules should be configured by default to "deny all" and access through the firewalls should be approved with supporting documentation. Sensitive data should be encrypted in transit and when transported outside of controlled areas.

a) Firewall Controls

According to NIST sp800-53A Rev.1 SC-7(3).1, the HCN should limit the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. The Associate Dean of Health Information Technology provided network diagrams for the EMR (Figure 1), financial, x-ray, ultrasound, PACS and fax server systems (Figure 2). The diagrams define the key internal and external boundaries and the security controls in place to protect the EMR information systems data.

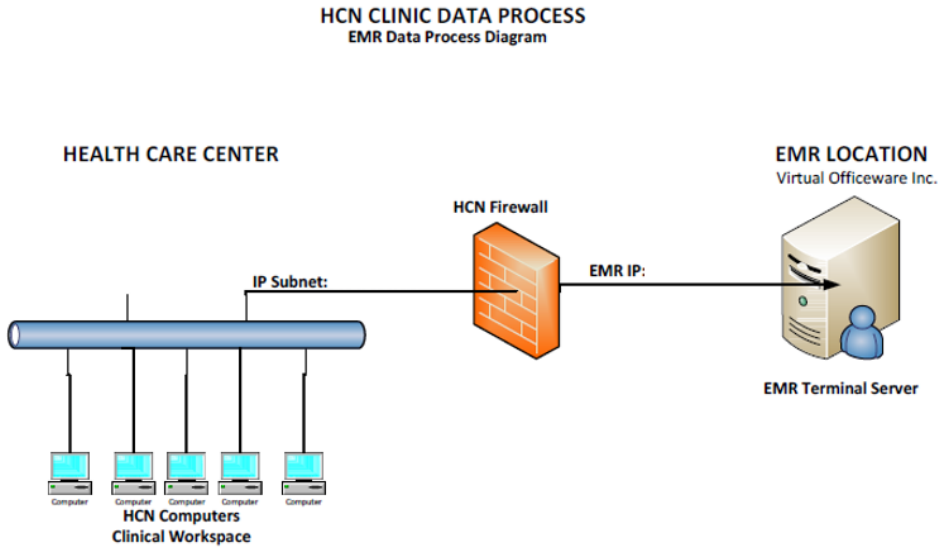


Figure 1

Our examination of HCN network diagrams and UTS' NSSE FW rules determined that greater amounts of private IPs were allocated than the HCN required. Segmented blocks of IPs by NSSE include 2 extra segments totaling 512 IPs to the EMR system; 3 extra segments totaling 768 IPs to the Billing system; 4 extra segments totaling 1024 IPs along with 3 additional static IPs to the PACS servers; and 3 additional segments totaling 768 IPs. UTS' NSSE is responsible for maintaining the network and the HCN is accountable to the appropriateness of the network connections. Although network controls through the use of private network segmentation were implemented, it did not effectively limit the number of access points to the EMR system. Limiting the network connection increases the effectiveness of monitoring efforts.

In addition, information systems inbound and outbound communications should be monitored for unusual or unauthorized activities or conditions. The firewall configurations from the HCN to the hosted applications are set to deny all. However, we noted that the Broward office's wireless router MAC address filtering option was disabled and was also set to allow up to 20 guest accounts onto the network. Also, the wireless router was not properly configured to deny all network traffic by default. The non-hardened router configuration settings decrease the effectiveness of information system network security.

A good network boundary protection practice should have firewall rules configured to deny all traffic and for each exception to the network traffic flow to include documentation with supporting mission/business need, review of traffic flow exceptions, and the removal of exceptions that are no longer supported by the mission/business need. Appropriate network access requests should include specific endpoint IPs, ports or duration. However, we noted that the former Director of Health IT emailed UTS' NSSE for network access requests to the EMR and Billing information systems, but the emails did not include sufficient information. The email for access to the EMR only contained the vendor IP and the email for access to the billing system only had names of the former Director of Health IT and the Director of Revenue. The HCN was also unable to provide network request emails for the X-Ray machine, Ultrasound, AHC II PAC server, Remote office PAC server, HCN Fax server, Microsoft exchange server and Broward location.

We also determined that a review of network traffic flow was not performed by the HCN and therefore it may: (1) not remove network connections that are no longer supported by their mission/business need; and (2) not be aware of the open ports for all of the IP ranges listed above.

b) Encryption in Transit

The EMR and Billing data is transmitted on secure ports to protect the confidentiality and integrity of sensitive information. Due to a misconfigured firewall, the remote office's PAC imaging data was transmitting in an unsecure manner. Upon our inquiry, the NSSE promptly removed 6 IPs connected to the remote office and moved the digital imaging port to a VPN tunnel.

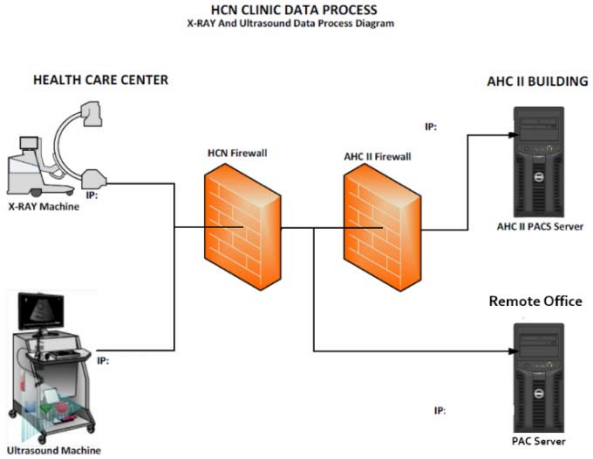


Figure *2*

There are 13 users including 7 HCN management, 5 COM IT Support staff members and 1 HCN staff member who were appropriately assigned to use VPN when accessing data from remote locations. The HCN staff member was given VPN access when she was a site manager during the opening of the Broward Health Services. In November 2012, a permanent site manager was hired and the previous manager was reassigned

as a coordinator of psychiatry where the VPN access was no longer necessary. Upon our inquiry, the coordinator of psychiatry's VPN access was promptly removed. The lack of periodic reviews of VPN user access increases the risk of unauthorized access.

Recommendations

The HCN should:	
7.1	Review all firewall rule sets to ensure firewall rules are appropriate.
7.2	Sufficiently document the firewall requests to ensure firewall rules are only allowed based on its mission/business need.
7.3	Ensure Broward wireless router settings are securely configured and deny all network traffic by default.
7.4	Periodically perform a formal review of their VPN user access list to ensure access is appropriate.

Management Response/Action Plan:

7.1 FIU Division of IT Networking Services (NSSE) is responsible for and manages all firewalls for FIU. HWCOM IT will continue to work with FIU's Division of IT to ensure firewall rules are appropriate.

Implementation date: February 10, 2014

7.2 FIU NSSE is responsible for all firewalls for FIU. However, this will be a joint effort involving HWCOM IT, but will continue to be managed by FIU NSSE. Policies and procedures will be formalized.

Implementation date: February 10, 2014

7.3 The Broward wireless router was securely configured.

Implementation date: Completed

7.4 HWCOM Security Engineer will be formally reviewing user access related to the VPN listing to ensure appropriateness.

Implementation date: March 28, 2014

8. Access Controls

Access controls reviewed include policies, audit logs, least privileged access, segregation of duties, and unique identification. User identity and logical access need to be managed to ensure that all users have information access rights in accordance with their business requirements. User roles, responsibilities and segregation of duties need to support the business process objectives.

a) Access Control Policies

Per the guidance of NIST sp800-53A Rev.1 AC-(i)(ii), an access control policy should be developed and formally documented. Accordingly, the HCN adequately developed and documented its access control policy (HCN 8.04) to maintain an adequate level of security to protect data and information systems from unauthorized access and non-mission critical access. This policy requires a confidential agreement to be signed by users who request access to HCN information systems and/or PHI. Also, an Access Request Form needs to be used.

During the initial EMR implementation, the onboarding access procedures did not follow Policy HCN 8.04 dated October 19, 2011, which require that "System access will not be granted to any user without appropriate approval. System access must be requested by the end-users and must be approved by the users supervisor and Chief Operating Officer or designee of the FIU HCN." Instead 42 users' access levels were informally authorized during an October and November 2012 training sessions. Starting in March of 2013, a formal EMR onboarding process was implemented based on the HCN 8.04 Policy. Supervisors submit User Access Request Forms to the EMR data custodian for approval and users also sign a Confidentiality Agreement Form prior to the creation of their user account.

Of the total 55 EMR individual user accounts tested:

- 35 users obtained their user access during the Go-Live training (EMR system) onboarding sessions. Only 1 user had an Access Request Form completed.
- 6 users had a completed Access Request Form, but did not attend the training sessions.
- 14 users neither attended the training sessions nor had an Access Request Form.
- Also, 5 of the 7 user Access Request Forms did not fully match their access levels in the EMR application.

The HCN was also unable to provide a Confidentiality Agreement Form for 49 of the 55 EMR users. Of the 6 Forms provided, 3 users signed their form 101, 273, and 278 days after either their Go-Live training session or start date.

In addition to attending CPS10 (the EMR system) training, users are also required to attend ITSO Security Training. Of the total 55 EMR users, 51 attended the training. The

4 users who did not attend the training are a student, a lecturer, a programmer, and an Assistant Professor.

The EMR off-boarding procedure is handled by the HWCOM Information Technology department via email or phone. Five of six terminated users tested had a completed Separation of Employment Form. One terminated user was still active 108 days after her termination. The termination process was promptly activated upon our inquiry.

Inappropriate access, not having or timely signing confidentiality agreements, and the delay in deactivating terminated employees' account may increase the risk of inappropriate user access.

b) Audit Logs

Pursuant to HIPAA §164.312(b) the HCN created two SQL queries (User and patient) for the HCN Privacy Officer, which are based on the EMR audit logging data. The queries create audit log reports that contain the date and time, event description, patient name, user ID, and the workstation used to access sensitive data during a user's session. The audit log reports reviewed by the HCN Privacy Officer were based on the HCN's draft policy, which states that activity reviewed are performed in response to "trigger events". Trigger events include: (a) complaints by patients regarding suspicion of inappropriate access of their records; or as determined by the Privacy Officer; (b) VIP patient records such as community figures; and (c) high-profile events, including motor vehicle and or criminal cases. Based on the above listed trigger events, user audit logs were not regularly reviewed by the HCN Privacy Officer. HIPAA §164.308(a)(1)(ii)(D) requires that the HCN implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

c) Least Privileged

The COBIT 5 DSS06.03.03 control objective of least privileged user access is to only allow authorized users access that is necessary to accomplish assigned tasks in accordance with their business functions. The HCN created 14 roles and 26 specific privileges within the EMR. Within the assigned roles, there are 9 users access that do not appropriately align with their job titles. According to the HCN CFO, due to the new EMR implementation and limited resources available with specific skills set that: (a) roles were granted that included a doctor with IT support privileges, IT support staff with compliance access, and a programmer with billing and provider privileges to improve the application's capability, and (b) the remaining 7 positions identified have multi-cross functional responsibilities.

d) Segregation of Duties

The separation of duties of individual user accounts is necessary to prevent malevolent activity of electronically protected health information without collusion. There is a super user role in the EMR application that contains 7 of 9 users which include an Assistant Professor, IT Support specialist, and training accounts. Additionally, 4 of the 7 super user accounts have multiple access roles. According to the HCN Associate Dean, a project has been ongoing to re-evaluate and fine-tune EMR roles and permissions. The inappropriate user roles increase Segregation of Duties risks.

e) Unique Identification

According to the requirements of HIPPA Security Standards: Technical Standards 1. *Unique User Identification (R)* - §164.312(a)(2)(i) covered entities must "Assign a unique name and/or number for identifying and tracking user identity. In addition, FIU Policy No. 1670.005, *HIPPA Security: Access Controls to Systems Containing Electronic Protected Health Information* "each department or unit employee who requires access to electronic protected health information shall be assigned a unique name and/or number for identifying and tracking user identity." Of the 61 user accounts within the EMR application, there were 55 uniquely identifiable and 6 generic accounts. Two of the generic accounts contained super user access to the EMR application, which may bypass existing identity management controls and impact the confidentiality, integrity, and availability of EMR data.

Recommendations

The HCN should:	
8.1	Review all EMR user accounts and their related access privileges to ensure access is appropriate and formally documented; as well as complete the Confidentiality Agreement Form.
8.2	Formalize the HCN draft policy on review of user activity within clinical information systems to be in alignment with HIPAA §164.308(a)(1)(ii)(D).
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.
8.4	Review roles and privileges allocation to user accounts and distinguish which privileges not to combine to prevent a segregation of duties conflict.
8.5	In light of current policy, reassess the use of generic accounts given the inherent risks and compliance issues associated with continuing to maintain them.

Management Response/Action Plan:

8.1 Access procedures were finalized and implemented in March 2013. Confidentiality Agreements have been obtained for each.

HWCOM Security Engineer will work with the Clinical Informatics Analyst to ensure that access privileges to the EMR are appropriate and formally documented for all established users prior to March 2013.

Implementation date: January 20, 2014

8.2 A formalized policy on user activity within the clinical system will be implemented by the Director of HWCOM IT and the Security Engineer.

Implementation date: January 20, 2014

8.3 Audit logs: Audit logs, as required under Section 164.308(a)(1)(ii)(D) are determined by the covered entity, based on risk analysis of the system and PHI contained within the EMR.

The AHC Privacy Audit policy has been amended to include regular reviews of accesses made by authorized personnel.

Implementation date: February 20, 2014

8.4 A policy establishing mitigating controls will be implemented for instances when certain personnel will have combined duties. Additionally, audit tasks will be performed as noted in 8.3 above.

Implementation date: January 2, 2014

8.5 Policy is in place. IT Director or designee is responsible for reviewing all generically named user accounts to ensure that they are only utilized as deemed necessary.

Implementation date: Completed

9. Business Continuity

The purpose of Business Continuity is to establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operations of critical business processes at a level acceptable to the HCN. The EMR and Billing information systems are hosted applications[5] that are critical to the daily operations, which highlight the need for periodic review of internal and external disaster recovery plans to ensure the confidentiality, integrity and availability of the applications information systems data.

a) Policies and Procedures

NIST sp800-53A Rev.1 CP-1.1(i) requires a contingency plan be developed and formally documented. The EMR vendor has developed and formally documented a contingency plan, which effectively contains policies, procedures and software to support EMR business functions in the event of a declared disaster. According to the HCN CFO, the billing application vendor informed the HCN that a Service Organization Controls (SOC)[6] report was not required for their organization. Without a current SOC report of the hosted billing system, the HCN is unable to determine the adequacy of the vendor's billing system's contingency controls to ensure the confidentiality, integrity, and availability of the HCN's information systems data.

b) Plan Coordination

As a best practice, copies of the business continuity plan should be distributed to key personnel and organizational units. According to the EMR vendor's SSAE 16 report, the Disaster Recovery Coordinator with assistance from their technical advisors is responsible for the planning, coordinating and managing of the Business Continuity Plan. The vendor's report also states that their periodic review of the various sections of the plan and training of disaster response participants ensures the efficacy of the total plan and that the disaster response participants remain cognizant of their functions.

c) Plan Testing

COBIT DSS04.04 states that it is good practice to test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated. According to the EMR vendor's SSAE 16 report, the EMR hosted systems are tested from time to time when unplanned events occur that affect network

[5] A hosted application is software as a service (SaaS) solution that allows users to operate a software application entirely from the cloud.

[6] Service Organization Control (SOC) reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsource service.

connectivity. The vendor planned disaster recovery testing is scheduled to occur once a year when more failures can be simulated and validated at a time when operations are least impacted. Additionally, the SSAE 16 report states that backup site exercises are conducted by members of the Restoration Team, the Operations Team, and the Customer Support Team and that the debriefings are scheduled on the days immediately following the backup exercises.

During the billing and collections testing, we noted one patient account that was not billed due to the loss of data from a system error within the EMR system. Adequate testing of the contingency plan should prepare for this type of system failure. During our audit, it was not evident that HCN had an EMR contingency plan. Subsequently, the HCN produced an EMR contingency plan and coordination documents, which appear to be adequate.

Recommendations

The HCN should:	
9.1	Ensure contingency plans for its third party billing vendor are: developed and documented; and distributed to key personnel.
9.2	Periodically perform tests on the EMR and Billing systems and take corrective actions as necessary.

Management Response/Action Plan:

9.1 Contingency plans do exist for the clinical operations and default to downtime procedures of "paper" medical records and telephonic communication. As to 3rd Party billing, we will request the formal documentation of their contingency plan and distribute it to the key personnel.

Implementation date: March 14, 2014

9.2 We will obtain all supporting recovery plans from the Billing and EMR system vendors and then convene a conference of key personnel to ensure "virtual" simulation of down time and recovery procedures. This will be appropriately documented.

Implementation date: April 2, 2014