FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Follow-up Audit of the Florida International University Health Care Network's (HCN's) Billing, Collections, and Electronic Medical Record Systems
Report No. 18/19-04
January 14, 2019

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

MEMORANDUM

DATE: January 14, 2019

TO: Robert Sackstein, Dean, Herbert Wertheim College of Medicine and Senior Vice President of Health Affairs

Eneida O. Roldan, Chief Executive Officer of the FIU Health Care Network

FROM: Trevor L. Williams, Chief Audit Executive

SUBJECT: **Follow-up Audit of the Florida International University Health Care Network's (HCN's) Billing, Collections, and Electronic Medical Record Systems**

We have completed our follow-up audit of the HCN's Billing, Collections, and Electronic Medical Record Systems. The audit included a review of transactions for the period of July 1, 2016, through December 31, 2017, and an assessment of current practices through December 31, 2018. During the fiscal year 2016-17, the HCN's operating revenues totaled approximately $8.2 million and operating expenses totaled approximately $4.9 million. Operating revenues consisted of approximately $4.3 million in management fee revenue, $3.4 million in Office of International Affairs revenue, and $0.5 million in rental income and other revenue. The cost for managing and operating the HWCOM Clinics was $2.1 million, representing approximately 50% of the management fee revenue.

The objective of the audit was to review the HCN's implementation status of prior audit recommendations and determine whether they were effectively implemented. The prior audit recommendations addressed the following areas: 1) accurate and timely medical billing and collections; 2) protection of electronic medical records' sensitive data; and 3) compliance with the University and HCN's policies and procedures, and applicable laws, rules, and regulations. Our assessment revealed that 18 of the 30 prior recommendations were fully implemented, 11 were partially implemented, and one was not implemented.

Also, while testing management's implementation of the prior audit recommendations, we found that opportunities for improvement existed in other areas, specifically related to billing and coding, HIPAA and Security Awareness trainings, asset management, breach notification policies, facility access logs, and the business continuity plan. This resulted in six additional 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: FIU Board of Trustees
Mark B. Rosenberg, University President
Kenneth G. Furton, Provost and Chief Operating Officer
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Javier I. Marques, Chief of Staff, Office of the President

TABLE OF CONTENTS

OBJECTIVES, SCOPE, AND METHODOLOGY

Pursuant to the Office of Internal Audit approved annual audit plan for the fiscal year 2017-2018, we have completed a follow-up audit of the Florida International University Health Care Network's (HCN's) Billing, Collections, and Electronic Medical Record Systems, Report No. 13/14-07.

Our audit included a review of transactions for the period of July 1, 2016, through December 31, 2017, and an assessment of the College's current practices through December 2018. The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* and the *ISACA IS Audit and Assurance Standards*. Audit fieldwork was conducted between February and December 2018.

We included tests of the accounting records and such other auditing procedures as we considered necessary under the circumstances. To accomplish specific Information Technology control objectives, we applied a governance, risk, and compliance framework, which utilizes COBIT 5.0 Framework, the National Institute of Standards and Technology (NIST) Special Publications 800-53A Revision 4*, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, and* the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

During the audit, we reviewed the University and HCN's policies and procedures, applicable Florida Statutes and federal laws, observed current practices, interviewed responsible personnel, and tested selected transactions and devices. Sample sizes and transactions selected for testing were determined on a judgmental basis.

We also reviewed other internal and external audit reports issued during the last three years to determine whether there were any prior recommendations related to the scope and objectives of this audit. We found that a coding/billing review for 2017 and 2018 was conducted by an external vendor, Ankura Consulting Group. A report was issued on August 29, 2018, and contained five recommendations for management to implement. The results of the review are addressed in the Other Observations section of this report under Billing and Coding Assessment.

Additionally, James Moore Certified Public Accountants and Consultants performs an annual audit of the financial statements of the HCN. For each year audited, the accounting firm issued an unmodified opinion and did not identify any deficiencies in internal controls related to financial reporting.

BACKGROUND

The mission of the HCN, is "To support the FIU Academic Health Center by facilitating the clinical practice of medicine by the Herbert Wertheim College of Medicine (HWCOM or "College") physicians and providing health care business services to all health care practitioners working under the Academic Health Center." The HCN performs various administrative functions related to the practice of medicine, including billing and collections, contract management with vendors and insurance plans, provider credentialing, and administration of practice operations.

In the fiscal year 2015-16, the HCN transitioned from a full risk clinical model to a Management Service Organization (MSO) model. In the MSO model, the HCN's revenue consists of management fees derived from managing the HWCOM Clinics, the Office of International Affairs educational program, the FIU Student Health Clinics, the Center for Children and Families, Embrace, and rental revenue from leases of the Ambulatory Care Center to Miami Children's Hospital and Gastro Health.

Since the transition to the MSO model in July 2015, patient revenues and respective accounts receivable from clinical services provided at the HWCOM Clinics are no longer recorded on the HCN's books, but are instead recorded on the books of the HWCOM. Conversely, the operating expenses of the clinics are processed and recorded in the books of the HCN under the Clinics line of business, but are reimbursed by the College using a cost reimbursement model. The expense reimbursements are recorded as revenue under the clinical management line of business. Both revenues and expenses from the Office of International Affairs program are captured in the books of the HCN and net profits are transferred to the College at fiscal year-end.

As part of the scope of the audit, we specifically focused on the HCN's management of the HWCOM's clinics. The timeline below depicts the HCN's transition to a MSO model and the effect on patient revenues and clinical operating expenses.

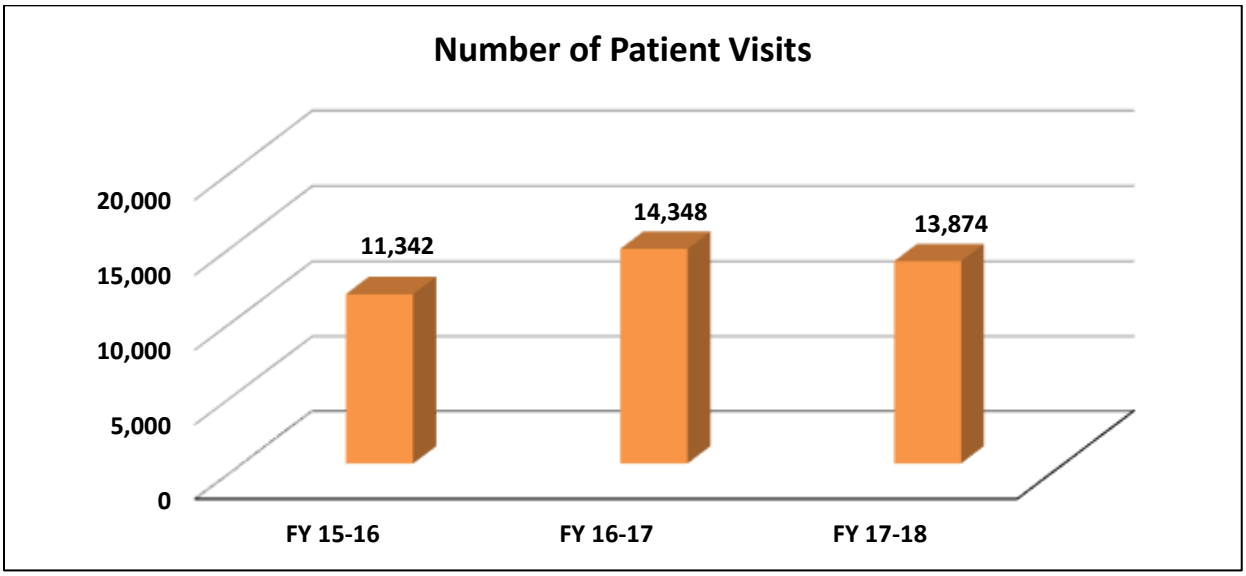
Evolution of HWCOM Clinics Financial Model

	FY 14-15	FY 15-16	FY 16-17	FY 17-18
	HCN is a full risk model	HCN evolves into a MSO	HCN operates as a MSO	HCN operates as MSO and aligns 100% of its operating expenses under the MSO line of business
MSO Fee to HCN	N/A	15% of clinical gross charges	Via payroll allocation: HCN admin staff effort allocation under clinics	Flat MSO Fee of $250K
Patient Revenue	Under HCN	Under HWCOM	Under HWCOM	Under HWCOM
Clinical Operating Expenses	Under HCN	Clinical support personnel, physician salaries and medical supplies under HWCOM	100% of clinical operating expenses, plus a percentage of HCN Admin effort allocation to clinics is paid by HWCOM	100% of HCN Admin personnel aligned under the HCN MSO, plus direct MSO expenses, operations, eligibility, credentialing and billing services

HWCOM Clinics

The HWCOM Clinics include two faculty group practices located in the Ambulatory Care Center (ACC) at Florida International University's Modesto A. Maidique Campus (MMC) and the Broward Health Medical Center in Fort Lauderdale, FL. The Clinics' physicians are accredited faculty members of the College and provide comprehensive care for patients in several specialty areas, including dermatology, family medicine, gynecology, hematology/oncology, internal medicine, psychiatry and behavior health, reproductive endocrinology, and travel medicine. There were 22 billing providers and over 14,000 patients seen at the MMC and Broward locations during the audit period.

The graph below shows the trend in patient visits over the past three fiscal years.

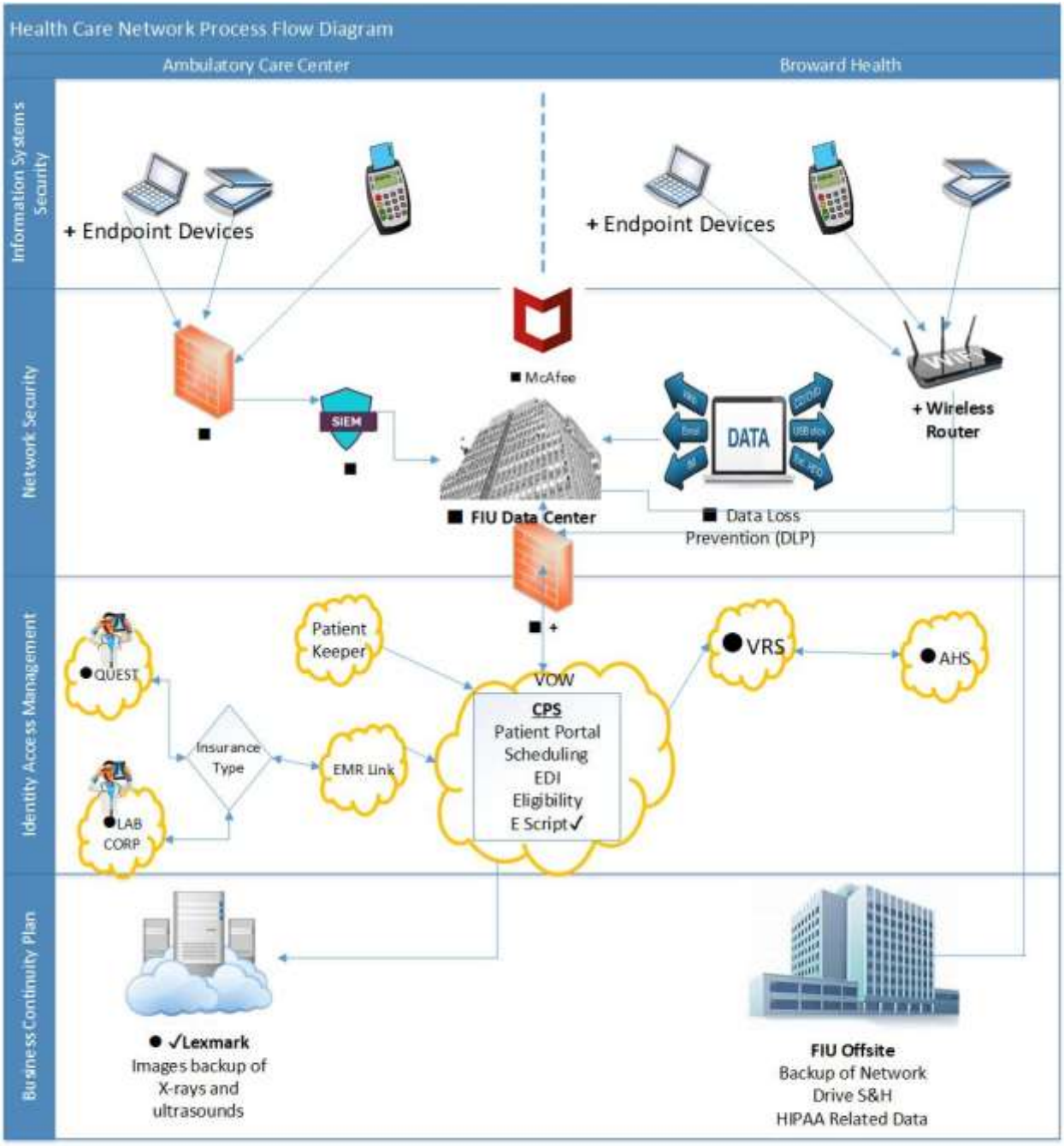


As part of the management of the clinical practices, the HCN provides support services including:

- Administration;
- Operations and Personnel Management;
- Inventory Management;
- Customer Service Training and Support;
- Patient Satisfaction Surveys;
- Provider Credentialing; and
- Billing and Collections.

Additionally, the HCN has a Revenue Cycle Management Services Agreement with Virtual OfficeWare Healthcare Solutions (VOWHS) to provide certain services related to billing and revenue cycle aspects of the clinical operations.

The HCN also utilizes the HWCOM's IT Department for system support. Below is an overview of the HCN's current IT environment. A glossary of terms can be found in Appendix A.

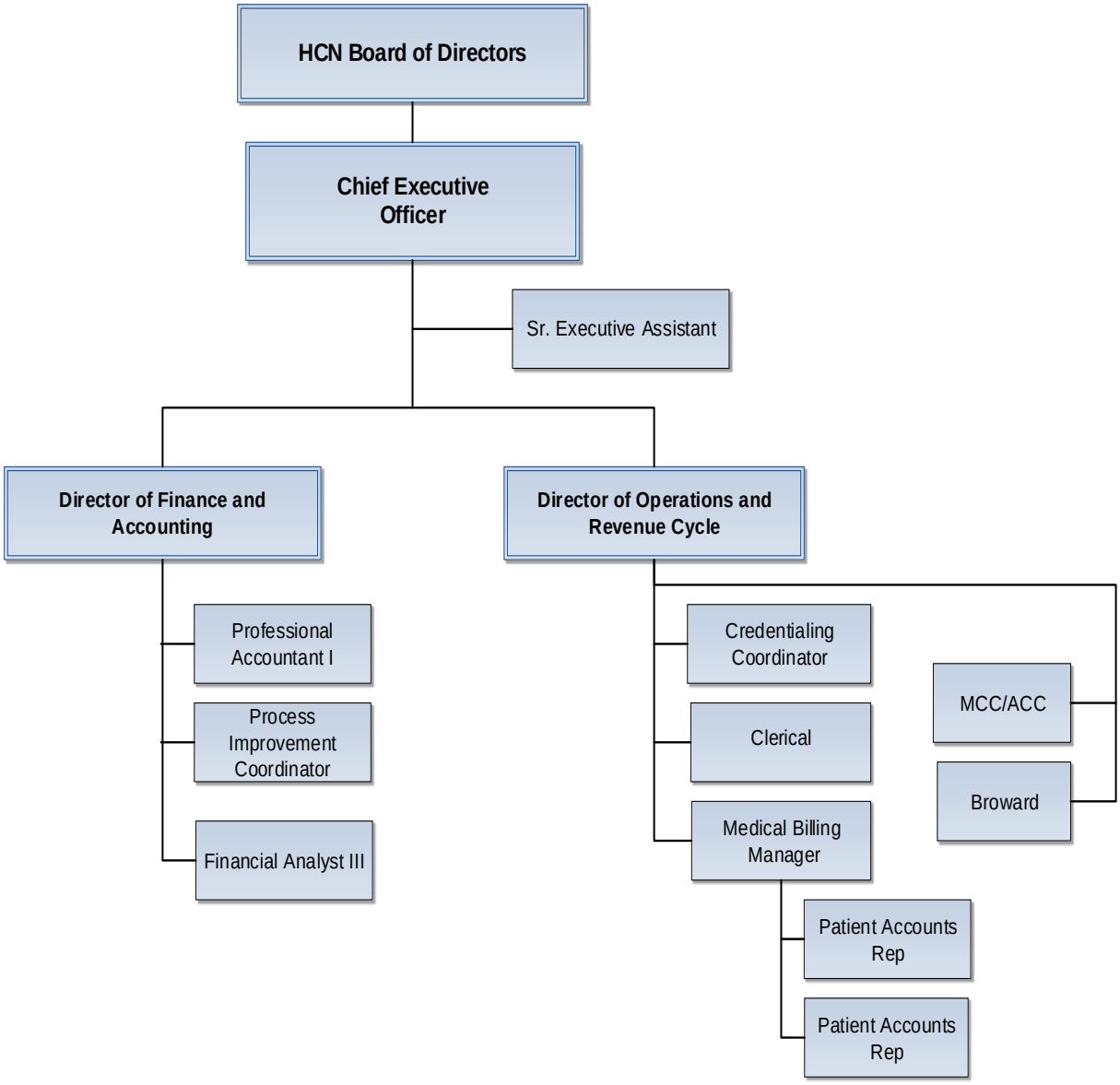


Legend:
- ■ Division of IT
- ✓ HWCOM Managed
- ● 3rd Party Managed
- + HWCOM Managed

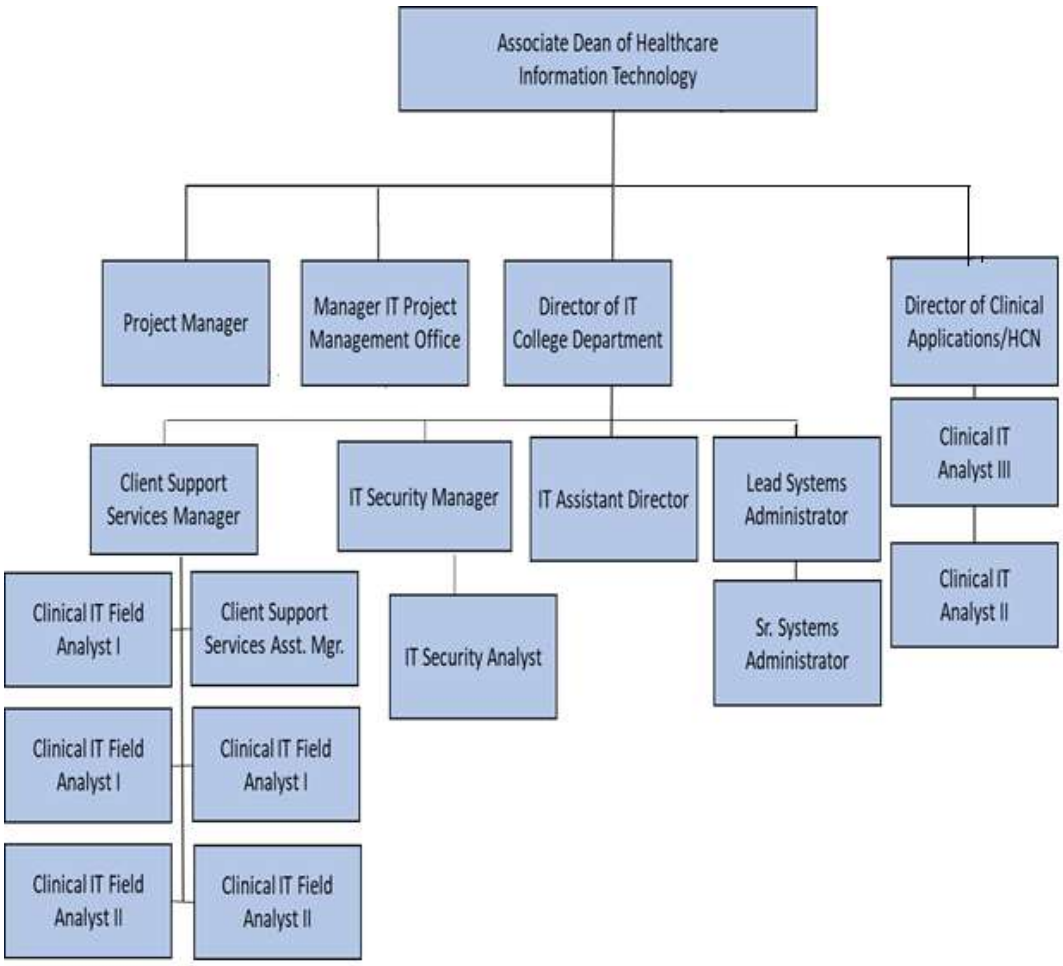
Diagram 1

Personnel

The following organization chart depicts the HCN's core organizational structure. The clinical support staff for the HWCOM Clinics report to the Director of Operations and Revenue Cycle, as shown below. Clinical providers report to their respective department chairs within the College.



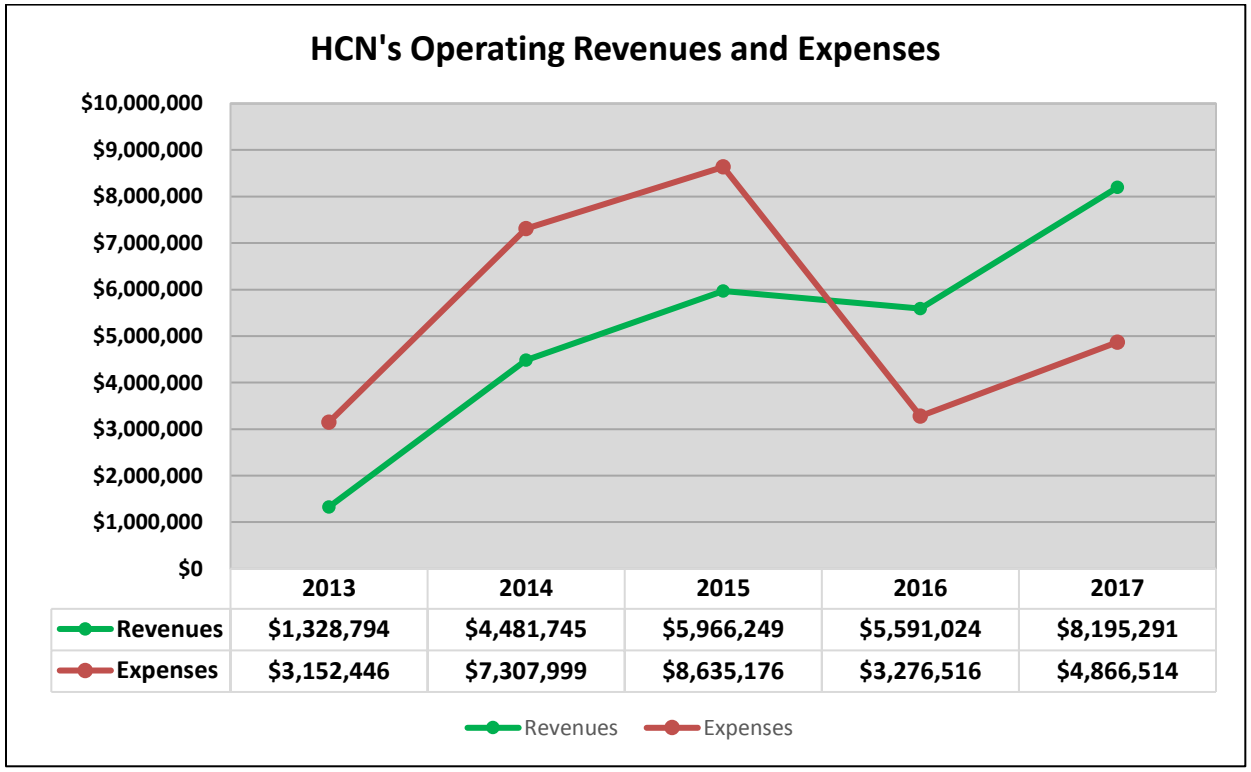
The following organizational chart depicts the HWCOM's IT personnel that provide support to the HCN and HWCOM Clinics.



Financial Information

During the fiscal year 2016-17, the HCN's operating revenues totaled approximately $8.2 million and operating expenses totaled approximately $4.9 million. Operating revenues consisted of approximately $4.3 million in management fee revenue, $3.4 million in Office of International Affairs revenue, and $0.5 million in rental income and other revenue[1]. The cost for managing and operating the HWCOM Clinics was $2.1 million, representing approximately 50% of the management fee revenue.

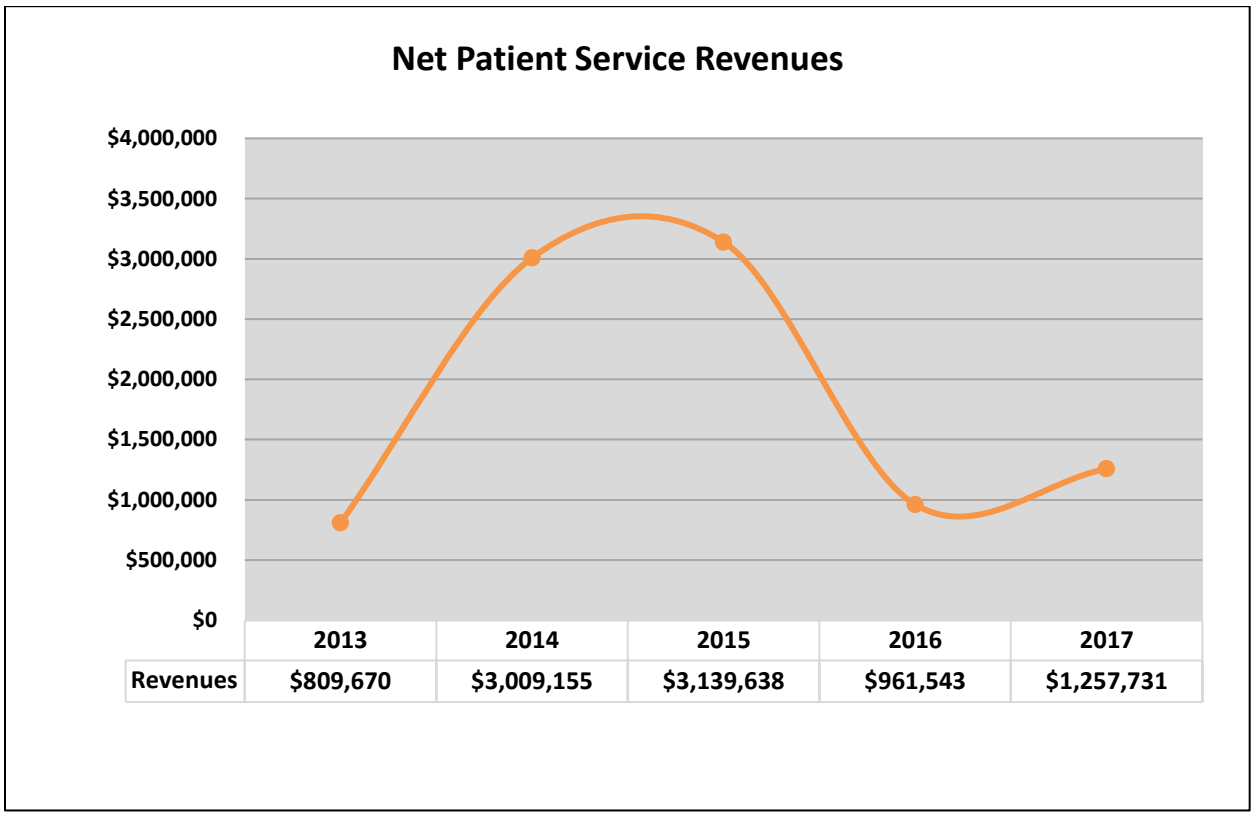
The following graph depicts the HCN's operating revenues and expenses[2] over the last five fiscal years.



	2013	2014	2015	2016	2017
Revenues	$1,328,794	$4,481,745	$5,966,249	$5,591,024	$8,195,291
Expenses	$3,152,446	$7,307,999	$8,635,176	$3,276,516	$4,866,514

[1] Source: The FIU-HCN's Audited Financial Statements for the Fiscal Year Ended June 30, 2017.
[2] Excludes non-operating expenses such as interest expense and transfers out.

Net patient service revenue earned during the fiscal year 2016-17 was approximately $1.2 million, of which, $1.1 million or 91% was from the HWCOM clinics. Total net patient service revenues since our prior audit are shown below[3].



	2013	2014	2015	2016	2017
Revenues	$809,670	$3,009,155	$3,139,638	$961,543	$1,257,731

[3] Revenues for fiscal years 2014 and 2015 represents clinical services provided at four sites. In the fiscal year 2015, the HCN undertook a restructuring that resulted in the elimination of three lines of business and divestment of two clinical facilities. (Source: The FIU-HCN's Audited Financial Statements.)

FINDINGS AND RECOMMENDATIONS

Overall, our audit disclosed that 18 of the 30 prior recommendations were fully implemented and 12 were not. There were areas where internal controls can be improved, particularly as related to patient recordkeeping and account review, the electronic medical record system, network security, and access controls. 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**

1. Implementation of Prior Audit Recommendations

The prior audit report of the HCN's Billing, Collections, and Electronic Medical Record Systems, dated November 13, 2013, contained 30 recommendations which management had self-reported as being fully implemented. During this audit, we compared management's assertions to current processes and performed tests to determine if the recommendations were effectively implemented. Our assessment revealed that 18 of the recommendations were fully implemented, 11 were partially implemented, and one was not implemented.

The test results for each recommendation are as follows:

No.	Recommendation	Implementation Status		
		Fully Implemented	Partially Implemented	Not Implemented
New Patient Registration Forms				
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.		✓	
Billing and Collections				
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.	✓		

No.	Recommendation	Implementation Status		
		Fully Implemented	Partially Implemented	Not Implemented
2.6	Update policies and procedures to include a cash control policy.	✓		
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.	✓		
Policies and Procedures				
3.1	Review and update all financial management policies and procedures, including policy numbers 5.11, 5.19, 5.22, and 5.25.	✓		
Reporting Tools				
4.1	Develop automated reporting tools that are fully supportable.	✓		
Compliance				
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.	✓		
Systems Security				
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.		✓	

No.	Recommendation	Implementation Status		
		Fully Implemented	Partially Implemented	Not Implemented
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.	✓		
Network Security				
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.	✓		
Access Controls				
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).	✓		

No.	Recommendation	Implementation Status		
		Fully Implemented	Partially Implemented	Not Implemented
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.		✓	
Business Continuity				
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.		✓	
	Total	**18**	**11**	**1**

Recommendation

1. The HCN should fully implement all outstanding prior audit recommendations.

The following are the recommendations that were determined to be either partially implemented or not implemented, along with our current observations, management's action plan, and revised implementation dates.

- **Recommendations 1.1 and 1.2** – Ensure that all patient forms are completed. Re-educate physicians and clinical support staff on the importance of obtaining and completing patient forms.

  Previously Reported Actions: 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. Re-education of both physicians and clinical staff will be completed with revised policy and staff meeting.

  Current Observation: We selected and reviewed 37 patients' electronic medical records to determine if the required patient forms and documentation were on file. These forms included Patient Demographics, Medical History, Psychiatry Initial Screening, General Consent to Treatment and Financial Responsibility (Acknowledgement of Receipt of Privacy Practices, Medical Records Release, and Assignment of Benefits), Notice of Social Security Number Collection, Use or Release, and a copy of the patients' identification and insurance card. We noted the Medical History form was amended and no longer requires the physician's signature. Our review also disclosed that eight record sets had missing documentation as follows:

  - Four did not have any patient forms or identification on file;
  - Three were missing the Psychiatry Initial Screening form; and
  - One was missing a proper form of identification.

  In addition, we reviewed HCN Policy 4.19 – *Medical Record Documentation* and found that it had not been revised since our last audit.

  Management Action Plan: 1) Retrained all staff by 12/14/18. 2) Began a self-audit on 12/3/18 to randomly establish a baseline. 3) Established internal controls by having user reminders on an ongoing basis. 4) Established continuous monitoring via report on an ongoing basis.

  Implementation Date: Immediately

- **Recommendations 2.2 and 2.3** – Ensure that work queues are timely reviewed and patient accounts with outstanding accounts receivable and credit balances are

properly followed up. Improve current processes to ensure timely billing of all seen patients.

Previously Reported Actions: For submission of charges and posting of payments, current policy will be revised and staff will be appropriately trained. Policies will be 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.
- Physician "bucket" to be reviewed by individual physician and all billing items to be completed within 7 business days.
- A/R reports to be reviewed monthly.
- Credit balance reports to be reviewed monthly.

Current Observation: We tested 38 patient accounts to determine whether claims for medical services provided were accurately and timely billed, collected, and recorded. Our testing revealed that:

- Six (16%) had charges that were submitted between 11 and 18 business days after the date of service;
- Fourteen (37%) did not have payments posted to their account until 16 to 18 days after receipt of the Explanation of Benefits (EOB) or payment;
- Five (13%) were still pending write-offs due to claim denials, non-receipt of co-payment from the patient or being a part of the College's NeighborhoodHELP program; and
- One EOB could not be located, as it was not properly placed in the medical record.

According to the Director of Operations and Revenue Cycle, the HCN relies on the Revenue Cycle Management Services Agreement with Virtual OfficeWare Healthcare Solutions (VOWHS) to handle follow-up of claims and to perform regular patient account inquiries. The agreement states that VOWHS is responsible for the posting of payments and adjustments, which includes review and analysis of insurance EOB's for appropriate reimbursement, underpayments, re-files, and rejections. VOWHS uses its sister company, Virtual Revenue Solutions (VRS), to perform follow-up when claims are denied, underpaid, and/or inaccurately reimbursed from the payer.

Our review of the agenda and minutes from three past meetings between the HCN and VRS revealed several issues that the HCN addressed with VRS including: untimely follow-up and/or resubmission of claims, preventable denied claims, incomplete and poor quality collections effort, incorrect ticket placement, low production volume, and patient complaints.

Management Action Plan: Patient posting is completed with the billing vendor (VRS). Internal charge retrieval process was implemented on November 1, 2017. The charge retrieval process reconciles every patient visit with respective charges and creates a ticket. Provider has 48 hours to complete open tickets. This was implemented in August 2017. Weekly reports with open tickets are submitted to Clinical Affairs and enforcement is done in collaboration with Clinical Affairs. Beginning in December 2018, the Chair of the respective department also started receiving the report via email to further enforce compliance.

Implementation Date: Immediately

- **Recommendation 6.2** – Ensure that virus definition files and operating system security updates are updated in a timely manner.

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

  Current Observation: We tested for unpatched vulnerabilities, which allow malicious code entry points into the network. Using a vendor based security analysis tool, we found that 12 of the 25 high-risk endpoint devices tested were missing from 1 to 25 critical updates. Once on the network, malicious code can cause temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses relating to restoring systems and files, and potential harm to an organization's reputation.

  An additional monitoring 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 stated that vulnerability scans were not performed on the HCN endpoint devices, which reduces the effectiveness of the network monitoring controls.

  Management Action Plan: HWCOM has completed all the identified endpoints that were missing virus definition files and OS updates except for one workstation. Client Support team is in the process of reimaging the endpoint. In addition, HWCOM is working with DoIT Security Office in deploying Nessus Vulnerability Client agent to all HCN endpoints.

  Implementation Date: January 30, 2019

- **Recommendation 7.1** – Review all firewall rule sets to ensure firewall rules are appropriate.

Previously Reported Actions: HWCOM has requested the monthly report on a periodic basis and will continue to request these for firewall review

Current Observation: In March 2017 and April 2018, HWCOM IT's former system administrator performed a review of the firewall rules and identified the firewall rules that should be kept. We selected rules from the second firewall assessment and confirmed that the Division of IT disabled rules as requested. To determine the effectiveness of the prior firewall reviews, we requested the Division of IT perform a zero-hit count test for the Ambulatory Care Center location to determine the number of ports actively being used. In our test of 157 rules selected, we identified that only nine rules had "hit counts" greater than zero, which signifies the ports were being used. The other 148 rules that showed zero "hit count" were not actively being used. These results indicate that although HWCOM reviewed the firewall rules, further assessment of the rules is warranted. Disabling open firewall rules that are no longer needed reduces the risk of unauthorized access.

Management Action Plan: HWCOM will work with HCN management to identify rules that can be removed that were previously utilized for X-ray services no longer in service.

Implementation Date: January 30, 2019

- **Recommendation 7.2** – Sufficiently document the firewall requests to ensure firewall rules are only allowed based on its mission/business need.

  Previously Reported Actions: Firewall rule request checklist has been created to memorialize all requests to the firewall.

  Current Observation: According to the HWCOM IT, the HCN's Director of Operations and Revenue Cycle sends an email with the request to HWCOM IT Helpdesk where they create a ticket and assign it to the HWCOM Infrastructure team. The HWCOM Infrastructure team evaluates the request's business need before sending it to the Division of IT. Firewall rules requests are documented in SharePoint.

  We examined 57 active rules and determined that only two were adequately documented, whereas 32 were not documented, and 23 were partially documented. We also examined six disabled rules and determined that two had partial documentation and four had no documentation. Without adequate documentation, management would be unable to determine whether a firewall rule is appropriate.

  Management Action Plan: Adequately documented firewall requests.

  Implementation Date: Immediately

- **Recommendation 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.

Previously Reported Actions: 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.

Current Observation: In its current configuration, the EMR application disseminates roles and privileges in a manner that does not accurately align with its users' job duties. For example, our test disclosed that seven (7) out of 45 users were assigned access to the Providers (MDs, APNPs, and PAs) role, which included the former Compliance Officer, IT staff, and third party billing staff. For the Broward Router; however, we did identify two HWCOM employees—the HWCOM IT Director and the former Senior Systems administrator—who should not have access to this router. HWCOM removed access immediately upon notification.

Prior to receiving access, users are required to complete the Confidentiality Agreement Form, HIPAA training, IT Security Awareness training, and EMR training. The Practice Manager fills out an access management form and HWCOM IT Security then reviews the request to ensure that the user meets all requirements prior to onboarding.

Overall, 24 out of 48 employees and providers on-boarded during the audit period successfully completed all four requirements. However, none of the 22 VRS staff who are application users completed all necessary requirements. See Diagram 2 for completion rates per application.

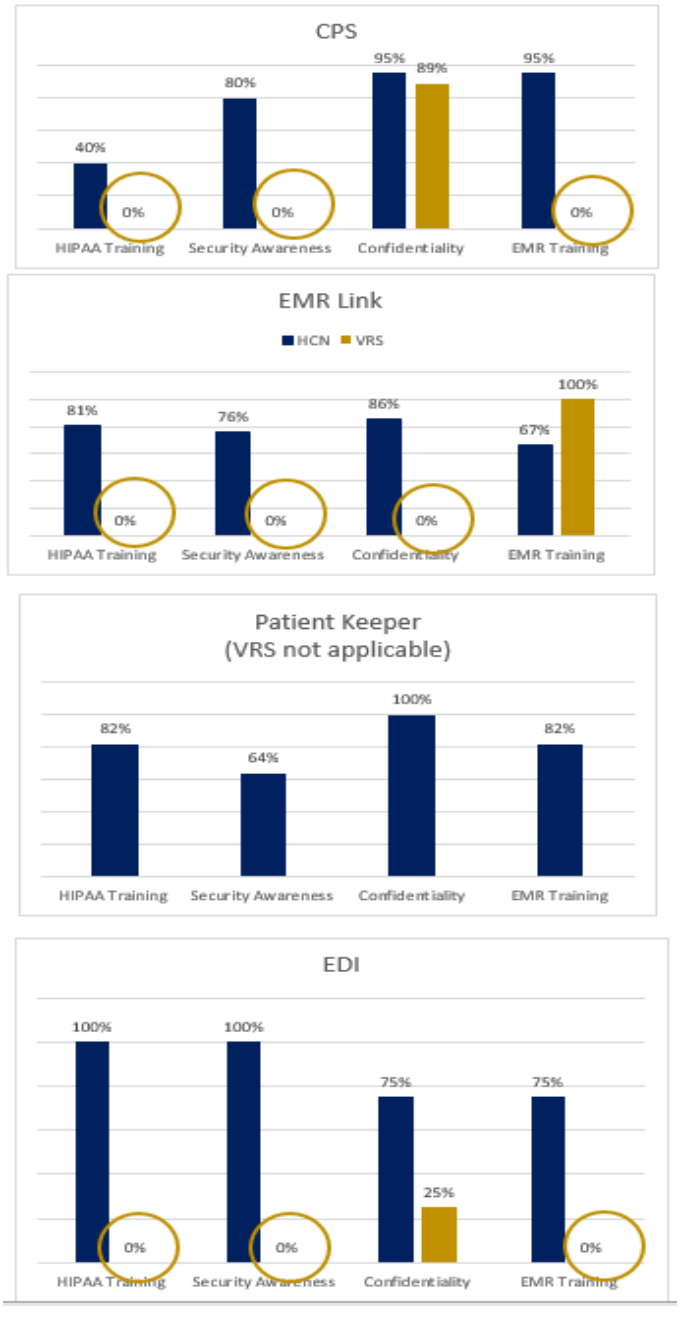


Diagram 2

The required training and signed confidentiality forms ensures that employees know and comprehend the importance of maintaining the confidentiality of sensitive data.

Management Action Plan: HCN management completed and formally documented all EMR users and respective privileges. HCN will be responsible for providers and billing vendors. HCN will collaborate with IT to review roles and respective privileges on an ongoing basis.

Implementation Date: Immediately

- **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.

  Previously Reported Actions: 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.

  Current Observation: Since our last audit, the responsibility of reviewing the audit log was redirected to the University's Compliance Office under the Director of Compliance for Health Affairs' position. During our audit period, audit logs were not reviewed and we were informed that the Compliance Office is in the process of recruiting for a replacement no later than spring 2019. During our examination of the CPS log files, we found that patient information was being accessed through a generic user account originally set up for training purposes. The absence of a review increases the risk that inappropriate access to sensitive patient information may go undetected.

  Management Action Plan: The new Director of Health Care Compliance will be starting on January 21, 2019, and will meet with Internal Audit to discuss the pertinent audit findings and develop a plan to address them.

  Implementation Date: March 31, 2019

- **Recommendation 8.4** – Review roles and privileges allocation to user accounts and distinguish which privileges not to combine to prevent a segregation of duties conflict.

  Previously Reported Actions: 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.

  Current Observation: Since our last audit, the HWCOM established the *Access Controls to Systems Containing Electronic Protected Health Information for Workforce Members Procedure* as a mitigating control to delineate the proper method of controlling access to ePHI. HWCOM annually verifies user access list through the

Access Verification Procedure. However, during our examination, we observed 16 non-IT related groups and users with administrator role in the EMR application. Typically, the administrator role is assigned to IT staff to maintain system configurations, including adding and modifying user accounts. Our current observation suggested that HWCOM needs to further review these users access for proper alignment with roles.

Management Action Plan: HCN management completed and formally documented all EMR users and respective privileges. HCN will be responsible for providers and billing vendors. HCN will collaborate with IT to review roles and respective privileges on an ongoing basis.

Implementation Date: Immediately

- **Recommendation 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.

  Previously Reported Actions: 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.

  Current Observation: Previously, the EMR application had six generic accounts. We examined the current user listings and found that five were removed and one remained. In addition, there were two generic accounts in EDI with administrator privileges and the ability to create other accounts managed by VRS.

  Generically named vendor accounts, specifically with administrator privileges, reduce the information systems' ability to track individual user actions that could bypass existing identity management controls.

  Management Action Plan: Reviewing with EMR vendor as part of contract negotiations.

  Implementation Date: January 30, 2019

- **Recommendation 9.2:** Periodically perform tests on the EMR and Billing systems and take corrective actions as necessary.

  Previously Reported Actions: IT team reviews month end activities to ensure EMR and PM systems are working as expected. IT team and HCN operations and revenue cycle leadership work collaboratively on this task. Ongoing to comply with quality performance measures.

  Current Observation: Documentation provided by the HCN showed that HWCOM IT performed monthly tests on the network drives that stored the HCN file systems data.

We noted that the HWCOM alerted the FIU Windows Security Group of errors encountered during testing, which they then corrected and retested. However, the only system that the HWCOM did not test was the EMR Link. According to their website, EMR Link has a 48-hour objective for their Disaster Recovery Plan. The HCN stated that they would process documents manually in the event the EMR Link application is down. Including EMR Link in their annual testing will increase management's ability to ensure the HCN has continuous operations in the event that the application is not operational.

Management Action Plan: This occurs on an ongoing basis. Refer to SOC2 report.

Implementation Date: Immediately

2. Other Observations

While testing management's implementation of the prior audit recommendations, we tested certain ancillary but important IT controls and found them to be functioning properly. For example:

- The HCN reviews audit logs to check for process errors to ensure the application's continuous operation, as required by FIU Policy No. 1670.015, *Authentication and Audit Controls for ePHI*.
- User access and permissions to the EMR LINK, Patient Keeper and e-Script applications comports with acceptable least privilege convention. (See Diagram 1 on page 4.)
- The Director of Operations and Revenue Cycle reviews the Data Loss Prevention (DLP) reports received from the Division of IT.
- As required by HIPAA regulations 164.308(a)(1)(ii)(A), *Risk Analysis,* comprehensive risk assessments of the HCN's systems that identified risk levels, business processes, and security recommendations were performed. In addition, the HCN will be included in a university-wide risk assessment currently being perform by an external company hired by the Division of IT.
- The Division of IT performed a PCIDSS assessment on the credit card machines located in the Ambulatory Care Center and Broward Health locations and found no security issues.

In addition to the accomplishments noted above, our tests also found that opportunities for improvement exist in the following areas:

a) Billing and Coding Assessment

AHC/HCN Policy 7.11 – *Auditing and Monitoring*, states that the FIU AHC Compliance Officer is responsible for monitoring and reviewing the coding and documentation practices of providers within the Faculty Group Practice and Student Health Services that are billing on behalf of and/or employed by FIU.

Since our last audit, the Director of Compliance for Health Affairs position (formerly the FIU AHC Compliance Officer) transitioned from HWCOM to the University's Compliance Office. Due to the position's vacancy, a third-party company, Ankura Consulting Group ("Ankura"), was hired to conduct a billing and coding assessment and evaluate the accuracy of providers' coding. The assessment included a review of 36 HWCOM providers and 10 Student Health encounters.

Based on the report issued by Ankura on August 29, 2018, the HWCOM's coding accuracy rate was 73%, as 249 out of 340 encounters reviewed were accurately coded. Likewise, the coding accuracy rate for Student Health was 50%, as 5 out of 10 student health encounters reviewed were accurately coded. The following issues were identified:

- Twenty-three services were over-coded. (HWCOM)

- Forty-six services were under-coded. (HWCOM)
- No documentation found for 18 encounters. (HWCOM)
- Two encounters were billed using an incorrect provider. (HWCOM)
- One encounter was coded with an incorrect CPT code. (HWCOM)
- One encounter was coded using the incorrect E/M category. (HWCOM)
- Two student health services were over-coded. (Student Health)
- Three student health services were under coded. (Student Health)

The following recommendations were provided:

1) Determine the acceptable error rate for the College of Medicine.
2) Review each provider's individual results and determine who needs immediate education and re-audit.
3) Feedback to the providers on the audit results and education for the providers.
4) Once education is provided, a re-assessment of coding practices and principles should be completed within 30 days.
5) Ongoing monitoring should be conducted to give providers real-time feedback and used for educational purposes.

Management acknowledged that in the interim, until a new Director of Compliance is hired, they would continue to utilize an outside vendor and perform quarterly spot-checks until coding percentages are at an acceptable level.

b) HIPAA and Security Awareness Training

The HIPAA Privacy Rule requires covered entities to train all workforce members on its privacy policies and procedures, as necessary for them to carry out their functions. 45 CFR §164.530 – *Administrative Requirements of the HIPAA Privacy Rule*, states that a covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.

HWCOM's Human Resources Department manages compliance trainings, which include tracking the employee's completion of the annual HIPAA requirements. Based on the 2017 HIPAA Training Report, as of the February 2018, only 432 out of 533 employees (80%) completed the HIPAA training in 2017. Of the remaining 101 employees who did not complete the training, three were HCN clinical support staff or providers of the clinics. After our discussion with the Director of Operations and Revenue Cycle, two of the employees completed the training and provided updated documentation. The other employee had previously completed the training and provided an email showing that it was done.

Subsequent to our testing, we also received the 2018 HIPAA Training Report and noted that 560/563 (99%) of employees had successfully completed the training as of October 17, 2018. These current results indicate that HWCOM has made significant progress towards ensuring that employees have completed the annual HIPAA training.

In addition, according to the FIU Security Website, all FIU faculty and staff are required to participate in the security awareness training. The University offers a comprehensive security awareness training to all employees in order to protect the organization and address the multitude of vulnerabilities day-to-day employee activity creates. Our examination of a Security Awareness training report for HCN, provided by the Division of IT, found that training had not been completed by three employees. Upon notification, these employees successfully completed the Security Awareness Training. Successful completion of the FIU security awareness training reduces the risk of an employee inadvertently creating opportunities for hackers to compromise the University's network and sensitive data.

c) Notice of Privacy Practices

As required by the HIPAA Privacy Rule, the Notice of Privacy Practices describes how protected health information may be used and disclosed by a covered entity and how an individual can get access to their medical information. 45 CFR §164.520 states that the notice must contain the name or title, and telephone number of a person or office to contact for further information. In addition, §164.520(c)(2)(iii) states that if the covered healthcare provider maintains a physical service delivery site, they must also have the notice available for individuals to request to take with them and post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read it.

During the audit, we observed that the Notice of Privacy Practices was not posted at either of the clinical sites, MMC or Broward. In addition, we noted that the contact information on the Notice of Privacy Practices was outdated, as the phone number listed went to the voicemail system of the former AHC Compliance & Privacy Officer who left the University over a year ago. Thus, the compliance privacy hotline was not being monitored and patients calling with a privacy matter may not have been afforded the opportunity to have their concerns addressed.

After this was brought to the attention of the Director of Operations and Revenue Cycle, the Notice of Privacy Practices was updated and posted at the clinics.

d) IT Asset Management

According to the HWCOM IT, they update the asset management list as soon as new devices arrive. In addition, they also add the risk rating in their inventory list. The HWCOM IT supplied an asset list that identified 94 devices, their location, risk factor and whether it was a desktop, laptop, printer, or scanner. We selected 18 devices from the Ambulatory Care Center (ACC) and seven from the Broward Health locations for our Malware Prevention testing. At the time we conducted our examination, we noted that 11 of the 18 ACC devices and two of the seven Broward Health devices were not included on the asset management list, not assigned, or incorrectly assigned to employees. Upon notification, HWCOM IT corrected the inventory list to reflect the current devices used and users assigned to them.

In our internal audit report, University's IT Network Security Controls (Report No. 15/16-02, dated September 29, 2015), we indicated that asset lists were stored on individual spreadsheets and were not shared with the Division of IT. FIU Policy No. 1910.005, *Responsibilities for FIU Network and/or System Administrator*, requires departments' IT administrator to send a quarterly report to the Division of IT of any systems implementation or changes to the IT environment. Based on the NIST Cybersecurity Framework 1.0, by supplying the lists to the Division of IT, they could better assess the adequacy of their network security controls. We found that a quarterly report was not provided to the Division of IT. HWCOM was aware of the policy but was unsure on how to report the changes to the Division of IT.

Periodically reconciling the asset management list ensures that all devices are listed and correctly assigned. Additionally, HCN should report the current asset list to the Division of IT on a quarterly basis to increase the effectiveness of the University's cybersecurity controls.

e) Security Incident Response

On June 27, 2017, Virtual OfficeWare Healthcare Solutions (VOWHS) identified an attack as ransomware on its network, which caused an inability to access data on its systems. According to the vendor, they immediately shut down the affected servers and began working with an independent forensic investigator to determine the exact cause of the incident. The investigator determined that the cause of the incident was due to the Petya/NotPetya malware that also caused global disruptions at other healthcare organizations. The investigation further determined that there was no evidence of unauthorized access or exfiltration of FIU's data resulting from the incident. In addition, a business advisory and advocacy law firm later engaged by FIU to assist in the legal analysis and risk assessment of the incident also confirmed that the malware variant was not capable of data exfiltration.

Notwithstanding the outcome of the incident, we identified gaps in the University's policies and processes, and the need for improvement in breach notification protocol and policy alignment. (See Appendix B: Security Incident Timeline.)

FIU Policy No. 1670.020, *HIPAA Security: Duty to Report Security Incidents Involving Protected Health Information,* effective September 1, 2009, as amended, requires workforce members to **immediately report** any and all suspected and actual breaches of information security involving protected health information to **one** of the following University representatives: the designated HIPAA Security Administrator for the department, the University IT Security and HIPAA Security Officer, the University HIPAA Privacy Officer, or the University Compliance Officer. The policy also requires the unit's designated HIPAA Security Administrator and the University HIPAA Security Officer to mitigate harmful effects of the security incident. [**Emphasis added**]

In addition, FIU Policy No. 1930.021, *Incident and Breach Response Policy [IRP],* effective August 17, 2016, requires the "Responding Party" designated by the Department

or Division to notify the FIU Security Officer **and/or** the Compliance/Privacy Officer **within 24 hours** of verifying an incident involving private information. [**Emphasis added**]

Further, FIU Policy No. 1610.005, *Health Insurance Portability and Accountability Act Compliance*, effective June 8, 2015, as amended, establishes breach notification responsibility to the Privacy Officer, wherein that individual must notify the FIU Information Security & HIPAA Security Officer and the University Chief Compliance Officer & Privacy Officer **within 48 hours** of any reported incident[4]. [**Emphasis added**]

Upon notification of the aforementioned June 27, 2017, Incident from VOWHS, HWCOM IT staff immediately reported the incident to the HWCOM HIPAA Security Administrator. During the hours following confirmation of the incident, there were various other communications among HWCOM's internal staff, the vendor, and the Senior University Counsel. However, approximately 14 ½ hours elapsed before there was any documented communication from HWCOM IT to the University IT Security and HIPAA Security Officer, the most appropriate University official in the notification protocols of Policies 1670.020 and 1930.021, under the circumstances. The said communication was in response to the University IT Security and HIPAA Security Officer's inquiry about why she was not notified about the incident. (See Appendix B: Security Incident Timeline). Although the IRP requires 24 hours notification, not contacting the University IT Security and HIPAA Security Officer immediately limits the Division of its ability to respond to a data security incident in a timely manner.

Furthermore, our review of the cited policies disclosed the following:

- Inconsistent incident reporting timelines—"immediately," "within 24 hours," and "within 48 hours."
- Policies 1670.020 and 1930.021 permit discretionary notification (i.e., "and/or") of a security incident to the University IT Security and HIPAA Security Officer, even when electronic data is involved.
- Policy 1670.020 does not cross-reference the IRP or its additional notification requirements.
- The University Operations Committee approved and adopted the IRP on August 17, 2016, but the scheduled communication of the policy was delayed by approximately 11 months, and its posting to the policy library was delayed by approximately 23 months.

Per our discussion with the University Compliance Office, they are currently undergoing a comprehensive audit with an outside consultant and have started to identify the appropriate audience for further dissemination of the IRP and a communications campaign around that dissemination. We acknowledge that they, along with the HIPAA Committee have been actively discussing and addressing the alignment of HIPAA policy

[4] Subsequent revision to the Policy, effective December 31, 2017, requires notification of breach only to the Compliance and Privacy Officer within 48 hours of any reported incident.

and procedures to the IRP and will determine final steps to take after the assessment is completed.

f) Facilities Access Log Controls

According to HIPAA §164.308(a)(1)(ii)(D), *Information Systems Activity Review*, Facility Access Controls must implement procedures to regularly review records of information system activity, such as audit logs and access reports. The Director of Operations and Revenue Cycle does not review facilities access logs since Facilities Management does not provide him the reports.

g) Business Continuity Plan and Procedure

A Business Continuity Plan details actions to enable the HCN and the University's Division of IT to respond to incidents and disruptions in order to continue operations of critical business processes at an acceptable level. We examined documentation provided which demonstrated that a suitable plan is in place. The Plan, which was revised 29 times in the last four years, includes the EMR, network files and the imaging system. However, the Plan does not include Patient Keeper and EMR-LINK. The inclusion of Patient Keeper and EMR-LINK ensures that the HCN is properly prepared to continue its operations in the event of a disaster.

Recommendations

The HCN or HWCOM should:	
2.1	Ensure all recommendations from the billing and coding assessment conducted by Ankura are implemented.
2.2	Ensure all employees complete the HIPAA and Security Awareness trainings in a timely manner.
2.3	Report the inventory list to the Division of IT on a quarterly basis.
2.4	Collaborate with the Chief Compliance and Privacy Officer to develop a plan of action to address the gaps identified in the breach notification protocol. The plan should include among other things, aligning the breach notification timeline across Policies 1670.020, 1930.021, and 1610.005; making immediate notification of a breach to the Chief Information Security Officer mandatory instead of discretionary; and communicating the Incident and Breach Response Policy university-wide.
2.5	Review facilities access reports on a periodic basis.
2.6	Include the Patient Keeper and EMR-LINK applications in the Business Continuity Plan.

Management Response/Action Plan:

2.1 Plan of action and corrections were presented to HCN's Board of Directors meeting on Oct 28, 2018.

Implementation Date: June 30, 2019

2.2 HCN will request from the staff the attestation of completion of training on an annual basis. The missing ones were completed in November 2018.

Implementation Date: Immediately

2.3 HWCOM IT has reached out to DoIT for standardized process or template to communicate this information. Meanwhile, HWCOM IT has sent the current inventory to DoIT's email (security@fiu.edu).

Implementation Date: Immediately

2.4 HWCOM will request to meet with the Chief Compliance and Privacy Officer to discuss the policies listed above by January 30, 2019. Once those policies are finalized, we will also communicate to staff.

Implementation Date: March 31, 2019

2.5 HCN management contacted the Key Control department to get an access report. Going forward, the report will be reviewed on a quarterly basis.

Implementation Date: Immediately

2.6 HCN developed down time procedures.

Implementation Date: Immediately

APPENDIX A

Glossary of Terms

- **ACC**: Ambulatory Care Center.
- **AHS**: Access Healthcare. Third party vendor used by VRS until July 5, 2018.
- **CPS**: Centricity Practice Solutions. Electronic medical record system that is hosted by VOWHS.
- **EDI**: Electronic Data Interchange. Interfaced system, used to submit and receive electronic claims and payments to and from payers (insurance companies).
- **EMR**: Electronic Medical Record.
- **EMR Link**: Interfaced system used to submit, process, and receive electronic laboratory orders and results.
- **eScript**: Interfaced system used to submit and receive electronic prescriptions and refill requests.
- **PatientKeeper**: Clinical and financial application used to streamline physician workflow for healthcare providers to improve patient care.
- **VOWHS**: Virtual OfficeWare Healthcare Solutions. Electronic Health Records & Practice Management software through Centricity Practice Solution for physician clinical, financial, and administrative needs.
- **VRS**: Virtual Revenue Solutions. Billing, A/R, and insurance claim processes vendor used by HCN.

APPENDIX B

Security Incident Timeline

No.	Action Taken
1	Tuesday, June 27, 2017, at 8:00 a.m., the vendor discovered that the VOWHS computer systems was attacked by a ransomware. According to the vendor, they immediately shut down the servers and began an investigation.
2	Tuesday, June 27, 2017, at 4:07 p.m., the vendor notified HWCOM IT Security Manager and Associate Dean for Health Information Technology about Security Incident.
3	Tuesday, June 27, 2017, at 4:14 p.m., the Associate Dean for Health Information Technology notified HWCOM's HIPAA Security Administrator of the Incident and also notified Senior University Counsel the at 4:32 p.m.
4	Tuesday, June 27, 2017, at 4:45 p.m., HWCOM IT, General Council, and vendor's COO and Account Manager met to discuss Incident.
5	Wednesday, June 28, 2017, at 3:24 a.m., the University's Chief Information Security Officer emailed Associate Dean for Health Information Technology inquiring about details of the Incident and why she was not notified. Associate Dean for Health Information Technology forwarded an email from the vendor at 6:26 a.m.
6	Wednesday, June 28, 2017, at 11:30 a.m., Incident Response Team (IRT) that included HWCOM IT, Division of IT, Compliance, and General Council met to discuss updates and incident mitigation actions, including disabling firewall rules, VPN connections, and applying patch updates. According to the IRP, the IRT must be notified as soon as possible but no more than 24 hours.
7	July 26, 2017, the vendor notified HWCOM that their internal forensic investigation determined that there was no evidence of unauthorized access or exfiltration of data. On September 9, 2017, FIU's forensic analysis determined that there was a low probability that PHI had been compromised.