AUDIT COMMITTEE
MEETING AGENDA

February 19, 2015

1:00 P.M.

125 Worth Street,
Rm. 532
5th Floor Board Room

CALL TO ORDER — Ms. Emily A. Youssouf

- Adoption of Minutes December 4, 2014 — Ms. Emily A. Youssouf

INFORMATION ITEMS

- Audits Update — Mr. Chris A. Telano
- Compliance Update — Mr. Wayne McNulty

EXECUTIVE SESSION

OLD BUSINESS

NEW BUSINESS

ADJOURNMENT

MINUTES

AUDIT COMMITTEE **MEETING DATE: December 4, 2014**
TIME: 10:00 AM

COMMITTEE MEMBERS
Josephine Bolus, RN

OTHER BOARD MEMBERS
Mark Page

STAFF ATTENDEES
Antonio Martin, Executive Vice President/COO
Salvatore Russo, Senior Vice President/General Counsel, Legal Affairs
Deborah Cates, Chief of Staff, Chairman's Office
Randall Mark, Chief of Staff, President's Office
Patricia Lockhart, Secretary to the Corporation, Chairman's Office
Lynette Sainbert, Assistant Director, Chairman's Office
Marlene Zurack, Senior Assistant Vice President/CFO, Corporate Finance
Paul Albertson, Senior Assistant Vice President
Jay Weinman, Corporate Comptroller
Gassenia Guilford, Assistant Vice President, Finance
Christopher A. Telano, Chief Internal Auditor/AVP, Office of Internal Audits
Wayne McNulty, Corporate Compliance Officer
Kathleen McGrath, Senior Director, Communications & Marketing
Kirk Leon, Director, Central Office Corporate Security
Alice Berkowitz, Assistant Director, Central Office Budget
Daren Ng, Senior System Analyst, Central Office Budget
Diane Toppin, Senior Director, Central Office Medical & Professional Affairs
Dean Moskos, Director, Office of Facilities & Development
Devon Wilson, Senior Director, Office of Internal Audits
Chalice Averett, Director, Office of Internal Audits
Carol Parjohn, Director, Office of Internal Audits
Steve Van Schultz, Director, Office of Internal Audits
Carlotta Duran, Assistant Director, Office of Internal Audits
Delores Rahman, Audit Manager, Office of Internal Audits
Frank Zanghi, Audit Manager, Office of Internal Audits
Roger Novoa, Supervising Confidential Examiner, Office of Internal Audits
Rosemarie Thomas, Supervising Confidential Examiner
Sonja Aborisade, Supervising Confidential Examiner, Office of Internal Audits
Armel Sejour, Supervising Confidential Examiner
Barbarah Gelin, Associate Staff Auditor, Office of Internal Audits
Gillian Smith, Associate Staff Auditor, Office of Internal Audits
Guzal Contrera, Staff Auditor, Office of Internal Audits
George Payyapilli, Confidential Examiner, Office of Internal Audits
Jean Saint-Preux, Confidential Examiner, Office of Internal Audits
Kiho Park, Associate Executive Director, Queens Health Network
Aaron Cohen, Chief Financial Officer, South Manhattan Health Network
Timi Diyaolo, Controller, Bellevue Hospital Center
Rolando Caldea, Controller, Coler/Carter Specialty Hospital & Nursing Facility
Daniel Frimer, Controller, South Brooklyn/Staten Island Network
Edie Coleman, Controller, Metropolitan Hospital Center
Zoya Shapiro, Assistant Controller, Coney Island Hospital
Ronald Townes, Associate Director, Kings County Hospital Center

OTHER ATTENDEES
KPMG: Maria Tiso, Partner; Joseph Bukzin, Senior Auditor

DECEMBER 4, 2014
AUDIT COMMITTEE MEETING
MINUTES

A meeting of the Audit Committee was held on Thursday, December 4, 2014. The meeting was called to order at 10:11 A.M. by Mrs. Bolus, Committee Member. Mrs. Bolus stated that Mr. Mark Page, Board Member, is here in a voting capacity. Mrs. Bolus then asked for a motion to adopt the minutes of the Audit Committee held on October 2, 2014 and the minutes for a Special Audit Committee meeting held on November 12, 2014. A motion was made and seconded with all in favor. An additional motion was made and seconded to hold an Executive Session of the Audit Committee.

Mrs. Bolus then turned the floor over to KPMG personnel and asked them to introduce themselves. Ms. Maria Tiso introduced herself as the Engagement Partner and she introduced Joseph Bukzin, Senior Manager. She stated that they were there to discuss the 2014 management letter; they will go through some of the key highlights rather than going through a 50-page document.

Ms. Tiso began with page one which is the opinion. The opinion talks about the review of internal controls and that there were no material weaknesses or significant deficiencies identified in the comments in the management letter. These comments are more a matter of the internal controls improvements or best practices. There was nothing noted that was a material weakness or a significant deficiency. The letter is broken into five sections, which is broken out in the matrix of observations, which gives a snapshot of where the findings fell under. We also have comments relating to Corporate Office, Information Technology, site visits and also added a section about prior-year comments that were cleared and then lastly the industry comments. These industry comments are comments that we have been including in many healthcare organizations and talks about items and issues that are going on in the healthcare industry globally.

Ms. Tiso continued by stating that page three is the matrix of observations. Many of our comments relate to Corporate Office and then some of the comments do relate to some of the networks. Page four begins with our observations; Ms. Tiso then turned the presentation over to Mr. Bukzin.

Mr. Bukzin saluted everyone and said picking up on page four, starting with some of the corporate observations. The first one relates to the External Financial Reporting Package Review. As part of the bond obligations, the organization is required to file their financial statement publicly online on a quarterly basis, and the recommendation is to make sure that the financial statement gets published quarterly; it is also reviewed and compared against what was approved during the Finance Committee and Board-level meetings. Management agrees to implement the control around that process. The next one is Accrued Expenses – with tight regulatory requirements and in the spirit of quarterly reporting, it makes sense as a best practice to make sure that the accruals are adjusted more frequently than annually, perhaps on a quarterly basis. Management has agreed to revisit the process for accruals to ensure that they are.

Mr. Page asked if it is realistic to try to do that on quarterly basis?

Mr. Weinman answered stating that currently in Central Office we take care of most of the quarterly adjustments because we must report quarterly expenses coming out of Central Office, but we are talking from the facility standpoint. Most of what they purchase is OTPS, supplies and services; we think it is realistic that we could accomplish this on a quarterly basis.

Mr. Page then asked if they are also reporting on the revenue side? To which Mr. Weinman responded yes.
Mr. Page asked if your accruals on the revenue side were working? Ms. Zurack answered that we do that now quarterly. Mr. Weinman added that a very large part of the audit's concentration is on the revenue, and we do that quarterly and is reviewed extensively by the end of the audit. Part of their opinion is based on the fact that we recorded appropriately.

Ms. Zurack stated that if a facility is following our standard operating procedures, when a good is received, it should be logged into the OTPS system, so that accruals should be almost automatic. It is about services, and there is not much of that going on.

Mr. Bukzin continued to page five and stated that the next comment is a repeat from the prior year regarding affiliation contracts, and there is a whole host of bullets that were carried over from the prior year management letter. Management has continued to work towards and implement policies and procedures to remediate and address these bullets. It is not fully remediated at this point, so we felt it was necessary to continue to carry it forward.

Mrs. Bolus asked about the incomplete human resources files where they do not have the letters from people who are exiting HHC.

Ms. Tiso said that this comment was the same that was in last year's management letter – it is identical.

Mrs. Bolus asked if they had been more diligent in getting this letters?

Ms. Tiso answered that there have been some improvements, but not enough for it to be taken out of the management letter. The Corporation is working towards it, but it is taking a bit longer to get the comment remediated.

Mr. Bukzin added that there is a 2014 observation that falls under the category of "Affiliation Contracts" and we just wanted to highlight that as something new that falls under this heading. This is the internal audit review of the PAGNY corporate expenses that did not occur but it is required to occur. It is our understanding that management is in the process of working with the PAGNY management team to make sure that the internal audit does occur on a timely basis.

Mr. Page referred back to the documentation of people coming in and out, and asked if we are dependent on the affiliate to produce that information, or is that something we do internally for individuals that we pick up through the affiliation?

Mr. Nelson Conde was asked to approach the table by Mr. Martin. Mr. Conde responded that we are dependent on the affiliate to produce the documentation for us.

Mrs. Bolus stated that she has come across this in two years and asked why it cannot be cleared up and why is it still such a problem that it has to appear in the letter.

Ms. Zurack asked if this is KPMG's direct finding? To which Ms. Tiso replied no, this is a comment that was issued in last year's management letter, and it was a sample of affiliates, so it is not just one affiliate. It was a sample that we have taken from last year.

Ms. Zurack then asked what audit work did they do to check to see whether it was cleared.

Mr. Bukzin replied that we work with Mr. Weinman and his team to understand the status of the prior-year comments. Ms. Zurack asked what did that work consist of? Mr. Weinman answered that generally, in response to a prior year's audit comments, we give an opportunity for those comments to provide some type of support of remediation for that comment. If we do not get any type of proof of remediation, it still appears on the letter. We still have an opportunity to clear this for next year, but we do not have any support yet.

Ms. Zurack asked in this particular comment, who did we solicit that opportunity to show the remediation, to the affiliates or to ourselves?

Mr. Weinman answered to us. Ms. Zurack then asked to which office? Mr. Weinman responded generally to the Office of Professional Services & Affiliations.

Mr. Martin asked who is responsible? Ms. Zurack stated that she thinks that Mr. Weinman is saying is that probably someone on my team went through all the comments and sent a note to someone on each area of responsibility to say, "If you cleared this up, show us," and OPSA would have gotten this one, not the facilities themselves. Maybe Mr. Conde has to do some homework and let us know what happened, but whatever you guys provided is not addressed.

Mrs. Bolus said that we have a lot vacancies, sometimes three to four month vacancies, and what offers are being made, then when people resign; we need to know why they are resigning.

Ms. Zurack suggested that we should come back to this, because it is such a long comment that probably Mr. Conde and his team had so much to answer that this one item may be on memory. We are still talking a lot about the recalcs and everything else and maybe this one had not been highlighted as important.

Mr. Bukzin continued with the next comment on page eight entitled Capitalization of Software Costs. This is an accounting treatment relating to computer software upgrades, major electronic medical records systems and costs incurred that may or may not meet the definition of expense versus capitalization. There were about $5 million of expenses that were reported as expense that should have been capitalized. Since the electronic medical records system is a significant ongoing project with a lot of expenses attached to it, we felt it was appropriate to recommend review of this area as well as working with the IT Department to capture payroll-related expenses as well.

Mr. Bukzin stated that the next comment titled Centralization also falls under the category of a best practice of revisiting certain functions that currently are not centralized. We do acknowledge that management has started centralizing certain functions, such as the procurement function, but perhaps there are also other areas for opportunity, and that opportunity could enhance controls, reduce costs to the organization, and promote cross-functionalization amongst employees.

Mr. Bukzin moved on to page nine, Vendor Listings – this is a new audit procedure that we did just to basically compare who was on the vendor master listing file to a listing of active employees, and we did identify some employees that were on the vendor master file. Our recommendation is for management to enhance controls of policies and procedures to ensure that when someone is hired that they are removed from that vendor master list on file. On page ten, Account Analysis Received from Other Departments, this is actually the subset from what we detailed when we presented the results of the financial statements. We only highlight a number of post-closing adjustments, one is related to the double accounting of an accrual for asbestos, pollution remediation liability. Then there was also a cut-off issue related to pool rather than for net patient services by account $100 million. This comment gets to the point of making sure there is a default review of analysis received from other departments that falls into the lap of the finance team. Page eleven has one of our IT-related findings around timely removal of

terminated users. There were two findings under the subcategory related to access perhaps after the employee was no longer employed by the organization. There should be tightened controls and processes between HR and IT process to make sure that the removal of employee occurs on a timely basis. This is a comment we see at many organizations, making sure there is not a huge issue related to these particular findings. We do look to see if terminated employees did access the system after their termination date, and there were no instances of that.

Mr. Bukzin continued with page twelve stating that it covers some of the site-visit findings or findings relevant to a specific entity. The first one relates to a finding at the Coney Island Hospital where there was a fixed asset that was marked as received and accrued for when in fact the facility did not have possession of it. This was somewhat of an isolated instance around Super Storm Sandy, and they did actually have possession of it, but the vendor took it back for safeguarding and safekeeping during the process. Ongoing communications enhancing policies and procedures around vendor payment and when assets are returned or perhaps not been received yet. Bottom of page twelve, Goldwater Movable Equipment Disposal – not material to the financial statements, but there were some assets that were transferred as part of that closure transaction that were not accounted for. This is an opportunity for enhancing policies and procedures and communication in that area.

Mr. Bukzin stated that page fourteen covers the prior-year comments that were addressed by management. These are comments that appeared in last year's management letter that were considered remediated or addressed by management. The first one falls under the heading Construction Management. There were several observations around construction progress, monitoring budgets, over-runs, making sure that items that are construction in progress (CIP) are properly accounted for and captured in a general ledger system. Management has gone through a process of implementing tools to track it. They mentioned a Scorecard Tool, which helps to identify scope issues and if there is going to be over-runs issues with the initial budget that was established for that project and they did provide to us to review as part of the remediation of this comment.

Mr. Bukzin continued with page fifteen, Material Management and stated that again, there were a handful of observations related to segregation of duties, related to receiving, paying and ordering goods. Management has implemented and adopted new procedures to ensure that there is segregation of duty between receiving and payments, approval process, and also the Office of Internal Audits plans to do a more detailed review of this area in connection with the centralized procurement function. The other observation relates to cut off of expenses and reporting of grants. We did not identify any similar issues related to that area in the current year, and management has offered a process of training its employees, making sure there is a verification review process in place to ensure those expenses are reported in the proper period in accordance with the grant management. On page seventeen, there are some prior-year site-visit findings around payroll and material management. These policies and procedures have been adopted and enhanced and we did not have any similar findings in the current year related to these.

Mr. Bukzin asked if there were any further comments at that point. He turned the presentation over to Ms. Tiso.

Ms. Tiso continued with page nineteen through thirty-one and stated that these are industry comments. These comments are specifically included in HHC's letter as information only and we do not include them in other health organizations. The first is Internal Audit Reporting – the best practice is that the Chief Internal Auditor should report to the Chief Executive Officer or the Chief Financial Officer. He currently reports to the Chief Operating Officer, so best practice is to change the reporting structure. The organization is currently looking into that. Page nineteen also talks about the DISRIP Program and page twenty talks about Convergence in Healthcare. To me they are similar comments, right now healthcare is transforming, the organization needs to merge and affiliate with other organizations and converge going forward.

Mrs. Bolus asked if DISRIP pays for any IT systems? To which Ms. Zurack responded that DISRIP does not pay capital. However, New York State in tandem with DSRIP has appropriated $1.2 billion for capital, but it is possible there could be some IT. That application is going kind of parallel to DSRIP and it is due the third week of February.

Mr. Martin added that yes, but that $1.2 billion is over a seven-year period. Ms. Zurack commented that that is for the whole State.

Ms. Tiso moved on to page twenty-four which talks about the ICD-10 extensions approved by the Senate. Obviously, the ICD-10 diagnostic and procedure codes need to be implemented over the next several years. The effective date was supposed to be October 1, 2014, but that has been extended. Our comment here is just to make sure that the organization is currently on track to implement the ICD-10 when the date gets approved. Page twenty-four and twenty-five and the top of page 26 talk about HIPAA compliance. There is a lot of discussion about protecting patient health information and making sure that your corporate compliance program addresses that, looking at subcontractor agreements and vendor agreements, making sure that those parties are also protecting the patient information. I know that HHC does a good job with that because KPMG gets forms to complete. Page 26 talks about data analytics – this is top-of-mind on all governance committee meetings now. A lot of people do not understand how to use them at this point, but going forward, this really needs to be looked at by the organization to figure out how to decrease expenses and increase quality. Page twenty-seven is social media. Our comment is to make sure that the organization has a plan in place to address any social media risk. Page 28, Use of Cloud Computing in Healthcare – healthcare in general is lagging behind on the use of cloud computing. Our comment is that healthcare organizations could really reduce costs as it relates to data storage. Page 29 talks about Oversight – there is a lot of oversight, the SEC obviously is involved in not only public companies but also government entities, bond offerings, municipal examinations. This comment is about the fact that the SEC is not only monitoring public accounts but also private and governmental accounts as well. Page thirty, the Sunshine Act, CMS requires any manufacturing or group purchasing organizations to have a list of any physicians that gets any type of payments or gifts. There needs to be a listing and Corporate Compliance probably needs to make sure physicians, or they are looking at conflict-of-interest statements, making sure those are completed accurately, making sure there are no surprises from the Corporation's perspective.

Mr. Page asked in terms of this latter section of the letter, is this something generic to your healthcare clients? Ms. Tiso responded yes.

Mr. Page then asked if they include this section in your management letters to all of your audit healthcare clients. Ms. Tiso answered yes, we typically do. Our management letters are broken out into the actual facility observations and the industry. The reason we do that is because the management letter is supposed to go to your governing body, and it is to keep them aware of what is going on.

Mr. Page then commented that it seems off as a vehicle because it strikes me as quite different in its substance from your client-specific comments. I am surprised that it is in the management letter, it is valuable and it is good that you give it to us.

Ms. Tiso added that historically it has been; we have had one-offs where the organization does not want it and we will issue a separate letter. It depends upon what you like. I prefer to put it in there, it gives everybody one place to look at the comments.

Ms. Zurack added that in other years you have told us how we are doing relative to others on some of those areas and it is helpful.

Mrs. Bolus asked for a motion to approve the management letter, it was seconded and approved by the Committee.

Mrs. Bolus said thank you very much, very complete and we will follow-up. Mrs. Bolus then moved on to the next item on the agenda, Mr. Telano.

Mr. Telano saluted everyone and stated that page three of the briefing summarizes the status of the audits being conducted by government agencies. The first one is the audit of the Lincoln Affiliation Agreement conducted by the New York City Comptroller's Office. It began last July 2013, and it is still ongoing. They are currently conducting interviews and obtaining information from the PAGNY side of the audit. The second audit is related to the Patient Revenue and Accounts Receivable. At this point in time they are attempting to request information that we consider protected health information, Mr. Russo and Mr. McNulty have been involved in the discussions with them because we do not want to provide this confidential information. This is an ongoing matter and we will keep you updated. On page four is the Bellevue Hospital's Emergency Operations Plan. The City Comptroller's Office has decided to close that audit at this time, but they reserve the right to reopen it at a later date. The next audit listed is one being done by the State Comptroller's Office, a follow-up of overtime and that is ongoing. We have sent them additional information this week and we hope to receive some status of the findings shortly.

Mr. Telano continued on with page five which lists the audits that the Office of Internal Audits has completed since the last meeting. Coincidentally, all of the audits for this meeting are of the South Manhattan Network. The first audit is of Hospital Police at Bellevue. Mr. Telano asked the representatives to approach the table and introduce themselves. They did as follows: Joseph Sweeney, Director of Hospital Police at Bellevue; Kirk Leon, Director of Corporate Security; Mr. Steven Alexander, Executive Director of Bellevue.

Mr. Telano stated that during the course of the audit, we evaluated the payroll and use of resources. We noted that security posts were not always regularly manned. On two specific dates, we found that 6 of the 27 posts were vacant. We also noted that extensive amounts of overtime were being earned by the Hospital Police, and additionally we found that the Bellevue Police was borrowing personnel from other sites and this expense was not always charged back.

Mr. Sweeney said that we have some posts assignments that are mandatory 24 hours a day, 7 days a week; there is no reason that the person assigned to that post should leave the post. However, we have many posts that may be covered all day except when that person is called to an emergency situation and some are left for meal or breaks. The people on the post are responsible to escort somebody out of the building or to our CPEP. There are variety of reasons why somebody might not be on the post that they assigned to.

Mr. Alexander added that on some posts there might be two people assigned, and that would be considered two posts for two individuals, so one person who had to respond to an emergency did not leave that particular post totally uncovered. It was basically reduced from two one person on that site at that time.

Mrs. Bolus asked how often you actually walk through the actual stations.

Mr. Sweeney responded not as often as I probably should. We do rounds maybe once every two weeks or so, but I will visit each post in the different course of my business a couple times a week.

Mrs. Bolus asked if there is any way that they may know what your schedule is. To which Mr. Sweeney responded no. I have many other supervisors that their job is to randomly go to these posts and the uniformed supervisors are mandated to go to the post at least twice a shift and they are supposed to sign their books, so we have a process to make sure that these folks are on the posts.

Mr. Martin added that we need to make a differentiation between the mandatory posts and the sort of posts that are good to have. Twenty-seven is a tremendous amount of posts to have any facility. They are operating at an overabundance of caution when they have 27 posts. I want the Board to feel comfortable that the mandatory posts, the ones that really protect the security of the facility are being manned on a consistent basis.

Mr. Page added that obviously the underlying point is you hope that the personnel you are paying for to man the posts are actually doing that as opposed to doing something else.

Mr. Sweeney stated that that is the concern, but I can assure you that it is busy enough that everybody is doing something at one point or another. I am confident that nobody is disappearing from the post and sleeping somewhere or off somewhere doing something they are not supposed to. If they are off the post, it is for a specific reason and we are on top of it.

Mr. Telano then asked about the overtime and the use of personnel from other facilities?

Mr. Sweeney responded that one of the issues we are consistently trying to address is mandatory overtime for my staff. I want people to want to stay at the hospital. The difference between somebody who wants to stay and somebody who is told they have to stay is quite stark. In an effort to reduce mandatory overtime, we had to set up a system that we can get folks from other facilities who are interested in working overtime to cover these posts. It has been an effective program – it helps, especially on weekends, fill some slots that would normally have to keep somebody from going home. The way the process was being set up, I worked with Payroll and Finance to figure out how we can do these charge backs and we keep separate time sheets. We keep overtime sheets and we send all the documentation to the facility where the person comes from and that facility then pays that person and is supposed to charge us back. One of the findings in the audit was that Bellevue did not always know what needed to be collected because the burden is supposed to be on the facility that pays that employee. We are now going to give copies of what we collect as far as overtime hours and pay that directly to our client so that they know what bill is coming. The part of getting the people paid from their facility was working. It is that facility charging Bellevue back for that overtime was the lag in how long they let that slide.

Mrs. Bolus asked if they would rather have 17 full time employees as opposed to paying overtime equivalent to 17 full time employees.

Mr. Sweeney responded yes, absolutely. That is a complicated answer because the process of hiring a special officer is a cumbersome one. It is a civil service position and they have to take a test. We have to have hiring pools and there is a lengthy process to vet those who are on the list that would eventually be candidates in the approval for the facility to actually choose their candidate that they want to hire and some point they have to do to the academy.

Mrs. Bolus asked how many vacancies are there at this point.

Mr. Alexander answered that we opened ten positions for hire about year ago and in the course of vetting individuals to bring them on board, some of the people leave, so we are trying to stay ahead of that. We opened another ten positions recently, anticipating that it is a bit of a protracted process to get people through to make sure we have the right qualified hospital police that can perform appropriately; we are basically going with an understanding that this is going to take nine months. I need to float the positions well in advance so that I always have a flow of people coming in. In order to get ahead of it, we had to advance that process a little more than we had in the past. For example, this last year those ten positions that we were successful in getting, they just finished the academy a couple of weeks ago

and since then we lost an additional six. This is the kind of attrition we are dealing with. I guarantee that those few people that just came out of the academy who will for a variety of reasons will not be here in six months.

Mrs. Bolus asked if he knew why? Mr. Sweeney said that some of it is they go to other City agencies, Corrections, NYPD or they are interested in law enforcement. Most of them leave for greener pastures or something.

Mrs. Bolus asked if you ask them to exit? Mr. Sweeney responded yes, that some of them do not work out. There is a probationary period and we want to weed that out at the front end rather than call in sick and have a problem on your hands.

Mrs. Bolus pointed out that this should be on our list of vacancies. It is very important, we should ask about the police department too.

Mr. Martin stated that he thinks that is a great point. When they talk about the protracted time it takes to bring somebody on. The academy only operates three times a year, so if you select somebody, you have to wait for the next academy session to put them in. It is not just HHC, it is other agencies, and you need a full list of a certain number of people for the academy to actually occur. It is difficult, but we will put it on the QA.

Mr. Page stated that it is a test, but it is a training period that you provide. Mr. Sweeney explained that after you go through the test process and you are selected as a candidate and Bellevue hires you, and so do the other facilities, they go through the same process. Then at some point, when there is enough vacancies filled, they go into an academy class, which is six weeks, plus an additional week for specific HHC training.

Mr. Page added that the training has a certain value to other employers. Mr. Sweeny said yes.

Mr. Page asked if you can get some kind of commitment from candidates for whom you provide training that they continue working for you for a year or something? Mr. Sweeney said that they all say they will.

Mr. Page asked if you can make it stick? Mr. Russo responded that they are collectively bargained, and any additional requirements we have to pose, we have to bargain with the unions.

Mr. Leon said that it should be noted that we have our own specific test for HHC, and there is also a citywide exam as well so we prefer those who are taking our test remain with us, but unfortunately, as Mr. Sweeney said that does not always happen, so we have to bargain, deal with other agencies.

Mr. Bolus asked how much does academy cost? To which Mr. Leon answered that prices varies depending on the number of candidates that we have. They do a per-person per number of days and then a proposal is sent. The proposal is looked at very carefully based on a number we have, it is anywhere from $50,000 to $80,000 per class.

Mr. Page asked what the cost of one of those positions is. Mr. Sweeny said that is somewhere in the high $30s, after a few years it goes up to $42.

Mr. Martin said that we have found is that the training they receive at the academy is very generic because they want to make it really applicable to all City agencies so Mr. Leon has added HHC-specific training because we have some unique situations within HHC that our hospital police have to refer to.

Mrs. Bolus asked if they are on salary from day one. To which Mr. Sweeny responded that as soon as they step into the academy. Bellevue folks are paid by Bellevue. Some of the directors and I have talked about perhaps maybe doing more of our own type of academy so we could have that HHC influence from the very beginning.

Mrs. Bolus asked if they would be certified and will this education then go from whatever hospital to hospital? Mr. Sweeney responded yes. Then Mr. Bolus asked if they would be paid a different salary at some places or the same salary? Mr. Sweeny said that within HHC it is all the same. People do transfer from different facilities.

Mr. Page asked if they would see value in trying to run this resource more broadly than just hospital to hospital. Mr. Sweeney responded yes.

Mrs. Bolus asked if there is any value in centralizing it. Mr. Alexander answered that there are some differences from facility to facility, there are some cultural things. Some of the basics of how you approach a patient and things like that would be the same, but there is a little bit of a learning going from Kings to Bellevue to Elmhurst.

Mr. Telano stated that he had additional comments related to Bellevue. There was licenses and certifications that we could not locate, and as a result we could not confirm that the security officers, the special officers and the watch persons, were properly trained or that they were authorized to perform the job that they were in.

Mr. Sweeney stated that they used to have a notification process and is not sure where that fell off. Locally it was not part of our responsibility to keep track of that, but the issue came up when the auditors were there and frankly I did not know the answer, so we started looking into it. The special officers are 100% compliant. It took us a while to track down the certification for about 11 of them, we verified they had certification. The watch persons' licensing, we had one person who was not up to date and they were previously relieved of duty until they get their certification back, so that is 99% personnel compliance. I think it was more of a bookkeeping error than actually certification.

Mr. Telano moved on to page six. We found confiscated patient items that are deemed harmful to patients or others that were not being properly disposed of in a proper period of time. There were no guns, but there were knives and screwdrivers.

Mr. Sweeney said that that is a challenge for us. We have had some historical issues with what is valuable to me might be different to you. The patients come in with items that we do not want them to have, and typically it is when they enter our CPEP. We do not want to give it back to them because it is something that they can hurt themselves with or somebody else regardless of whether they have been treated and released. In doing that they ended up with a collection, we revamped that process; we have a couple of things to iron out as well with the sharp objects. A lot of the stuff we will discard if it is obvious it is just garbage and dangerous, but the stuff that is dangerous and may not be garbage maybe somebody's personal property we hang on to. We are going to transfer that stuff over to our property office for disposal so that it is all documented. Some of the stuff we had around is because we do use it for training purposes to show new coming officers what they might see out there as far as taking stuff off, but we sort of cleaned that up as well.

Mr. Telano continued by stating that during the course of the audit there was the lack of use of the HHC custom-built Hospital Police Incident Reporting system and asked them if they were now utilizing it.

Mr. Sweeney responded yes, that that was bad timing. We had just gotten it and there was a bit of a learning curve. A lot of folks were not used to using the Group-wise, so we have been training them and it is working much better.

Mr. Telano moved on to the next audit regarding nursing employment agencies at Coler and Bellevue and stated that it should be noted that this was not an audit as much as it was a request by the Chief Financial Officers at both sites. He asked the representatives to approach the table and introduce themselves. They introduced themselves as follows: Aaron Cohen, Chief Financial Officer of the South Manhattan Network; Robert Hughes, Senor Executive Director of Coler and Henry J. Carter; Manuela Brito, Chief Financial Officer of Coler and Carter; Leah Matias, Chief Nurse of Coler and Carter.

Mr. Telano stated that the objective of this audit was to ascertain if nurses who work for both HHC and employment agencies, they are called recycled nurses, were not being paid by both parties for the same hours worked. At Coler we tested 12 recycled nurses and we found that 10 were paid for overlapping hours, and at Bellevue we reviewed about 50% of the sample. There were over 80 recycled nurses, we reviewed 43 and there were only 6 in which they were double paid. We also found some issues in which log sheets were missing and one or two instances in which people were overpaid for a certain number of hours.

Mr. Cohen said that we became aware that there problems and we called Mr. Telano and his folks to come in and they did a very thorough review. Some of the problems that we had discovered they obviously agreed with, and they made a series of recommendations and we agreed with all of the recommendations that they made and we are in the process of implementing all the recommendations. We are very pleased, if one can be pleased about something like this, in terms of them coming in and sort of reinforcing what we saw was happening and coming up with a very useful, helpful report, and we also appreciate the comment at the very end of the audit that the Nursing Director has been very helpful in making changes to make sure that this does not happen. We should mention that this is a consolidated function. Payroll is a consolidated function in the South Manhattan Network. We are physically located at Bellevue for all of the facilities in the network. The timekeepers are at the individual facilities.

Mr. Hughes commented that Mr. Cohen summed it up as far as how this unfolded and Mr. Telano's office had been requested to come in. We have locally at Coler and Carter put a moratorium on using recycled nurses to do overtime. They are not able to do agency, as a way to prevent this from recurring again until we can take the time and put into place a process, a system that will give us the safeguards to prevent this type of abuse from happening again.

Mrs. Bolus said that the one I have the most problem with was the Bellevue nurse who was suspended without pay and yet actually worked that day – could not understand that one.

Mr. Cohen said that it is a significant problem, and we have put things in place with Nursing so that it cannot happen again.

Mr. Telano continued with the last audit which is at Coler, Employee Salary Changes. Overall the findings have to do with record-keeping deficiencies and a lack of a verification process, and as a result, employees were sometimes overpaid or underpaid and sometimes when they were doubled paid, it was not reversed on a timely basis. We also found some inefficiencies in the manner in which they enter items into PeopleSoft, and we also noted that personnel requisition forms were not always fully approved by the required individuals.

Mr. Cohen stated that the first finding has to do with duplicate payments of employees and it is a little bit misleading. When an employee first comes on to the payroll system, sometimes it takes a few payroll cycles, and as a result, we issue advanced checks. What is supposed to happen is once a person gets on payroll, you are supposed to eventually deduct what they have already been paid. In this case that was not happening as timely as it should have been happening. Eventually it was, it is not that it does not get done. It just should be done sooner as opposed to later. The other issue relates to the fact that there were some errors made, and the recommendation by Internal

Audits is that we use a scanner; we have a scanner at Bellevue, but not at Coler. Three years ago we requested from the Contract Review Committee that we wanted additional scanners and we were turned down twice. We will bring Mr. Telano to the next meeting of the Contract Review Committee. The scanner is important because there are too many manual things happening in this process. Once you have a scanner, then the manual things that you have to do are much more limited. In the interim we are now bringing the Coler time sheets to Bellevue to be scanned to make this work better. Our network has the most employees, which is why we need additional scanners.

Mr. Page asked how many scanners are you talking about? Mr. Cohen responded that we have one right now. We asked for two more and we were turned down.

Mr. Page asked if this kind of thing you buy from your local store on Broadway. Mr. Cohen answered that it is a bigger deal than that. It is one for HHC's payroll system and probably each network has one.

Mr. Page asked if it is literally wired into the payroll system? Mr. Cohen answered that that is correct.

Mr. Martin stated that he was not aware that they had come and he will speak to the Senior Vice President of the network to make sure that happens.

Mr. Telano then continued and stated that on page nine of my briefing is the audits we are currently working, and on page ten is the status of our follow-up audits and if there are no further comments or questions, I conclude my presentation.

Mrs. Bolus then turned to Mr. McNulty for an update of Corporate Compliance.

Mr. McNulty saluted everyone and began his update on page three of the Corporate Compliance Report (the "Report") by discussing the HHC Compliance Program Certification. Mr. McNulty informed the Audit Committee (the "Committee") that under the Social Services Law and its implementing regulations, HHC is required to annually certify, establish and maintain an effective corporate compliance program aimed at detecting fraud, waste and abuse and to put in place a system of controls to deter and detect fraudulent and criminal conduct. Mr. McNulty explained that to be an effective compliance program, the compliance program must cover the following seven key core areas: (i) billings; (ii) payments; (iii) medical necessity and quality of care; (iv) corporate governance; (v) mandatory reporting, such as overpayments; (vi) credentialing; and (vii) other risk areas that are or should be with due diligence identified by HHC.

Mr. McNulty further explained that an effective compliance program must also consist of eight elements and continued by listing seven of the eight elements: (i) the development of written policies and procedures on corporate compliance issues that include a code of conduct and a code of ethics; (ii) the designation of a chief corporate compliance officer; (iii) the development of a training and education program on compliance issues; (iv) the establishment of direct communication lines between the corporate compliance officer and the workforce members throughout the organizations including the establishment of a toll-free hotline; (v) the implementation of a system designated to routinely identify risks; (vi) the establishment of a system to respond to compliance issues as they are identified: and (vii) the creation of a policy that prohibits the intimidation or retaliation of individuals who participate in the compliance program in good faith.

Mr. McNulty continued by discussing the certification program further. In summary, he stated that every year the Office of Corporate Compliance ("OCC") has to certify through the Office of the Medicaid Inspector General's ("OMIG") website that HHC has an effective corporate compliance program. In summary, he stated that the certification is performed by the President and Chief Executive of the Corporation, Dr. Raju, advising that the certification would be

performed at the end of December. He informed the Committee that documentation of the eight elements must be kept. He stated that the eight elements may be audited by OMIG. In summary, he added that, because OMIG generally audits a handful of hospitals throughout the State every year, OCC maintains documentation that HHC satisfies all of the elements.

Mr. McNulty continued to page four of the Report and updated the Committee on the previously reported data breach at the East New York Diagnostic Treatment Center ("East New York"). He reminded the Committee that the subject breach occurred when medical records were stored in an employee garage in East New York, stating that these records came from five previously closed clinics. He informed the Committee that breach notification was provided to the 10, 058 affected patients, as well as the Office of Civil Rights of the United States Department of Health and Human services. In summary, he stated that notice of the breach was provided on HHC's website and to major media outlets throughout New York State. He informed the Committee that the cost of the breach to provide patient notification and credit monitoring and identity theft services to all affected patients totaled $53, 376.

Mrs. Bolus asked who that is charged to? Mr. McNulty responded that it comes from the OCC budget.

Mrs. Bolus asked that if the breach occurred at East New York, why is it then you have to pay for it. Mr. McNulty answered that historically we handle the data-breach vendors, and therefore we respond to data breach and we make the evaluation of the types of services that have to be provided to the patient because it is not every HIPAA incident that results in actual breach that we would have to provide these notifications, so historically it is budgeted every year that we have a certain amount of money allocated to respond to data breaches.

Mr. Page asked what is our obligation to maintain records when we close? Mr. McNulty said that when you a close a clinic, you have to establish a facility closure plan with the Department of Health, and the Department of Health outlines where those records should go and how they should be stored. In this particular process, that was not followed when this facility closed. We have to store depending on the type of records. If a record is related to a minor, we have to keep them until the minor is 21 years old. If it is a record pertaining to any other patient, we have to keep it six years. If it is a record that was dealing with the billing of Medicaid or Medicare, we have to keep it for ten years.

Mr. Russo added that generally, the closure plan focuses on two things: one, transition of patients to another setting and two, the maintenance of records.

Mr. McNulty continued by advising the Committee that, in addition to the closure plan, a procedure was developed that the facility executive directors must now follow. He stated that the procedure should be out by the end of the month, and it designates a specific person who would be responsible to make sure the records get from point A to point B, explaining that, in sum and substance, the records would either go to the facility medical records department or to HHC's offsite vendor, City Storage. He advised the Committee that he would be personally visiting all of the diagnostic treatment centers, citing that in the past month he visited Gouverneur, Renaissance, and Belvis by performing a walkthrough of the medical records departments at those sites.

Mr. McNulty moved on to the next item on the Report – the Compliance Reporting Index for the Third Quarter of Calendar Year 2014. He advised the Committee that for the third quarter, July 1 to September 30, 2014, there were 110 compliance-based reports. He noted that one was classified as a Priority A report, 51 were Priority B reports and 58 were Priority C reports. He elaborated that, of the 110 reports, 55 were received by the OCC through its anonymous tell-free compliance hotline. He stated that 19 reports were also received through e-mails, and 11 were through face to face. He added that 11 were received directly through telephone call to OCC. He stated that, with

regard to the different categories of complaints received, the majority, 36 or 32% pertained to policy and process integrity - - mainly violation of corporate OPs or violations of statutes and regulations.

Mr. McNulty continued on to section IV, the Privacy Reporting Index for the Third Quarter, explaining that 29 incidents were reported through the HIPAA Complaint Tracking System. He further explained that, out of those, 12 were found to be actual violations of the HHC HIPAA Privacy Operating Procedures ("OPs") and 13 were found not to be a violation of said OPs. He advised that, out of the 12 that were found to be violations, 3 were determined to be breaches of protected health information, which he informed the Committee he would detail in the executive session. He noted that one of those breaches was the East New York breach that we discussed earlier.

Mr. McNulty moved along to page six of the Report advising the Committee that there were no reports of excluded providers since the last time the Committee convened on October 2, 2014. Mr. McNulty then concluded the Report.

Mrs. Bolus then stated that they going into executive session.

Mrs. Bolus stated that they are back from the Executive Session; they discussed matters that were confidential and related to patient care and quality assurance as well as ongoing investigations.

There being no further business, the meeting was adjourned at 11:43 A.M.

Submitted by,

Mrs. Josephine Bolus
Audit Committee Member

AUDIT COMMITTEE OF THE HHC BOARD OF DIRECTORS

Corporate Compliance Report

February 19, 2015

Table of Contents

Agenda

I. Completion of Compliance Program Certification

Background

1) Pursuant to Social Services Law § 363-d and 18 NYCRR part 521, HHC is required to establish and maintain an effective compliance program that covers the following seven areas: (i) billings; (ii) payments; (iii) medical necessity and quality of care: (iv) governance; (v) mandatory reporting; (vi) credentialing; and (vii) other risk areas that are or should with due diligence be identified by HHC.

Required Elements of an Effective Compliance Program

2) In addition to the above, an effective compliance program must contain the following eight elements: (i) the development of written policies and procedures that, among other things, describe compliance expectations as embodied in a code of conduct or code of ethics, implement the operation of the compliance program, and provide guidance to employees and others on dealing with potential compliance issues; (ii) the designation of an employee vested with responsibility for the day-to-day operation of the compliance program; (iii) the development and implementation of a training and education program concerning the compliance program, its expectations, and its scope of operation - such training and education must reach the governing body; (iv) establishment of direct communication lines to the employee vested with the day-to-day direction of the compliance program that are accessible to workforce members, including executives and the governing body, as well as persons associated with the provider; (v) establishment of disciplinary policies to encourage the good faith participation in the compliance program; (vi) implementation of a system designed to routinely identify, evaluate, and address corporate vulnerabilities and risks; (vii) establishment of a system designed to respond to compliance issues as they are raised and/or identified; and (viii) the creation of a policy that prohibits intimidation or retaliation for the good faith participation in the compliance program.

Certification Completed on December 2014

3) On December 22, 2014, HHC President and Chief Executive Officer Ramanathan Raju, M.D., through the New York State Office of the Medicaid Inspector General's ("OMIG") website, certified that HHC has an effective compliance program. Specifically, Dr. Raju certified that HHC has done the following:

- implemented written policies and procedures that describe compliance expectations which support a compliance program;
- designated an employee vested with responsibility for the day-to-day operation of the compliance program;

- established routine training and education of all affected employees and persons associated with the provider, including executives and governing body members, on compliance issues, expectations and the compliance program;
- provided all employees and persons associated with the provider access to the compliance officer to allow for compliance issues to be reported, including a method for anonymous reporting;
- established disciplinary policies been implemented and enforced to encourage good faith participation in the compliance program by all affected individuals;
- established a system for routine identification of compliance risk areas specific to your provider type and do you conduct audits of those risk areas;
- established a system for investigating and responding to compliance issues as they are raised, including reporting compliance issues to DOH or OMIG and refunding overpayments;
- implemented a policy of non-intimidation and non-retaliation for good faith participation in the compliance program;

II. Completion of Deficit Reduction Act Certification

Background

1) Pursuant to the Deficit Reduction Act ("DRA") of 2005, the New York City Health and Hospitals Corporation ("HHC") is required, as a condition of its participation in the Medical Assistance Program ("Medicaid"), to establish written policies and procedures that inform its employees, contractors, agents, and other persons about the following[1]:

- HHC's internal policies covering the prevention and detection of fraud, waste, and abuse;
- the federal False Claims Act and any similar law under the State of New York that governs false claims and statements; and
- whistleblower protections under federal and State laws.

Overview of HHC's Policies and Procedures Designed to Prevent Fraud Waste and Abuse

2) HHC's policies and procedures designed to prevent and detect fraud, waste, and abuse include, without limitation, the following:

- HHC's Corporate Compliance Plan
- Operating Procedure 50-1 (Corporate Compliance Program)
- HHC's Principles of Professional Conduct

[1] *See* 42 USC § 1396a [a][68][A-C]

- HHC Guide to Compliance at the New York City Health and Hospitals Corporation

HHC'S Corporate Compliance Plan

3) The overall breadth of HHC's Corporate Compliance Program (the "Program") is best reflected in its Corporate Compliance Plan (the "Plan"). Specifically, the Plan outlines and explains the structural and operational elements of the Program, highlighting HHC's development and/or adoption of written policies and procedures covering compliance, including, without limitation, HHC's Operating Procedure 50-1 - Corporate Compliance Program ("OP 50-1"), which details the structure of the Program; HHC's Principles of Professional Conduct ("POPC"), which establishes HHC's prohibition of fraudulent billing and other improper business practices; and HHC's A Guide to Compliance at the New York City Health and Hospitals Corporation ("Guide to Compliance")[2], which provides a summary of important compliance issues and compliance standards and expectations at HHC. The Plan, OP 50-1, the POPC, and the Guide to Compliance may all be accessed through HHC's Intranet under the Office of Corporate Compliance ("OCC") at http://compliance.nychhc.org/, or by way of HHC's public website at http://www.nyc.gov/html/hhc/html/about/About-PublicInfo-Compliance.shtml. You may also contact your local Network Compliance Officer or the OCC - by phone at (646) 458-7799 or by e-mail at COMPLIANCE@nychhc.org - to obtain copies of the same.

The Plan also underscores HHC's commitment to routinely identify potential areas of corporate risks and vulnerabilities, and to perform self-evaluations and audits of its operations and practices, which are required under New York's mandatory compliance program regulations.[3]

HHC Operating Procedure 50-1

4) As evidenced by its internal operating procedures,[4] HHC has implemented a Program that satisfies the mandatory provider compliance program regulations promulgated by the New York State Department of Social Services.[5] Additionally, the Program also adopts the principles set forth in the United States Sentencing Commission 2013 Federal Sentencing Guidelines pertaining to effective compliance and ethics programs. The Program is responsible for, among other things, aggressively identifying, directing, and addressing corporate-wide and local compliance activities and concerns. The following are some key highlights of the Program:

[2] *See* HHC's A Guide to Compliance at New York City Health and Hospitals Corporation (revised: July 2014)
[3] *See* 18 NYCRR § 521.3[c][6]; *see also* HHC's Corporate Compliance Plan (Updated 11/09/11), p.35
[4] *See* HHC Operating Procedure (OP) 50-1 - Corporate Compliance Program
[5] *See* 18 NYCRR part 521

- the appointment of a Corporate Compliance Officer ("CCO") charged with the oversight and implementation of the Program;
- the creation of an annual Corporate Compliance Work Plan ("Work Plan") designed to proactively address compliance vulnerabilities;
- the institution of a confidential process and toll-free hotline (1-866-HELP-HHC) to receive complaints;
- the implementation of corporate-wide training and education regarding corporate compliance issues;
- the requirement that the CCO report, at least quarterly, HHC compliance activities to the Chairperson of the Board of Directors ("BOD"), the Chairperson of the Audit Committee of the BOD, and HHC's President and Chief Executive;
- the requirement that all HHC workforce members report violations of OP 50-1, as well as of all applicable laws, rules, codes and regulations (collectively "Laws"), to the CCO;
- the investigation of allegations regarding: (i) violations of applicable Laws and HHC OP 50-1; and (ii) allegations of intimidation and retaliation; and
- the prohibition of intimidation and retaliation against any person who, acting in good faith, engages in the Program.

HHC's Principles of Professional Conduct ("POPC")

5) The POPC is a guide to direct HHC employees to conduct official business in an ethical and lawful manner. Some examples of violations of professional conduct are:

- improper billing practices;
- accepting gifts from a vendor;
- inappropriate patient referrals;
- breaches of patient confidentiality; and
- failure to adhere to HHC policies concerning patient care.

HHC's Guide to Compliance

6) The Guide to Compliance defines the terms *compliance*, *fraud*, *waste*, and *abuse*. The Guide to Compliance also describes the goals of HHC's Program, the consequences of non-compliance with applicable Laws and internal policies, and the responsibilities of each employee with regard to compliance. In addition to the foregoing, the Guide to Compliance provides information regarding the following compliance subjects:

- federal and State False Claims Acts;
- HHC's policy on retaliation; and
- instructions on how to report a compliance issue.

Certification of DRA Requirements completed

7) Senior Assistant Vice President and Chief Corporate Compliance Officer Wayne A. McNulty certified, through OMIG's website, HHC's compliance with the DRA on December 29, 2014. Specifically, Mr. McNulty certified that HHC has written policies for all employees, including management, and any contractor or agent of the entity, that provide detailed information about the Federal False Claims Act, remedies for false claims and statements, and state laws pertaining to civil or criminal penalties for false claims and statements and that these policies:

- address whistleblower protections under the Federal False Claims Act and state laws;
- address the role of the Federal False Claims Act and state laws in preventing and detecting fraud, waste, and abuse in Federal health care programs; and
- provide detailed provisions regarding the entity's policies and procedures for detecting and preventing fraud, waste, and abuse.

8) Mr. McNulty also certified that HHC has an employee handbook that includes: (i) a specific discussion of the state and federal laws covering fraud, waste and abuse and the False Claims Act; (ii) a specific discussion of the rights of employees to be protected as whistleblowers; and (iii) a specific discussion of the entity's policies and procedures for detecting fraud, waste, and abuse

III. Report on HHC's Compliance with the HIPAA Security Rule Risk Analysis Requirements

Overview

1) Pursuant to Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or the "Act") and it implementing regulations found at 45 CFR Parts 160 and 164, "The Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule") HHC is required to ensure that it implements a risk assessment program the purpose of which is to prevent, detect, contain, and correct security violations affecting electronic protected health information ("EPHI").[6]

[6] "Security Standards for the Protection of Electronic Protected Health Information" (the "Security Rule") found at 45 CFR Part 160 and Part 164, Subparts A and C. was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The HIPAA Security Rule is all about implementing effective risk management to adequately and effectively protect EPHI. The assessment, analysis, and management of risk provides the foundation of a covered entity's Security Rule compliance efforts, serving as tools to develop and maintain a covered entity's strategy to protect the confidentiality, integrity, and availability of EPHI *See also, generally,* 18 NYCRR Part 521.

Security Rule Requirements

2) The Security Rule requires that covered entities, such as HHC, perform periodic technical and non-technical evaluations of applications that access, house or transmit EPHI. More specifically, HHC is required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI that is accessed, stored or transmitted by HHC's systems and applications and is required, at minimum, to conduct periodic technical and nontechnical evaluations of those systems and applications to establish the extent to which HHC's security policies and procedures meet the requirements of the Security Rule.[7]

Performance of Risk Analysis

3) Pursuant to the Security Rule at 45 CFR Section 164.308(a)(1)(ii)(A), HHC is required as to each of its applications and systems that possess EPHI to do the following:

> Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

4) To meet the risk analysis requirements under the Security Rule, HHC is required to conduct an accurate and thorough risk analysis of the vulnerabilities and potential risks to the confidentiality, integrity, and availability of EPHI of each of the systems and applications used by HHC.[8] The required risk analysis is an assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the EPHI held by HHC and the likelihood of that risk's occurrence[9] and its use is considered a foundational first step in identifying and implementing physical, administrative and technical safeguards that comply with and carry out the standards and implementation specifications required in the Security Rule.

5) In its risk analysis of its applications and systems, HHC must (1) demonstrate that it has evaluated the risks associated with a specific application or system that use, store or transmit EPHI; and (2) document that it has established all of the safeguards (technical, physical and administrative) that would reasonably serve to protect the information that is exchanged along its network. [10]

[7] 45 CFR §164.308(a)(8).
[8] 45 CFR §164.308(a)(1)(ii)(A).
[9] 45 CFR § 164.308(a)(1)(ii)(A).
[10] http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2017.html

Conducting and Inventory of Systems and Applications that House EPHI

6) As part of the risk analysis process, is required to, among other things: (1) inventory all systems and applications used by HHC that access and house EPHI; and (2) classify those systems and applications by their level of risk.

7) While it is required that HHC conduct a risk analysis of its applications and systems, there are numerous methods of performing this analysis and the Security Rule does not prescribe a specific methodology that HHC must follow, recognizing instead that methods will vary dependent on the size, complexity, and capabilities of the organization.[11] With regard to performing a risk analysis, there is no single method or best practice that assures compliance with the Security Rule.[12] Notwithstanding this fact, National Institute Standards Technology ("NIST") SP 800-30 provides examples of steps that might be applied to a risk analysis process.[13]

8) Regardless of the methodology used, a risk analysis must at the minimum incorporate the following eight steps to satisfy the Security Rule: (i) identify the scope of the analysis; (ii) gather data; (iii) identify and document potential threats and vulnerabilities. (iv) assess current security measures; (v) determine the likelihood of threat occurrence; (vi) determine the potential impact of threat occurrence; (vii) determine the level of risk; and (viii) identify security measures and finalize documentation.[14]

HHC's Compliance Status with Security Rule Risk Analysis Requirements

9) With regard to HHC's compliance with the Security Rule risk analysis requirements, the OCC has found, in pertinent part, that: (i) the inventory of the HHC information systems and applications that access, house, or transmit EPHI is a work in progress and therefore is not comprehensive at this juncture; and (ii) although HHC's Enterprise Information Technology Services ("EITS") has taken numerous and significant measures to enhance and maintain the confidentiality, integrity, and security of HHC's information systems including the formation of an information governance and security program, the implementation of security controls, and the performance of a formal risk analysis on a handful of its applications, it appears that further

[11] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
[12] Department of Health and Human Services Office of Civil Rights ("OCR") Guidance on Risk Analysis Requirements under the HIPAA Security Rule found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf accessed on 2/9/15.
[13] National Institute of Standards and Technology (NIST), is a federal agency that publishes guidelines relevant to the HIPAA Security Rule. *See* NIST 800 Series of Special Publications (SP) – specifically, SP 800-30 - Risk Management Guide for Information Technology Systems at http://www hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance html. . Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI.
[14] OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule, *supra*, note 31.

measures must be taken by EITS to fully satisfy the extensive risk analysis and implementation measures required under the Security Rule.

Recommendations

10) Based on the foregoing, OCC is recommending that the following measures be taken by HHC's Enterprise Technology Information Services:

- Identify and inventory, as a priority and no later than within 30-days, all HHC systems and applications that access, house or transmit EPHI;

- Provide a written schedule that will specify date(s), over an 12-month period, by which all inventoried HHC systems and applications that access, house or transmit EPHI will have a completed risk analysis;

- Provide a written schedule that will specify date(s), over a 12-month period, by which all inventoried HHC systems and applications that access, house or transmit EPHI will have been assessed as to the presence of the required implementation standards set forth in the Security Rule;

- Provide a written schedule that will specify date(s), over a 12-month period, by which all systems and applications that access, house or transmit EPHI will have been assessed as to the presence of each addressable implementation standard set forth in the Security Rule or, in the alternative, documentation as to the reason(s) why the addressable specification was not implemented;

- Immediately begin a risk analysis of the top 25 high-risk applications (based on criticality, amount of EPHI, impact etc.);

- Inventory all remediation recommendations resulting from any completed risk analysis and document that the required remediation was completed or, if not completed, provide a date by which remediation was expected;

- Ensure that, regardless of the methodology used to perform the required risk analyses, any risk analysis that is performed consists of and documents the following eight steps:

- Outline the scope of the analysis (including the potential risks, threats, vulnerabilities to the confidentiality, availability and integrity of all e-PHI that HHC creates, receives, maintains, or transmits)
- Collect/gather data (identification of where data is stored)
- Identify and document potential threats and vulnerabilities
- Assess current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of threat occurrence
- Determine the level of risk present
- Document all findings and risk analysis conclusion

- Use a recommended best practice guide when performing a risk analysis to enhance the likelihood of compliance with the Security Rule. Such guides include, but are not limited to, the National Institute of Standards and Technology (NIST) Introductory Resource for implementing the Security Rule[15] and HIPAA Guidance on Risk Analysis Requirements under the HIPAA Security Rule.[16]

Follow up

The findings of the OCC provided above have been communicated to ETIS leadership. At this time, OCC is awaiting management's response to this report, which will be provided by Bert Robles, HHC Senior Vice President, Information Services/Corporate Chief Information Officer.

[15] An Introductory Resource for Implementing the Health Insurance Portability and Accountability Act Security Rule http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf; also see NIST Guide for Technology Systems at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

[16] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf; also see Department of Health and Human Services. "Security Rule Guidance Material." at atwww.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.;
Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health Information; Final Rule." *Federal Register* 67, no. 157 (Aug. 14, 2002). at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-20554-filed.pdf. and
National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995. Available online at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.
National Institute of Standards and Technology. "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." NIST Special Publication 800-66. October 2008. at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

Management's response and remedial steps taken will be presented to the Audit Committee when it next convenes in April 2015.

IV. Compliance Reporting Index for the Fourth Quarter of Calendar Year 2014 ("CY2014")

Summary of Reports

1) For the fourth quarter CY2014 (September 1, 2014 to December 31, 2014) there were 136 compliance-based reports of which 1 was classified as a Priority "A" report, 50 (or 36.8%) were classified as Priority "B" reports, and 85 (or 62.5%) were classified as Priority "C" reports. For purposes here, the term "reports" means compliance-based inquiries and compliance-based complaints. Of the 136 reports received during this period, 68 (or 50%) were compliance complaints received on the OCC's anonymous toll-free compliance hotline.

Mode of Reporting

2) Below is a summary of how the OCC received the 136 CY2014 fourth quarter reports:

- 68 (50%) were received on the Help Line;
- 21 (15.4%) were received via E-Mail;
- 19 (14%) were received via Telephone;
- 12 (8.8%) were received Face to Face;
- 6 (4.4%) were received via Mail;
- 3 (2.2%) were received via Web submission;
- 2 (1.5%) were received via Office Visit;
- 1 (0.7%) were received via Intranet;
- 1 (0.7%) were received via Other;
- 1 (0.7%) were received via referral from other HHC Office;
- 1 (0.7%) were received via Fraud & Abuse Form (e);
- 1 (0.7%) were received via Interoffice Mail.

Allegation Class Analysis

3) The breakdown of the allegation classes of the 136 reports received in the fourth quarter of CY2014 is as follows:

- 23 (16.9 %) Guidance Request;
- 17 (12.5 %) Patient Care;
- 16 (11.8 %) Unfair Employment Practices;
- 13 (9.6 %) Inappropriate Behavior;

- 12 (8.8 %) Falsification or Destruction of Information;
- 6 (4.4 %) Environment, Health and Safety;
- 6 (4.4 %) Disclosure of Confidential Health Information – HIPAA;
- 4 (2.9 %) pertained to Accounting and Auditing Practices;
- 4 (2.9 %) Customer Relations;
- 4 (2.9 %) Retaliation or Retribution;
- 4 (2.9 %) Theft;
- 4 (2.9 %) Harassment – Workplace;
- 4 (2.9 %) Misuse of Resources;
- 3 (2.2 %) Conflict of Interest – Personal;
- 3 (2.2 %) Disclosure of Confidential Information;
- 2 (1.5 %) Fraud or Embezzlement;
- 2 (1.5 %) Billing and Coding Issues;
- 2 (1.5 %) Other;
- 2 (1.5 %) Quality Control;
- 2 (1.5 %) Threats and Physical Violence;
- 1 (0.7 %) Conflict of Interest – Financial;
- 1 (0.7 %) Gifts, Bribes and Kickbacks;
- 1 (0.7 %) Quality Control – Medical.

V. Privacy Reporting Index for the Fourth Quarter of CY2014 (October 1, 2014 to December 31, 2014)

Incident Reports and Investigations (Fourth Quarter 2014):

1) During the fourth quarter of October 1, 2014 through December 31, 2014, thirty (30) complaints were entered in the HHC HIPAA Complaint Tracking System, an HHC proprietary database. Of the 30 complaints entered in the tracking system nine (9) were found after investigation to be violations of HHC HIPAA Privacy Operating Procedures; six (6) were determined to be unsubstantiated; eleven (11) were found not to be a violation of HHC HIPAA Privacy Operating Procedures; and four (4) are still under investigation. Of the nine (9) confirmed violations, seven (7) were determined to be breaches and two (2) were determined not to be a breach. A total of seven individuals were affected by the seven confirmed breaches.

Confirmed breaches (Fourth Quarter CY2014):

2) Below is a summary of the confirmed privacy breaches for the fourth quarter of 2014.

- Metropolitan Hospital – May 2014. This incident at hand was a late entry into the tracking system and involved an employee verbally disclosing the protected health information ("PHI") of a patient (who was also an HHC employee) in the presence of

other employees and hospital visitors in a public area. Breach notification was sent to the affected patient in January 21, 2015.

- Woodhull Medical Center – October 2014. This incident involved the unauthorized disclosure of PHI to an unauthorized recipient patient. The recipient patient received the discharge documents belonging to another patient. Breach notification was sent to the affected patient on December 16, 2014.

- Jacobi Medical Center – October 2014. This incident involved the unauthorized disclosure of PHI to an unauthorized recipient patient. The recipient patient received a prescription belonging to the affected patient. Breach notification was sent to the affected patient on December 24, 2014.

- Jacobi Medical Center – October 2014. This incident involved the unauthorized disclosure of PHI to an unauthorized recipient patient. The recipient patient received the discharge documents belonging to the affected patient. Breach notification was sent to the affected patient on December 24, 2014.

- Woodhull Medical Center – November 2014. This incident involved the unauthorized disclosure of PHI to an unauthorized recipient patient. The recipient patient received a prescription belonging to the affected patient. Breach notification sent to the affected patient on January 7, 2015.

- Kings County Hospital – November 2014. This incident involved the unauthorized disclosure of PHI to an unauthorized recipient patient. Upon a return follow-up visit to the facility the recipient patient provided hospital staff with documents that included a surgical schedule. The schedule contained the PHI of thirteen Kings patients. The document was recovered by a Kings staff member. Breach notification was sent to all affected patients on January 5, 2015.

- Bellevue Hospital Center – October 2014. This incident involved the unauthorized access of one patient's medical record by numerous HHC workforce members, including residents and nurses. The affected patient was a person of notoriety. Disciplinary action is pending against said workforce members. Breach notification was sent to the affected patient on December 24, 2014.

VI. Monitoring of Excluded Providers

1) The OCC has not received or uncovered any reports of excluded providers since the Audit Committee last convened on December 4, 2014.

VII. April 2015 Audit Committee – Report on Ongoing Compliance Matters

1) In its Corporate Compliance Report in April 2015, the OCC will report on, among other things, the following:

- the status of its revision of Operating Procedure 50-1 (Corporate Compliance Program); the HHC Principles of Professional Conduct; and the HHC Corporate Compliance Plan;

- its review and findings regarding HHC's compliance with HIPAA Business Associate Agreement requirements; vendor management activities; and Center for Medicaid and Medicare Services ("CMS") regulatory requirements for contractors; and

- compliance and privacy training activities and corresponding compliance rates.