AUDIT COMMITTEE
MEETING AGENDA

April 16, 2015

12:30 P.M.

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

CALL TO ORDER — Ms. Emily A. Youssouf

- Adoption of Minutes February 19, 2015 — Ms. Emily A. Youssouf

INFORMATION ITEMS

- MetroPlus – Accounts Payable Audit Update — Mr. Chris A. Telano, Mr. John Cuda, CFO
- Audits Update — Mr. Chris A. Telano
- Compliance Update — Mr. Wayne McNulty

EXECUTIVE SESSION

OLD BUSINESS

NEW BUSINESS

ADJOURNMENT

MINUTES

AUDIT COMMITTEE **MEETING DATE: February 19, 2015**
TIME: 1:00 PM

COMMITTEE MEMBERS

Emily Youssouf, Chair
Josephine Bolus, RN
Jo Ivey Boufford, MD (VIA VIDEO CONFERENCE)

STAFF ATTENDEES

Antonio Martin, Executive Vice President/COO
Barbara Keller, Deputy General Counsel, Legal Affairs
Deborah Cates, Chief of Staff, Chairman'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
Gassenia Guilford, Assistant Vice President, Finance
Christopher A. Telano, Chief Internal Auditor/AVP, Office of Internal Audits
Wayne McNulty, Corporate Compliance Officer
Wayne Hanus, Controller, MetroPlus Health Plan
Nelson Conde, Director, Office of Professional Services & Affiliations
Alice Berkowitz, Assistant Director, Central Office Budget
Daren Ng, Senior System Analyst, Central Office Budget
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
Jonathan Delgado, Supervising Confidential Examiner
Sam Malla, Associate Staff Auditor, Office of Internal Audits
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
Jean Saint-Preux, Confidential Examiner, Office of Internal Audits
Milenko Milinic, Controller, Queens Health Network
Kiho Park, Associate Executive Director, Queens Health Network
Alessandro Cavallo, Pharmacist, Governeur Healthcare Services
Kathy Bowman, Senior Associate Director, Governeur Healthcare Services
Matt McDevitt, Senior Associate Director, Governeur Healthcare Services
Daniel Frimer, Controller, South Brooklyn/Staten Island Network
Martin Novzen, Senior Associate Director, Woodhull Medical & Mental Health Center
Ronald Townes, Associate Director, Kings County Hospital Center

FEBRUARY 19, 2015
AUDIT COMMITTEE MEETING
MINUTES

An Audit Committee meeting was held on Thursday, February 19, 2015. The meeting was called to order at 1:05 P.M. by Ms. Emily Youssouf, Committee Chair. Ms. Youssouf then asked for a motion to adopt the minutes of the Audit Committee meeting held on December 4, 2014. A motion was made and seconded with all in favor to adopt the minutes. An additional motion was made and seconded to hold an Executive Session of the Audit Committee to discuss matters of personnel and potential litigation.

Ms. Youssouf then turned to Chris Telano for the audits update.

Mr. Telano saluted the Committee Members and said that we will start with the briefing on pages three and four, which is the summary of the audits currently being conducted by City and State Comptroller's Office. The first one is of the Navigant consulting billing practices. This audit started in July 2013 – they worked on it for about six weeks. Then we did not hear from them from September 2013 until we received a letter on January 28, 2015. The letter stated and I will quote "the audit has been terminated without issuing a report because there is no need to do so at this time". However, they did take the opportunity to make some observations and recommendations to improve our operations. Sal Russo and I had a conference call with them to discuss their concerns advising them that controls have been put in place and we have a more robust Audit Committee and internal auditing department to evaluate those controls to alleviate any fears that they might have. I followed that up with a letter reiterating what we discussed. That audit is closed.

Ms. Youssouf stated that that is good and asked if that seems to have satisfied them. Mr. Telano answered yes.

The second audit Mr. Telano continued on page three is of the Affiliation Agreement with Lincoln Hospital and PAGNY. This audit is status quo – they are still obtaining information and have been ongoing since July 2013. On page four, another audit by the Comptroller's office, is also kind of on hold. This audit is the one that they requested reports with patient information and we declined due to confidentiality concerns. There were subsequent discussions between Wayne McNulty, Sal Russo, the Comptroller's office and myself and we are waiting for some counterproposal on their part as to how we are going to resolve this. The last one on page four is the final audit of overtime cost by the state Comptroller's office.

Ms. Youssouf stated that let it be noted that Dr. Boufford has joined the Audit Committee meeting. We are on page four in internal audits. Chris was giving us a rundown of where we are.

Mr. Telano continued and stated that the State Comptroller did a follow-up audit on their original overtime audit. There were three recommendations and due to the limited scope of their review, they did not consider the reduction in staffing that we had and those types of costs. The findings were partially resolved from their perspective -- it is a good audit and that was closed also.

Mr. Telano moved on to page five of the audits completed since the last meeting. The first one is of Patient Implantable Devices at Harlem Hospital. He asked the representatives to approach the table and introduce themselves. They did as follows: Ebone Carrington, Chief Operating Officer; Carmen Holt, Senior Associate Director; Franklin Armas, Manager; Lynette Faust, Senior Associate Director; Nelly Valentine, Senior Associate Director; Holly Gilbert, Hospital Police. Mr. Telano stated that I will go over the findings altogether and then you can address all three of them after I finish discussing them. The first one has to do with the improper billing of implantable devices. For example, we looked at 13 bilateral breast implant procedures and we noted that billing was for only implant instead of two. In addition, there was one other bilateral breast implant procedure that was not billed

at all although it was coded. Overall 11 of the 13 bilateral breast implants procedures were not properly billed. We also found that one out of three Medipoint implant procedures was not billed at all. Keep in mind that our review did include looking at pacemakers, stents and gastric bands for arthroscopic procedures. It seems like it is just limited to those findings. We did not note any findings in the other procedures.

Mrs. Bolus asked if we are past the time to bill for these. Ms. Faust answered that most of those procedures were cosmetic so they were self-pay. What happened was the patient paid in advance for both the implants as well as the procedures. So what we did after the findings were divulged to us, we added those implantables so we could adjudicate the account and bring it to a zero balance.

Mrs. Bolus asked if they requested the money from the patient. Ms. Faust responded no, we did not. Mr. Telano continued by stating that the second finding had to do with the lack of an inventory system regarding the implantable devices. In lieu of an inventory system, we had a representative from Cardinal monitor our inventory levels and then recommend the items that we should have and order from Cardinal. We paid them $100,000 a year to perform this function. Ms. Holt stated that one thing we have done since then is we have requested an FTE, full time equivalent, which had been approved and that person will take over managing the inventory.

Ms. Youssouf asked does that mean you are going to bring the management of the inventory in-house and not have the contract with Cardinal anymore. Ms. Carrington responded correct. Ms. Youssouf then asked when that is effective. Ms. Carrington answered that the position has been approved and is being actively recruited for.

Ms. Youssouf said great and asked if they have the software behind for the inventory system. Ms. Holt responded that what we are currently doing is looking at our eCommerce system where we can generate reports related to our inventory that we currently have on hand. We are also working on the PXYSIS system, bringing that on board into the institution. We will be going to site visits to see how it is being used at another one of our facilities.

Mr. Telano continued stating that the last issue regarding this audit has to do with general access to the operating room suite. That area had various entries; some were accessible via swipe cards and others were accessible through the keypad code and one door was unlocked. There were 199 pages of individuals with access. My staff, when they were given a temporary ID card from Harlem, were able to access using this swipe card. Ms. Gilbert stated that since then the two doors that were in the back that were accessible by combination have been changed from combination access to card swipe, which is only accessible to authorized personnel. The front door that was unlocked has been secured and the amount of card swipe accessible parties has been limited to only authorized personnel.

Ms. Holt added that the authorized personnel list includes those who were approved by the Division Chiefs and we did not want to be restrictive because of the criticality of the area. Those physicians, nurses, members from pharmacy, administration and other approved personnel and as people are on board in each of these divisions; it has to be vetted by the department.

Ms. Youssouf asked if that is the procedure at other HHC facilities. Mr. Telano responded that I believe it is similar.

Ms. Youssouf then asked if this could be checked to be sure that is the similar procedure. Ms. Holt responded that we do know that is the case at our network facilities but I will reach out to other networks to see if that is a similar procedure.

Dr. Boufford asked if the self-pay cash payments may become more of a part of what we do over time and if you are satisfied that the fiscal and administrative procedures are in place to collect cash on-site at the facility. To which Ms. Zurack answered that we can take a look at that corporate wide in terms of cosmetic procedures.

Mr. Telano continued, the next audit that we completed was of the accounts payable process at MetroPlus and he asked the representatives to approach the table. He introduced himself as Wayne Hanus, Comptroller. Mr. Telano said that first issue found at MetroPlus is not making use of the automated approval system in which they use GHX to eCommerce to produce the purchase order, which is then paid in OTPS. There is a three-way match as a result of that, and the approvals are at the front end of the purchasing process. They also have chosen to use a handwritten voucher to obtain the approval after the invoice comes in instead of making use of the automated system.

Mr. Hanus stated that this procedure has been in place since the new system came onboard. The process that we have in place allowed us to ensure that there was uniformity in the signatures, the review and the attachments that were coming over to accounts payable because we had over 20 different departments submitting. We think the suggestion is certainly one worth pursuing if we can cut down on some of the paperwork or the waiting for that manual sign-off that you already have in the system. We are going to take a look at that and make a recommendation to the CFO by the end of March in terms of how we want to proceed with that.

Mrs. Bolus asked how long has the accounts payable been in that process. Mr. Hanus answered that it is probably ten years we have proceeded with this process. Ms. Youssouf asked why.

Mr. Hanus responded that that it is a methodology that the users of the system preferred because it allowed them to put together a package in a consistent manner and allowed us to review the items presented for payment.

Ms. Youssouf asked isn't GHX also a consistent manner? Mr. Hanus replied sure, that is why we want to look at it. We do have invoices that are coming from accounts payable that might be payable under a blanket order or those that might be just standard individual items and by doing it this way everything looks the same to the accounts payable unit coming in. Everything is processed in a similar manner to the different user groups.

Ms. Youssouf asked Ms. Zurack if she had any concerns about that. To which Ms. Zurack responded that I think when, in all fairness, you should have reviewed this internally and come to this committee with what you are doing. When you are saying you are going now recommend to your CFO, that is the MetroPlus CFO, this is the HHC Audit Committee it is sort of out of order.

Mr. Hanus stated that I understand – it is just the timing of the work going on in MetroPlus and we wanted to take the appropriate time to set something in motion.

Ms. Youssouf said that this report was issued January 5. Ms. Zurack added that she will have a conversation with Mr. Arnold Saperstein – they should have their solutions before they come here. They are their own corporation so they do not have to follow our operating procedures and all our systems. This is just our recommendation that we think it would be better for them. It does not mean that they did not have a control; they could have used ours and had a better control. It is really more of a recommendation that a finding, but I do think it is inappropriate to come to the Audit Committee without having it resolved and just say we are going to talk about it and look at it. My recommendation would be in the future MetroPlus comes here fully prepared.

Mr. Hanus said that that is fine – when we did set this up there was a lot of discussion with the central office folks and the team that was setting up GHX thought to be the best process for MetroPlus going forward. At that time, we

thought it was the best way to ensure uniformity in the information being submitted and it has worked quite well. I think all we are talking about is a sheet of paper that is attached to the supporting documentation that comes over to accounts payable.

Ms. Youssouf stated that I am a little concern because you seem to be dismissing this as nothing important. Even though MetroPlus is a separate organization, we are the only member and so we own it. If our internal audit department and our CFO believe that our system is better, I think it would be wise of you to actually look at it and try to match our system. Take this a little more seriously than a piece of paper – it is a little disconcerting.

Ms. Zurack commented that Chris Telano, in all fairness, is offering efficiency. It is not that they have a bad control. Mr. Telano said that it is an efficiency matter and it is over controlled. Basically the process is too long and that is the way HHC has it set up.

Ms. Zurack said that in the interest of newness, Wayne Hanus is a terrific controller. Typically, John Cuda, CFO and the procurement person should have come to this.

Ms. Youssouf added that it would be great at perhaps the next Audit Committee meeting somebody comes back and says you are in the process of doing it or whatever the solutions is. To which Mr. Hanus said that we can do that.

Mr. Telano continued by stating that the other finding is lack of proper documentation related to two consultant payments. One was paid without a contract in place and another one was being paid without supporting time sheets. I believe they were resolved.

Mr. Hanus said that they were resolved. The one physician without the contract in place we no longer use the services and with regard to the physician that was submitting the invoice without the time, the individual is actually performing those services on-site. It was an oversight that a time sheet was not prepared and that individual has been preparing time sheets for several cycles.

Mr. Telano said that in the interest of time, we will not be calling anyone up to the table from Coney Island and Elmhurst; they have similar findings in which the unannounced count, surprise counts, revealed discrepancies around 20 percent. At Elmhurst, it equaled $2,400 in differences. There was also commingling of inventory at the pharmacy in Coney Island – there were some wholesale acquisition costs items intermingled. At Elmhurst in the medical surgical, there was Hemodialysis supplies commingled within the inventory. To the best of my knowledge, everything has been resolved and they took the necessary steps during the course of this audit.

Mr. Telano stated that that concludes his presentation.

Ms. Youssouf asked if there were any questions for Mr. Telano. She then turned to Wayne McNulty for the compliance update.

Mr. McNulty saluted everyone and started by discussing the following two certifications that HHC is required to implement in order to participate in the Medicaid program: (i) the compliance program certification; and (ii) the Deficit Reduction Act of 2005. With regard to the compliance program certification, Mr. McNulty informed the Audit Committee (the "Committee") that on December 22, 2014, HHC President and Chief Executive Officer Dr. Ramanathan Raju certified through the Office of the Medicaid Inspector General's ("OMIG") website that HHC has an effective compliance program. Mr. McNulty explained that several elements must be met in order to certify that an entity has an effective compliance program and continued by providing the following overview of some of the required elements: (i) written policies and procedures; (ii) having a designated compliance officer; and (iii) having a

nonintimidation and nonretaliation policy for good faith reporting and participation in a compliance program. Mr. McNulty proceeded by discussing the Deficit Reduction Act of 2005 certification. He stated that the Deficit Reduction Act requires HHC to have policies and procedures to detect and deter fraud, waste and abuse and policies and procedures related to the False Claims Act. In summary, he explained that the aforementioned policies and procedures must be set forth in each HHC facility employee handbook.

Mr. McNulty continued on to page seven of the Corporate Compliance Report (the "Report"), which provided an overview of some of the compliance program and DRA requirements. He informed the Committee that on December 29th he certified through the OMIG website that HHC was in compliance with the Deficit Reduction Act.

Mr. McNulty further continued on page seven of the Report by discussing HHC's compliance with the HIPAA Security Rule Risk Analysis requirements. He stated that, pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its Security Rule regulations, HHC is required to perform a risk assessment program to prevent, detect, contain and correct any security violations. Moving on to page 8 of the Report, he explained that one of the key elements of a risk assessment program is the performance of a risk analysis. He stated that under the Security Rule, HHC is required to conduct an accurate and thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information throughout HHC. He moved on to page nine of the Report to discuss the risk assessment requirements further. He explained that a risk assessment could be performed in a number of ways and that there is no particular methodology required to perform the same. However, he elaborated, that a risk assessment must include the performance of eight key steps to be in compliance with the Security Rule. Mr. McNulty went over some of the key eight steps: (i) the scope of the analysis must be identified; data and information must be gathered; (iii) potential threats and vulnerabilities must be identified and documented. Mr. McNulty paused and defined a threat as any action that if it occurred would put the confidentiality and integrity of HHC information at risk and vulnerability of the likelihood of that threat occurring. Continuing with the key steps of a risk assessment, Mr. McNulty provided the following: (iv) the assessment of current security measures must take place; (v) the likelihood of threat occurrence must be determined; (vi) the potential impact of threat occurrence must be determined. Mr. McNulty explained that impact could mean financial impact, legal impact or reputational impact. He continued by stating that the risk assessment must also: (vii) identify security measures; and (viii) finalize documentation.

Mr. McNulty informed the Committee that the OCC reviewed HHC's compliance with the Security Rule risk analysis requirements under HIPAA and determined that the inventory of HHC's information systems and applications that access, house or transmit electronic protected health information was a work in progress and therefore, at the current juncture, was not comprehensive. He stated that, although HHC's Enterprise Information Technology Services has taken numerous and significant measure to enhance and maintain the confidentiality, integrity and security of HHC's information systems - including the formation of information governance and security program, the implementation of security controls and a performance of formal risk analysis on a handful of applications - it appeared that measures must be taken by information technology to fully satisfy the extensive risk analysis and implementation measures required under the Security Rule.

Mr. McNulty provided the following recommendations:

- identify inventory as a priority, all HHC systems and applications that are housed and transfer electronic protected health information;
- provide a written schedule over a 12-month schedule by which all systems will be inventoried and have a completed risk analysis; and
- provide a written schedule over a 12-month schedule that would look at the other standards of the security rule to be assessed

Before continuing with his recommendations, Mr. McNulty paused to explain that under the Security Rule identifies two types of requirements. These requirements, he explained, are addressable requirements and requirements that are required in the Security Rule -- meaning, that the Corporation does not have the option to forego the same. With regard to the addressable requirements, he elaborated, if you perform a risk analysis and that risk analysis shows particular areas of low vulnerability you do not have to follow those particular regulations for that area. However, he stated, you have to perform a risk analysis first before you can make that assessment. Mr. McNulty then continued with his recommendations:

- immediately begin a risk analysis for the top 25 high-risk applications;
- inventory all remediation recommendations resulting from any completed risk analysis; and
- ensure that, regardless of the methodology used to perform the required risk analysis, documentation of the eight steps mentioned earlier in the Report occurs.

He further recommended as a practice guide that IT take a look at the National Institute of Standards and Technology and their risk assessment and the HIPAA guidance on risk analysis under the HIPAA Security Rule as well. In summary, he informed the Committee that the findings outlined in the instant Report were communicated to EITS leadership and the OCC is now awaiting management's response to the same. He stated that Information Services is expected to come before the Audit Committee in April to provide a response to the same.

Ms. Youssouf asked if that puts us at any risk between now and April. To which Mr. McNulty responded that if we have a system that transmits and houses EPHI and we are not aware that vulnerability exists then that could put us at risk. In sum and substance, he stated that IT has a significant amount of security controls in place, a security governance program, and has performed the risk analysis on a handful of the very high-risk applications. However, he opined, additional measures would be necessary for HHC to be in full compliance with the Security Rule.

Mrs. Bolus asked did the warehouse fire have any effect on that. Mr. McNulty answered that I will discuss the fire in executive session.

Moving along to section four, Compliance Reporting Index for the Fourth Quarter, Calendar Year 2014 October 1 to December 31, 2014. Mr. McNulty stated that there were 136 reports that we have received at the Office of Corporate Compliance ("OCC") - one Priority A report, 85 priority B reports, and the remaining were Priority C reports. He added that some notable reports were ongoing investigations that would be discussed in executive session. He continued with the Privacy Reporting Index for the Fourth Quarter, Calendar Year 2014 - - October 1 to December 31, 2014. He stated that 30 complaints were received into the OCC's HIPAA tracking system. We determined seven were breaches of health information, elaborating that the majority of the breaches occurred because wrong documentation was sent to the wrong patient. He added that one breach occurred at Bellevue Hospital and involved the unauthorized access of a patient's medical record by numerous workforce members. In that case, he stated, the patient was notified and the Department of Health and Human Services, which receives notification of breaches of PHI, was also notified of this incident. Given the ongoing investigation of this incident, Mr. McNulty informed the Committee that more details of the incident would be provided in executive session.

Dr. Boufford asked in the incident reporting, you used the word complaints. Is there a distinction there and any kind of incentive for people to be sort of reflective and self-critical about what is going on or did it come up because a third party cites a problem. Mr. McNulty responded that the majority is because a third party notifies us that information was breached. He added, in sum and substance, that information is provided by HHC staff members who notify the OCC and relay that X, Y and Z occurred. He stated that staff members have been forthcoming when they provide notice that a breach occurred based on inadvertent error. In summary, he stated that the majority of

times the notice comes from a patient because the reporting patient has received a notification of another patient's name on it and the Corporation is unaware of the same until it receives said notice from the reporting patient.

Dr. Boufford stated that I am curious about how much self-policing there is. There is opportunity there in terms of the way the procedures are set up. It sounds like you are doing that. Mr. McNulty said absolutely, we take that into account as far as our disciplinary policies.

Mr. McNulty moved on to the Monitoring of Excluded Providers – he reported that the OCC did not received or uncover any reports of excluded providers since the last time the Audit Committee convened in December 2014.

Mr. McNulty continued onto page fifteen of the Report and informed the Committee that he will report some ongoing compliance matters to the Audit Committee in April 2015, including the status of the revision of: Operating Procedure 50-1 (which he explained is the operating procedure that governs the Corporate Compliance Program); the Principles of Professional Conduct; and HHC Corporate Compliance Plan. He explained that compliance best practices the revision of compliance policies and procedures every several years. He also stated that he would like to review the OCC's findings of HHC's compliance with the HIPAA business associate agreement requirements, as well as vendor management activities and CMS regulatory requirements for contractors. Last, he added, he would like to discuss compliance and privacy training activities and corresponding compliance rates.

Ms. Youssouf stated that that is good news about excluded providers. It has been a while – that is a great improvement.

Mr. McNulty asked the Audit Committee if they had any questions and then concluded his Report.

Ms. Youssouf thanked Mr. McNulty, and then indicated that the Committee was going into Executive Session. (Executive Session was held).

Ms. Youssouf stated that they are back from the Executive Session.

There being no further business, the meeting was adjourned at 2:35 P.M.

Submitted by,

Emily Youssouf
Audit Committee Chair

NEW YORK CITY HEALTH AND HOSPITALS CORPORATION

AUDIT COMMITTEE OF THE HHC BOARD OF DIRECTORS

Corporate Compliance Report

April 16, 2015

Table of Contents

Agenda

I. Follow up on February 2015 Audit Committee Report on HHC's Compliance with the HIPAA Security Rule Risk Analysis Requirements

Overview

1) On February 7, 2015, Wayne A. McNulty, Senior Assistant Vice President/Chief Corporate Compliance Officer, provided the Audit Committee with an overview of HHC's compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or the "Act") and its implementing regulations (found at 45 CFR Parts 160 and 164, "The Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule")), which requires that the New York City Health and Hospitals Corporation ("HHC" or the Corporation") implement a risk assessment program the purpose of which is to prevent, detect, contain, and correct security violations affecting electronic protected health information ("EPHI").[1]

Security Rule Requirements

2) Specifically, 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. HHC is also 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.[2]

HHC's Compliance Status with Security Rule Risk Analysis Requirements

3) With regard to HHC's compliance with the Security Rule risk analysis requirements, the OCC informed the Audit Committee that, in pertinent part: (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

[1] 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.
[2] 45 CFR §164.308 (a)(8).

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

Recommendations

4) Based on the foregoing, the OCC has recommended that the following measures be taken by HHC's EITS:

- 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; and
  - 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[3] and HIPAA Guidance on Risk Analysis Requirements under the HIPAA Security Rule.[4]

[3]NIST - An Introductory Resource for Implementing the Health Insurance Portability and Accountability Act ("HIPAA") 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

[4] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf; *see also* Department of Health and Human Services. "Security Rule Guidance Material." at www.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.

Follow up

5) In response to the findings and recommendations provided above, EITS has taken steps to procure a third-party vendor to provide, among other things, the following services:

- HIPAA Risk Analysis (Application & EPHI);
- HIPAA Compliance Assessment;
- Application Security – Penetration Test;
- Infrastructure Security – Internal Penetration Testing;
- Infrastructure Security – Internal Server Penetration Testing;
- Infrastructure Security- Perimeter/DMZ Penetration Assessment; and
- Vendor/Third Party Assessment.

6) Sal Guido, Senior Assistant Vice President/Acting Chief Information Officer, will provide the Audit Committee with the additional measures EITS has taken to address the risk assessment requirements mentioned above at today's meeting.

II. Compliance Reporting Index for the First Quarter of Calendar Year 2015 ("CY2015") (January 1, 2015 to March 31, 2015)

Overview of Reports Received[5]

1) For the first quarter CY2015 (January 1, 2015 to March 31, 2015), there were 81 compliance-based reports of which one was classified as a Priority "A" report, 31 (or 38.3%) were classified as Priority "B" reports, and 49 (or 60.5%) were classified as Priority "C" reports. For purposes here, the term "reports" collectively means compliance-based inquiries (including requests for compliance guidance), compliance-based reports (including self-reporting), and compliance-based complaints. Of the 81 reports received during this period, 51 (or 63%) were received through the OCC's anonymous toll-free compliance helpline (the Helpline").

Mode of Reporting

2) Below is a summary of how the OCC received the 81 CY2015 first quarter reports:

- 51 (63%) were received on the Helpline;
- 9 (11.1%) were received via Telephone;
- 8 (9.9%) were received via E-mail;

[5] There are three (3) different report categories: (i) Priority "A" reports - matters that require immediate review and/or action due to an allegation of immediate threat to a person, property or environment; (ii) Priority "B" reports – matters of a time-sensitive nature that may require prompt review and/or action; and (iii) Priority "C" reports – matters that do not require immediate action.

- 5 (6.2%) were received Face to Face;
- 3 (3.7%) were received via Mail;
- 2 (2.5%) were received via Other;
- 2 (2.5%) were received via Intranet; and
- 1 (1.2%) were received via Office Visit.

Allegation Class Analysis

3) The breakdown of the allegation classes of the 81 reports received in the first quarter of CY2015 is as follows:

- 20 (24.7 %) Misuse or Misappropriation of Assets or Information;
- 19 (23.5 %) Policy and Process Integrity;
- 18 (22.2 %) Other;
- 16 (19.8 %) Employee Relations;
- 5 (6.2 %) Environmental, Health and Safety;
- 2 (2.5 %) Diversity, Equal Opportunity, and Respect in the Workplace; and
- 1 (1.2 %) Financial Concerns.

III. Privacy Reporting Index for the First Quarter of CY2015 (January 1, 2015 to March 31, 2015)

Overview of Privacy Incident Reports and Investigations (First Quarter CY2015)

1) For the first quarter of CY2015 (January 1, 2015 through March 31, 2015), 45 Reports were entered in the HHC HIPAA Complaint Tracking System, a HHC proprietary database. Of the 45 Reports entered in the tracking system, 14 were found after investigation to be violations of HHC HIPAA Privacy/Security Operating Procedures; five were determined to be unsubstantiated; five were found not to be a violation of HHC HIPAA Privacy Operating Procedures; and 26 are still under investigation. Of the 14 confirmed violations, four were determined to be reportable breaches of protected health information ("PHI"), seven were determined not to be a breach, and three are pending breach determination.

Breach Defined

2) A breach is an impermissible use, access, acquisition or disclosure (hereinafter collectively referred to as "use and/or disclosure") under the HIPAA Privacy Rule that

compromises the security and privacy of PHI maintained by the Corporation or one of its business associates.[6]

3) Pursuant to 45 CFR § 164.402 [2], the unauthorized access, acquisition, use or disclosure of PHI is presumed to be a breach unless HHC can demonstrate that there is a low probability that the PHI has been compromised based on the reasonable results of a thorough risk assessment, that is completed in good faith, of key risk factors.[7]

Factors Considered when Determining Whether a Breach has Occurred

4) Under HIPAA regulations, at a minimum the following four key factors must be considered to determine whether there is greater than a low probability that a privacy and/or security incident involving PHI has resulted in the compromise of such PHI:[8]

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

5) As detailed in the paragraphs immediately below, a total of 36 individuals were affected by the four confirmed breaches.

Confirmed Breaches First Quarter 2015)

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

- Coney Island Hospital – This incident occurred on January 23, 2015 when packages containing PHI that were entrusted to a courier service for delivery, were found on the street in Queens. Apparently documents containing PHI fell off the delivery truck and were later found by a bystander. Some of the documents recovered were sealed; other documents were opened and not intact.

[6] 45 CFR § 164.402 ["Breach" defined].
[7] *See* 45 CFR § 164.402[2]; *see also* 78 Fed. Register 5565 at 5643 and 5695 [January 25, 2013]
[8] *See* 45 CFR § 164.402 [2][i-iv].

Breach notifications were sent to the affected eight patients on March 30, 2015. All of the affected patients were provided with credit monitoring.

- Queens Medical Center – This incident occurred on January 15, 2015 when an unauthorized recipient-patient received the discharge papers of another patient. The daughter of unauthorized recipient-patient contacted the Queens Medical Center ("Queens") clinic from which the documents originated from to inform them of the delivery error; however, she refused to return the papers containing PHI to Queens. She insisted upon sending the discharge papers directly to the affected patient (the patient who was the subject of the discharge papers). Breach notification was made to the affected patient on March 20, 2015.

- Harlem Hospital Center – This incident occurred on January 30, 2015 and involved the unauthorized access of the electronic medical record of a patient/employee by several employees at the facility. The nine employees who improperly accessed the medical record were disciplined by way of suspension. Breach notification was sent to the affected patient on April 8, 2015.

- Coler Nursing and Rehabilitation Center - This incident, which occurred on February 20, 2015, was identified when Coler Nursing and Rehabilitation Center ("Coler") Pharmacy noticed that one out the group of 7 bags of medications was missing. This amounted to one week's supply of medications for 27 residents on one of the floors at Coler, whose names were on the medications. The medications were scheduled to be delivered from Henry J. Carter Specialty Hospital and Nursing Facility ("Carter") to Coler the day before, February 19, 2015. Carter is where the medications are prepared, processed, and packaged and are then transported to Coler.

  An investigation into this matter was launched and completed by Hospital Police, the Director of Pharmacy, the Facility Risk Manager, and the Facility Privacy Officer. According to the driver, he/she was alerted by a passing vehicle that the back door of the van transporting the medications from Coler was open. The driver pulled over on Madison Avenue and closed the door and then proceeded to Coler. A review of Carter's external cameras confirmed that the van's rear door was in fact open when it departed from the loading area of Carter. The OCC has determined that a breach occurred and will notify the affected patients before April 20, 2015.

IV. Monitoring of Excluded Providers

1) The OCC has not received or uncovered any reports of excluded healthcare providers or other workforce members since the Audit Committee last convened in February 2015. The OCC did uncover one vendor that was excluded on the GSA list and referred the matter to the HHC

Office of Procurement for handling. Apparently, the vendor is not an active vendor, therefore, there are no potential overpayment issues here to address.

V. Revision of Corporate Compliance Policies and Procedures - Status Update

Overview

1) Consistent with compliance best practices that recommend the periodic assessment and revision of existing compliance policies and procedures, the OCC is revising the following HHC compliance-related policies:

- Operating Procedure ("OP") 50-1 (Corporate Compliance Program);
- HHC Corporate Compliance Plan; and
- HHC's Principles of Professional Conduct ("POPC").

2) All of the aforementioned policies will be provided to the Audit Committee in its final draft form for comment and questions, if any, prior to execution by HHC President and CEO Ramanathan Raju, M.D., for official promulgation as Corporation policy.

OP 50-1

3) OP 50-1 describes the eight elements of HHC's Corporate Compliance Program (the "Program") and how compliance activities are directed across the Corporation. OP 50-1 will be supplemented to, among other things: (i) further highlight important risk areas covered by the Program; and (ii) address special compliance considerations related to HHC's wholly owned subsidiaries and ancillary compliance programs.

Corporate Compliance Plan

4) The Corporate Compliance Plan (the "Plan") discusses in detail how HHC implements all of the required elements of an effective compliance program. In sum and substance, the Plan provides a detailed overview of how OP 50-1 is carried out corporate-wide. The Plan will be updated to provide more detail related to current compliance activities and will be supplemented to address compliance initiatives within HHC's wholly owned subsidiaries.

POPC

5) Pursuant to Department of Social Services compliance program regulations found at 18 NYCRR § 521[c][1] and Department of Health and Human Services Office of Inspector General ("OIG") Compliance Program Guidance to Hospitals, HHC is required to develop written

policies and procedures embodied in a code of ethics or standards of conduct.[9] Under OIG guidance, the standards of conduct must cover all workforce members and outline the Corporation's "commitment to comply with all Federal and State standards, with an emphasis on preventing fraud, waste and abuse."[10] According to OIG, the standards of conduct shall "state the [Corporation's] mission, goals, and ethical requirements of compliance . . . ."[11] HHC's "standards of conduct" is embodied in, and referred to as, the HHC POPC.

6) The content of the POPC has been sent to an outside vendor for an update as to its content and graphics. The POPC, after appropriate approval as provided in paragraph 2 of this section, will thereafter be disseminated to all affected workforce members.

VI. Compliance Training Update

Overview

1) Compliance program regulations set forth at 18 NYCRR § 521.3 [c][3] require the Corporation to periodically provide compliance "training and education [to] all affected employees and persons associated with the [Corporation], including executives and governing body members, on compliance issues, expectations and the compliance program operation…."[12]

2) The training cycle for the current compliance training period ends on Tuesday, June 30, 2015.

Implementation of Compliance Training Corporate-wide

3) The OCC previously developed the following four compliance training modules:

- Compliance training for physicians;
- Compliance training for healthcare professionals who are licensed under Title VIII of the Education Law (*i.e.*, physical therapists; respiratory therapists; occupational therapists; nurses), as well as other individuals involved with patient care activities;
- Compliance training for Group 11 employees (and individuals designated by their Group 11 supervisors), as well as workforce members whose duties involve coding and/or billing functions; and

[9] *See* NYCRR § 521.3[c][1]; *see also* Department of Health and Human Services Office of Inspector General Publication of the OIG Guidance for Hospitals, 63 Fed. Register 8987, 8989 [February 23, 1998].
[10] OIG Guidance for Hospitals, 63 Fed. Register at 8989-90.
[11] *Id.*
[12] 18 NYCRR § 521.3[c][3]

- Compliance training for Members of the Board of Directors.

4) In Fiscal Year 2015, all of the aforementioned training modules were supplemented to address emerging compliance issues.

- The revised training modules for the physicians and healthcare providers are currently live and affected workforce members have been accordingly enrolled in the same.

- The revised training modules for Group 11 employees are expected to be finalized by Friday, April 17, 2015. Group 11 employees (and other affected workforce members) will be enrolled into the same on or before Friday, April 24, 2015.

- The revised training module for the Members of the HHC Board of Directors will be completed by Friday, April 17, 2015. In the interim, the OCC has been working with Sr. AVP/Acting CIO of EITS to ensure that the module, when completed, will be accessible by Board Members via their I-Pad tablets.

Current training numbers

5) Current training numbers as of April 6, 2015 are as follows:

- Healthcare Professionals Module**:**
  - 20,490 enrolled
  - 5,486 completed
  - 20% completion rate

- Physicians Module
  - 6,615 enrolled
  - 1,332 completed
  - 27% completion rate

Efforts made to increase training numbers:

6) The OCC has formally reached out, via written memorandum among other methods, to each medical chief of service and administrative head of affected clinical departments, respectively, regarding the mandatory compliance training requirements.

7) The OCC anticipates that the mandatory training completion rates for physicians and healthcare professionals will significantly improve by the next time the Audit Committee convenes in June of 2015.

VII. Outline of Calendar Year 2015 ("CY2015") Corporate-wide Risk Assessment

Overview

1) On or about the first week of May 2015, the OCC will begin conducting the CY2015 Corporate-wide Risk Assessment (the "Risk Assessment"). The results of the risk assessment will be used, in pertinent part, by the OCC to develop the fiscal year 2016 ("FY2016") New York City Health and Hospitals Corporation ("HHC") Corporate Compliance Work Plan. The risk assessment process is expected to be completed by mid-July 2015.

Legal Requirements

2) The Risk Assessment is undertaken in furtherance of New York State Social Services Law § 363-d (2)(f) and New York State compliance program regulations found at 18 NYCRR § 521.3 [c][6], which require the establishment of "a system for routine identification of compliance risk areas . . . ." The performance of such Risk Assessment is an important step in "identify[ing] those events, conditions or risks that could significantly affect the achievement of [HHC's] objectives, including the protection of assets and the efficient operation of financial operations and other services."[13]

3) Equally important as the requirements set forth in the foregoing paragraphs, is that the Risk Assessment is a component of HHC's Corporate Compliance and Ethics Program (hereinafter referred to as the "Program"). The OCC is responsible for implementing, overseeing, and monitoring the Program, which is centered on promoting the prevention, detection, and mitigation of fraud, waste, and abuse, as well as any other unprofessional or criminal conduct; and ensuring HHC's compliance with City, State and Federal laws, rules, and regulations, and its own business and ethical standards of practice**.**

Defining Risk

4) As the first step in identifying the risks applicable to HHC, it is necessary to understand what "risk" is. Risk has been described as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."[14] In simpler terms, "[r]isks are events or conditions that may occur and, if they do occur, would have a harmful effect" on HHC.[15]

[13] Office of the N.Y.S. Comptroller ("OSC") - Division of Local Government and School Accountability ("DLGSA") - Local Government Management Guide - *Management's Responsibility for Internal Controls*, Oct. 2010, at 9 (discussing "The Process of Risk Assessment.")
[14] NIST, U.S. Dep't of Commerce, *Guide for Conducting Risk Assessments* (Special Publication 800-30) Information Security, September 2012, at 6.
[15] HCCA Professional's Manual, Risk Assessment Chapter, ¶ 40,105, at 41,001.

5) Risks generally fall into two distinct categories: (i) *inherent risks*, the possibility of an undesired circumstance coming to fruition without due consideration of any factors that may mitigate such a risk; and (ii) *residual risks*, which are those risks that remain even after employing corresponding internal controls.[16]

Identifying Risk

6) HHC will incorporate the following three distinct approaches to identify its risk:[17]

(i) Conducting a survey of key subject matter expert corporate stakeholders utilizing generic open-ended questions – developed by OCC – to determine the presence and scope of risks;
(ii) Conducting one-on-one interviews or small group meetings regarding the presence of corporate risks; and
(iii) Utilizing a list of "pre-defined compliance risks" developed from various internal and external sources.

The Health Care Compliance Association ("HCCA") has noted that organizations may use a combination of approaches to identify potential compliance risk.[18] HHC has utilized a combined approach in the past.

Risk Scoring and Prioritization

7) The OCC will lead a process to score and prioritize all identified risks and take into account, among other things, the potential impact of a given risk, the likelihood of risk occurrence, and the presence of internal controls to mitigate identified risks.

Risk Tolerance and Appetite[19]

8) At the end of the risk prioritization process, the OCC will provide the results of the risk assessment, identification, scoring, and prioritization exercises to HHC President/CEO Dr. Raju and the Audit Committee of the HHC Board of Directors. These findings will be used by Dr. Raju and the Audit Committee to determine and establish the Corporation's risk tolerance and risk appetite.

[16] *Id.*; *see also* COSO, *Risk Assessment in Practice*, October 2012, at 7.
[17] HCCA Professional's Manual, ¶40,120, at 41,006, discussing risk identification.
[18] *Id.*
[19] *See* Dr. L. Rittenberg and F. Martens, COSO Enterprise Risk Management Understanding and Communicating risk Appetite, (2012) (defining risk appetite as "[t]he amount of risk, on a broad level, an entity is willing to accept in pursuit of value," and defining risk tolerance as the "acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives," which is one consideration affecting risk appetite along with existing risk profile, risk capacity, and attitudes towards risk).