AUDIT COMMITTEE
MEETING AGENDA

June 11, 2015

12:30 P.M.

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

CALL TO ORDER — Ms. Emily A. Youssouf

- Adoption of Minutes April 16, 2015 — Ms. Emily A. Youssouf

ACTION ITEMS

INFORMATION ITEMS

- KPMG 2015 Audit Plan — Ms. Maria Tiso
- Audits Update — Mr. Chris A. Telano
- Compliance Update — Mr. Wayne McNulty

OLD BUSINESS

NEW BUSINESS

ADJOURNMENT

MINUTES

AUDIT COMMITTEE **MEETING DATE: April 16, 2015**
TIME: 12:30 PM

COMMITTEE MEMBERS

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

STAFF ATTENDEES

Antonio Martin, Executive Vice President/COO
Salvatore Russo, 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
Roslyn Weinstein, Senior Assistant Vice President, OFD
Julian John, Corporate Comptroller
Paul Albertson, Senior Assistant Vice President
Gassenia Guilford, Assistant Vice President, Finance
Kathleen McGrath, Senior Director, Central Office Communications
Christopher A. Telano, Chief Internal Auditor/AVP, Office of Internal Audits
Wayne McNulty, Corporate Compliance Officer
Nelson Conde, Director, Office of Professional Services & Affiliations
Ernest Williams, Director, Corporate Support Services
Jim Gomez, Interim AVP, Corporate Support Services
Hector Lewis, Associate Director, EITS
Jose Mendez, Coordinating Manager,
John Cuda, Chief Financial Officer, MetroPlus Health Plan
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
Nastasya Barnett, Staff Auditor, Office of Internal Audits
Guzal Contrera, Staff Auditor, Office of Internal Audits
Erica Nairne-Hamilton, Staff Auditor, Office of Internal Audits
Jean Saint-Preux, Confidential Examiner, Office of Internal Audits
Lisa Scott-McKenzie, Deputy Executive Director, North/Central Brooklyn Healthcare Network
Gil Vegas, Assist. Director, Facility Support Services, North/Central Brooklyn Healthcare Network
Rick Walker, Chief Financial Officer, North/Central Brooklyn Healthcare Network
Caswell Samms, Chief Financial Officer, Generations + Northern Manhattan Healthcare Network
Georgia Bond, Interim Regional Director, Generations + Northern Manhattan Healthcare Network
Ruby Ditchfield-Agboh, Chief Information Officer, Generations + EITS

Mark Sollazzo, Associate Director, Material Management, Harlem Hospital Center
Thomas Scully, Senior Associate Director, Harlem Hospital Center
Livio McLennon, Associate Director, Telecommunications, Harlem
Edie Coleman, Controller, Metropolitan Hospital Center
Michell Bisette, Assistant Director, Metropolitan Hospital Center
Timi Diyaolu, Controller, Bellevue Hospital Hospital Center
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
Anthony Saul, Chief Financial Officer, Kings County Hospital
Andrew Tymcoz, Senior Associate Director, Kings County Hospital
Ronald Townes, Associate Director, Kings County Hospital Center
Pamela Williams, Associate Director, Kings County Hospital Center

OTHER ATTENDEES:
PAGNY: Luis Marcos, Chief Executive Officer; Reginal Odom, Chief Human Resources Officer; Anthony Mirdita, Chief Financial Officer; Wendy Wung, Controller; Katherine Kreutz, Executive Assistant

APRIL 16, 2015
AUDIT COMMITTEE OF THE BOARD OF DIRECTORS
NYC HEALTH & HOSPITALS CORPORATION
MINUTES

An Audit Committee meeting was held on Thursday, April 16, 2015. The meeting was called to order at 12:30 P.M. by Ms. Emily Youssouf, Committee Chair. Ms. Youssouf asked for a motion to adopt the minutes of the Audit Committee meeting held on February 19, 2015. 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 Compliance matters.

Ms. Youssouf directed Mr. Christopher Telano, Chief Internal Auditor to begin his presentation.

Mr. Telano saluted everyone and stated that the first item on the agenda is to get an update on an audit that was presented at the February meeting related to the MetroPlus Health Plan, Inc. - Accounts Payable review. He asked the representative from MetroPlus to approach the table. He introduced himself as John Cuda, Chief Financial Officer for MetroPlus. Mr. Telano then said that just to familiarize everybody with what transpired at the February meeting, there was a suggestion for improving operations and efficiency regarding the processing of invoices. At MetroPlus they still use voucher request forms instead of using the approval by senior management granted through the various systems that have been set up for quite a while. At the last meeting there was no commitment as to which direction MetroPlus was going, and was asked to report back to the Committee on their improvements going forward.

Mr. Cuda stated that they took the Committee and Internal Audits' recommendation very seriously. We did take the time to go back and look at our processes and see why we were using the form, which we agree was overkill in the process. We have eliminated that now. We have held training with our areas that have to do with receiving and purchasing and accounts payable where now we can utilize the GHX or the OTPS system to go in, receive an invoice through the mail. Accounts payable can then take the invoice, take the purchase order number, enter it into the GHX system, identify the receiving number and process the payment through GHX in an orderly fashion.

Ms. Youssouf said thank you and welcome to the 21st century. I am very glad that you were able to do that so quickly.

Mr. Telano then touched upon the external audits that are being done by the City Comptroller's Office. The first one is the affiliation agreement with PAGNY at Lincoln Hospital. In March there was meeting called by the Comptroller's Office to discuss the preliminary issues found by the auditors and they found that subcontractor agreements were paid by PAGNY without adequate supporting documentation. They also noted that the recalculation documents were not completed timely although they have been completed and that the bank accounts for the faculty practice plan were not established timely by PAGNY. We expect to receive a draft report from them sometime soon and we will follow that up with an exit conference and go from there. Since this audit started in July 2013, I could not tell you when we will receive this document.

The other item on the Comptroller's audit is the one regarding patient revenue and accounts receivable, and I talked about the same situation the last three or four meetings. We are kind of at a standstill with the Comptroller's Office. More recently we offered the services of my staff, internal auditing, or to hire other professional auditors to conduct their review and they declined both. At this stage, the resolution is pending.

Ms. Youssouf asked Mr. Russo if legal has anything to add. Mr. Russo responded that most recently, the Comptroller cited standards stating they were unable to allow this delegation of activities. Mr. Telano responded to them and pointed out that those are the same standards by which his very office operates, and to that extent there should not be a problem. This was sent some time ago and we are awaiting a response. I neglected to make a follow up call to remind them that we are waiting for a response. The pivotal issue here is that there is language in our enabling broad access to the Comptroller to our books and records, but specifically exempts out medically-privileged information. We believe that they will need medically-privileged information and in fact have proposed ways in which we can get around this, and yet the Comptroller's Office is not comfortable with it because of their interpretation of the government auditing standards, which we believe should not be an impediment to them. We are going to try to work this out, but it is an important issue and we believe that we have to follow both our enabling statute and all other statutes that protect confidentiality.

Mr. Telano said that there are specific citations within those standards that allows the work to be done by other parties other than the auditors, and as long as the party is valid, such as a CPA firm, they should be willing and ready to accept work done by someone else.

Mr. Telano continued on with the completed audits. The first audit is of PAGNY Corporate Operations and he asked the representatives to approach the table and introduce themselves. They did as follows: Luis Marcos, Chair; Reggie Odom, Chief Human Resources Officer; Anthony Mirdita, Chief Financial Officer; Wendy Vung, Comptroller.

Mr. Telano said that I will go over the findings in the report and then you can respond to them. The objectives of the audit were to evaluate the internal controls in place regarding Corporate PAGNY's operations. Corporate employees are those administrative personnel that are located at the five PAGNY/HHC affiliate facilities and the others that work at PAGNY's corporate headquarters, which is located on 125th Street. In total there are 68 active employees with an average salary of $96,000 as December 31, 2014. Overall this was a very good audit. We noted only minor recordkeeping inconsistencies and omissions. Specifically, we found that bank reconciliations were not always properly prepared. We found employee human resources files did not always include exit checklists. In addition, two employees began work in November 2013 but they signed their acceptance letters in January 2014. There were some approved policies and procedures that were not implemented for a couple of processes. The ADP human resources and payroll system inaccurately showed termination dates for active employees, and the timesheet of the Chief Executive Officer was signed and approved by him.

Dr. Marcos stated that thanks to the recommendation, his timesheets are being signed by the head of the Human Resources, and the Board of PAGNY is reviewing them.

Mr. Mirdita said that on the banking ones, there are a couple of findings and I have to say that Ms. Rahman and her team were wonderful. It was a very well-run audit. With regard to the banks, there were checks outstanding over six months; we took this finding very serious. In fact that policy was already put in place six months before the audit began and have already corrected it, but this audit did cover 18 months from July 1, 2013 to December 31, 2014 so it was very large in scope, so that is already been fixed in June. We are monitoring all checks, every six months, we will send out a letter to make sure the outstanding checks that we had are in the second letter and then at some point when the outstanding checks are over the three-year threshold, we will remit them to New York State Unclaimed Funds. We have another year before any of checks are returned.

With regard to the bank reconciliation, preparer and reviewer did not date them – they signed them but did not date them. It is another one of those policies that has been corrected, for a good part of the audit we were not dating them. The last finding on the finance side that was highlighted was the bank recs, we have 18 months of

bank recs. One of those months, the bank rec was done on the 13th business day and the policy in effect calls for the bank recs to be done by 7 business days. In this case the person was on vacation and we were having some staff changes, so we did not have someone trained to fill in. Since then Ms. Vung and her team have fixed all items either previously to the audit commencing or, in this case, it was while the audit was going on.

Ms. Youssouf asked if the policies and procedures for the receiving and corporate employee exit processes have been implemented.

Mr. Odom responded that they have been implemented throughout the process of the audit and some right after the audit. In regard to Human Resources component, we did not have a formal exit process. It was done in different manners, and now we have a process that includes the exit checklist to make sure that items do not walk away as appropriate. Referring to the two individuals that Mr. Telano mentioned, there was some confusion between the site and the corporate human resources team about who was going to manage the hiring process in terms of the offer letter. It was caught later on, which is why a couple of months later we went back and formalized the offer letters. The other item mentioned was probably just an oversight. We were in a personnel action that I was personally involved in and took care of, and nobody on my staff made sure that I followed the right process and put the forms in. We corrected that and I have advised them to make sure the process is followed.

The last item is related to our Active Directory Protocol (ADP) system. It is going through a lot of changes as you know with PAGNY and what is reflected there is that in the prior system there were five separate kinds of sites-based systems. If a person moved from Jacobi to Lincoln, they were effectively terminated at Jacobi and then rehired at Lincoln. That was because the way the process was set up, you could not transfer from a technological standpoint. We got a new ADP system that was implemented in November 2014, and now you can transfer between sites.

Mr. Telano requested that while we have you at the table, I believe it was at the meeting last October or perhaps September in which the Committee had some outstanding questions related to the status of the recalcs and other issues. Let's take advantage of the opportunity for you to give us an update.

Dr. Marcos answered that the first one was related to the Recalcs for 2011, 2012 and 2013, and was happy to report that all those Recalcs have been completed. It was an opportunity not only to do a better job but also to share with the Committee, and he thanked the Committee for being open to discussions and to the fact that recalcs take more than one entity. Recalcs are a process that includes also the facility and central office, so it is very much a cooperative effort and I have to report that those have been finished and the recalcs for December 31st 2014 have been sent to the hospital and now the hospital may have questions and central office may have questions, but we hope that that will be resolved timely.

The second issue had to with contracts, and was happy to report that all the contracts were found to be complete or still with the former contractor – in the case of Downtown Bronx Medical Associates (DBMA), for example, it was DBMA and PAGNY, although from a legal point of view I am told that PAGNY was responsible for it, but we have fixed all of them. There are two or three contracts that involve Columbia University that we are still in cooperation with the facility. Our counsel is here, Mr. Walter Ramos and he confirmed that there are three contracts. Those are still in the process of being negotiated, so they are still open.

Ms. Youssouf stated that I am very happy that guys have worked hard and got through all this and I think your new hires have helped dramatically. Thank you for being so cooperative with us on this – it has been a long process.

Mr. Telano continued with the next audit regarding employee equipment. Although we went to six different sites, because there will be centralized policy being rolled out by the Interim Chief Information Officer, Mr. Sal Guido -- I would like him to approach the table.

Mr. Telano reiterated that IA staff went to six different sites, Kings County, Coney Island, Harlem, Elmhurst and Queens Hospitals and also reviewed the Corporate Department of Enterprise Information Technology Services (EITS). In the summary of findings matrix, strong internal controls do not exist and excessive money is spent as a result of the lack of a centralized function overseeing the issuance, return and disposal of employee equipment. For the purpose of this audit, employee equipment is defined as cell phones, laptops, tablets and pagers.

A summary of the findings are follows; at the facilities, we are using more than one cell phone carrier and there was disproportionate number of plans, lines and monthly costs. For example, at Central Office there were 907 lines, 47 different plans, and the cost of those plans range from a low of $5.95 to a high of $172 per month. Due to the high number of lines, the cell phone invoices were too voluminous to be reviewed. However, we contacted the vendors and got a download of the invoices so we were able to review them and we found that there were many lines not assigned to individuals or they were assigned as spares, so we do not know whose possession these cell phones are in.

We also found a lack of centralized cell phone and laptop inventory at these sites, so we did not know the status of either of those items. At all the sites except for Harlem, the local cell phone policies did not adequately cover the purchasing, the issuance, the monitoring and the return of the items. Lastly we noted that issuance forms were either not located or lack proper approval or justification.

Ms. Youssouf asked if they had plan.

Mr. Guido said that they do and over the history of HHC there were eight separate IT functions within HHC. They were decentralized; each one of them had their own processes and their own audit capabilities. Over the last four months, we have combined those organizations into one for realigning. We are now centrally managing the assets that Mr. Telano alluded to. We have a complete inventory of everything right now. We have very strong controls over the approval process for these devices. We are working with Ms. Zurack and her team on the operating procedures to make sure that everything is seamless and auditable. We are putting in a codified framework for all of our controls not only from this audit, but for all of IT. We plan to have a lot of these components in place by the end of the year. We actually have a very good handle on the mobile devices now throughout HHC. We have a full inventory, we have accounted for each one of the devices. We have terminated quite a few of those lines to reduce our costs, so a lot of good work is in progress.

We are also in the process of signing a central cellphone policy with a vendor to eliminate all of these disparate one-off contracts and things like that. We are working with Ms. Zurack and finance group to get that in place. We welcome Mr. Telano and his team once we complete all work to validate that all the controls are actually in place.

Ms. Youssouf stated that I think that is great. It would be good maybe at some point if you can let us know how many devices, phone, laptops we have now and this is what our costs were. It sounds like there is going to be significant savings from this, which is very well done and you should thank Mr. Telano for finding this out.

Mr. Guido thanked Mr. Telano.

Ms. Zurack commented that in all fairness, I do not know the date of the audit, but Mr. Guido has been working with us on this for quite a while. He probably was working on it even before the audit, just to give credit where it is due.

Mr. Guido said that we were just getting there, so we had a couple of other priorities that needed to get handled first, and this was on the list, so as Mr. Telano's team were coming in, we were actually rolling this out. First site it was rolled out, so we are pretty confident that we have the controls in place, and again we welcome Mr. Telano's team back to validate those controls.

Mr. Telano continued on with the next audit and said that this is similar to the employee equipment audit. It was done at various HHC facilities. We went to the Generations Plus Network, South Manhattan Network and North/ Central Brooklyn Healthcare Networks and once again Corporate Support Services. Coincidentally, there was a corporate initiative headed by EITS and Corporate Procurement to centralize and manage the print service solution, Mr. Telano asked the representatives to join Mr. Guido at the table. They introduced themselves as follows: Paul Albertson, Senior Vice President, Material Management; Jim Gomez, Interim AVP at EITS.

Mr. Telano once again stated that I will go through the findings and you can address them. Overall we found that the printing activity is managed differently throughout the Corporation. As a result of those operations, we found the following inconsistencies. Different printer equipment vendors were being used at different prices and for different services. Some sites leased their equipment while others rented them. Half of the sites we visited charged back their internal services to the requesting department while the other half did not. Each facility used their external printing services with Vanguard differently as indicated by the diverse range of printing expenses, and equipment usage and monthly payments were not adequately monitored at all six locations.

Mr. Gomez stated that Mr. Telano knows my appreciation for his auditing efforts and all the things that are uncovered. I am going to go through them, but my answers are going to sound remarkably like Mr. Guido's answers because we are all part of the similar efforts to consolidate under one organization as part of the realignment. The different equipment from different vendors will be addressed by our Request for Proposal (RFP). We currently have an RFP out on the street today with the objective to select one vendor to provide support to all our printing services and printers across the entire Corporation, which includes the six print shops that were part of the audit. Various vendor responses are coming in.

Ms. Youssouf asked if the plan would be to replace Vanguard. To which Mr. Gomez answered that it would be replacing our in-house printing work, but it is just a contract for the equipment – it will be standardized equipment. It will be either leased or rented depending on what the vendors bring back as a solution. It will not really impact our need to go externally if we do not have the capability in-house. This is what Vanguard represents. Due to our fractured system, we now have six print shops and six different networks doing six different types of work. There are different organizations in each with different functionality in each, so that is why you see such disparate spending with Vanguard, which will be addressed in the outsourcing agreement. From a charge-back perspective, Mr. Guido has been working with Ms. Zurack for a while on a model to charge back for services.

Mr. Guido added that that is correct. We are looking from a wireless standpoint, a different mechanism of supplying those wireless devices to the resources within HHC. We are looking at a bring-your-own-device (BYOD) policy, and allowing us to secure those devices while allowing our resources to come in use their own devices for access to our environment.

Ms. Zurack commented that all those discussions took place before the Hillary Clinton incident. We thought about it -- would be an efficiency and a major savings to allow people to use their personal devices and we would support their using their personal devices and we can control and save on it.

Mr. Albertson stated that we have really broken our approach to our print servicing into three different components. The biggest one, which Mr. Gomez was talking about, relates to all of the photocopy machines, the desktop printers that we have throughout the corporation. We have about 2,300 different copy machines across the Corporation. We own some, lease some, rent some; we have about 23,000 desktop printers. Between the two of them, the 25,000 devices that we have, we print about 400 million black and white copies a year and another 25 million color copies, so our interest in this opportunity is being able to identify a single vendor who is going to be managing all of our printing. We want this vendor to take all of the existing agreements and manage them and help us in the context of doing so. We have worked with a value-analysis team which has representatives from each of the networks from Mr. Gomez's office, finance and a few other departments to help us put this kind of complicated document together, have identified a series of key performance indicators that relate to what the vendors have to provide, what the future state looks like as it relates to our engagement with EPIC and the fact there will a natural attrition of paper as an outcome of different applications going up that currently are paper driven now. We will be working with each of the facilities as we roll this out to right size it with both the IT liaison and the appropriate chief operating officers to make sure we work together to achieve this.

Ms. Youssouf asked that if the point is to eventually get to one contract? To which Mr. Albertson replied yes, it is a single contract and a single vendor. Mr. Gomez added that we will actually manage the contract and provide governance over the contract.

Ms. Youssouf asked if they will keep all of the various contracts. Mr. Guido responded no, that that is not the intent. The intent is to collapse all of the subcontracts into this one major contract. One vendor will manage our printing facilities across HHC thus should reduce our costs, but with that there is more to it. There are also 23,000 printers that we have today – is that necessary? It is more of a process driven as well as a secondary to make sure that we are rightly aligned with the requirements and the capabilities that IT has to provide from standpoint.

Mrs. Bolus asked, you say that you have 2,300 copiers. Mr. Guido answered correct, copiers are about 2,300 and 23,000 printers.

Mrs. Bolus then added that that is difficult then when you consider that you will probably need about ten at least in each of the buildings because each department will want their own and who owns the software because the software has to have HHC letterhead or whatever you are going to put on these objects that you are using. There are people who actually know the software and design what is necessary. Mr. Guido responded that we do have quite a few of these here. We have design folks, communication folks that have been trained in this area with specifically more of these type of features and functionality.

Mr. Martin asked if they did an assessment as to whether or not we need print shops.

Mr. Albertson answered that that is the other component that we are talking about. One is the RFP that is now on the streets relates to the volume of work that we are doing. With the print shops themselves, we know that there will be a reduction in the work they are being asked to do as an outcome of EPIC going up because they currently print a lot of documents that are part of the patients' record that we will not need going forward.

The second piece is, we collected all the information on what every print shop is doing and the variability that they are engaged in. There is going to continue to be a need for internal printing on a more modest rate than

what we are currently doing. Some of them do work that others send out to Vanguard or other companies, so we collected all of that information with the intent of reducing the work variability across the facilities, reducing the number of shops that are probably going to be needed and the work that is actually being done.

Ms. Youssouf asked with the advent of EPIC, shouldn't that be a major reduction? Mr. Guido said yes, it is a lot of different areas. The print shop is one the reduction of these 23,000 printers is another.

Ms. Youssouf asked why we still need Vanguard. Mr. Albertson responded as we are evolving the introduction of EPIC, it should be going away, but over the next three or four years while EPIC continues to roll out, there will be some facilities that still need those forms to be part of the patient's record.

Ms. Youssouf stated that that was the question. To which Mr. Guido responded that that it is only for a short term. As we modernize and digitize most of those files and records, the requirement for Vanguard would dissipate over time.

Mr. Martin asked if we have print shops at all of the facilities. Mr. Albertson responded that we have nine print shops in total today -- one in Central Office and eight in the facilities.

Ms. Youssouf stated that we will be looking forward to hearing from you – now that we have all this information. I think that hopefully it would be a nice savings benefit and thank you.

Mr. Guido once again thanked Mr. Telano and said that we do appreciate all the work and look forward to seeing you again.

Mr. Telano continued by stating that on page 10 and 11 of the briefing it gives you the status of audits we have in progress and the status of our follow-up audits and that that concludes my presentation.

Ms. Youssouf directed the meeting to Mr. Wayne McNulty for the Compliance update.

Mr. McNulty, HHC's Senior Assistant Vice President and Chief Corporate Compliance Officer, introduced himself and saluted everyone. He began his presentation by providing a follow up report on HHC's compliance with the HIPAA Security Rule risk analysis requirement, which he initially reported to the Audit Committee of the HHC Board of Directors (the "Committee") in February. He advised the Committee that under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHC is required to implement a risk-assessment program, which requires HHC to conduct an accurate and thorough assessment of the potential risks and vulnerabilities of the confidentiality, integrity, and availability of electronic protected health information ("EPHI") that is accessed for and transmitted by HHC's systems and applications.

He reminded the Committee, in sum and substance, that his February report on the Corporation's compliance with the risk-analysis requirements held that the inventory of HHC's information systems and applications that access, house and transmit EPHI was a work in progress and therefore was not comprehensive at the present. He added that, although HHC's Enterprise Information Technology Services ("EITS") has taken numerous and significant measures to enhance and maintain 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 appeared that further measures were required by EITS to fully satisfy the extensive risk analysis and implementation measures required under the security rule.

Mr. McNulty explained that, to perform an adequate risk analysis, the following eight specific steps must be taken: (i) outline the scope of the analysis including the potential risks, threats and vulnerabilities to the confidentiality, availability and integrity of all EPHI that HHC creates, receives, maintains and transmits; (ii) collect and gather the information where it is stored; (iii) identify and document potential threats and vulnerabilities; (iv) access current security measures; (v) determine the likelihood of threat occurrences; (vi) determine the potential impact of threat occurrences; (vii) determine the level of risk present; and (viii) document all findings and risk analysis conclusions.

He advised the Committee that, since his last report to the Committee, EITS had taken steps to procure a third-party vendor to provide, among other things, the following services: (i) a HIPAA risk analysis on the applications of electronic protected health information; (ii) a HIPAA compliance assessment; (ii) the application security penetration test; (iii) an infrastructure security internal penetration testing; (iv) infrastructure internal server penetration assessment; and (iv) a vendor/third party assessment.

Mr. McNulty, in summary, informed the Committee that, Mr. Sal Guido, the Acting Corporate Information Officer, who was present before the Committee, would inform the Committee of any additional measures that EITS has taken or plans to take regarding this matter.

Mr. Guido introduced himself and stated, in summary, that his office has worked with Mr. McNulty for quite some time on getting a lot of the audit requirements in place, getting external auditors to come in and audit HHC, and have been very closely aligned with Mr. McNulty and his office on getting these things done. Mr. Guido further stated, in sum and substance, that, as Mr. McNulty has alluded, EITS put out a solicitation to security vendors through City and State contracts to provide services around application security risk assessment from preliminary perimeter as well as the HIPAA requirements from an audit standpoint. He added that, EITS had received those solicitations back and was hopeful to have those secured within the next 30 days.

Mr. Guido continued by stating that, from an application standpoint, we have conducted an inventory of all of our applications and the PHI associated with it, and the way it will work is we have 131 applications that you have PHI on. In summary, he explained that, over the next three years, approximately 40 applications a year would undergo a risk assessment and, where necessary, resulting remediation plans and remediation implementation of those same applications. He advised that the reason why the whole 131 could not be accessed was because it was not practical at this time, stating that his office wanted to take a higher priority application, make sure we secure those and go on from there.

Ms. Youssouf commented that that is a big job. Mr. Guido answered that a lot of it was in progress over the last six months with the realignment, so his office understood where some of the deficiencies were and started to address these things very rapidly. He added that his office really secured HHC's infrastructure from the outside world. He explained that this was really securing it from the inside world.

Mrs. Bolus asked if he thinks we need to reemphasize what is a breach to staff. Mr. McNulty said that the education has to be almost continuous, adding that, although we have HIPAA training and all the employees and workforce members are going into the training, periodic notices are sent to employees, and his office speaks to employees at the facilities. He informed the Committee that he has personally performed walkthroughs throughout the various facilities of the Corporation and stopped employees in the hallway and asked them about the different HIPAA procedures, and for the most part they were very familiar with the policies and procedures. In summary, Mr. McNulty reiterated that the education has to be continuous, and his office has to keep at it with respect to privacy and security and any other compliance policies.

Mr. Guido added that we have to put some technology in place to help Mr. McNulty out to actually track where PHI goes, internal as well external, so we understand exactly where the data is. It is protected internally and if any of it is going out from an unauthorized matter, so I think from that standpoint we have done a pretty good job. The problem with security is that things change very rapidly, and we just have to keep up on it.

Ms. Youssouf requested that it would be good if you can come and give us a little update in a couple of months because it is a huge amount of issues that are on your plate, and it would be good to keep us informed. We will be completing our fiduciary responsibility to make sure it is all going along.

Dr. Boufford asked if we are managing HIPAA and research and do we have a process to make more people's patient records available to them. To which Mr. McNulty responded that the issue with respect to HIPAA and human-subject research, we have HIPAA operating procedures in place that are specific to research use and disclosure and access of PHI. He added that, under HIPAA privacy rules, it does allow some access to PHI by researchers. He commented that, however, New York law is more stringent, so there are additional controls if you are a hospital or healthcare provider with regard to accessing PHI for research purposes, but we treat it just like any other PHI with respect to security and privacy, and clinical research is an area that we will be auditing to ensure there is no inappropriate access for that particular source.

Mr. Guido said that currently we have an operational patient portal that provides those records to the patients. They have to log into our portal in order to do so. We also have capabilities of transferring data of patients from physician to physician through referrals in that system as well. In the future we will be putting something called "My Chart" in place for EPIC, which allows for a little bit more richer content of those patients records for their viewing. With that comes a security concern – with the security, we have actually put in place something called federated active directory or a federated way of allowing our patients to come into the portal by authenticating off of a known database like DMZ so we are working with the DMZ to make sure that from identity-management standpoint that the patients that are actually coming into the portal are actually the right people. That has to be work out with Ms. Zurack (Senior Vice President of Finance and Managed Care/Chief Financial Officer) and Finance as well as quite a few other organizations within HHC to see how do we start looking at bio-med devices for identification of those patients, which has great benefits to us in a number of different ways. One is we know who the patient is and second is that we would eliminate or greatly reduce the need to clean up data on an annual or semi-annual basis. Those are the technologies that we are looking at to really secure and make our patients feel much safer about accessing that information on line.

Mr. McNulty continued on with Section II, the Compliance Reporting Index. He advised the Committee that for the first quarter of calendar year 2015 there were 81 compliance-based reports. He elaborated the following with regard to these reports: one was classified as a Priority A report, three were Priority B reports, and 49 were classified as Priority C reports. He stated that, because these reports involved ongoing investigations, he would discuss the pertinent reports in executive session. He then moved on to Section III, Privacy Reporting Index for the first quarter of calendar year 2015. He advised the Committee that there were 45 reports of potential HIPAA violations. He stated that fourteen of these reports were confirmed breaches of PHI. In summary, he explained to the Committee that term breach is defined as the impermissible use, access, acquisition or disclosure of PHI in a manner that compromises the security and privacy of PHI maintained by the Corporation.

Mr. McNulty went on to further explain that, to have a breach, his office has to do an assessment where the following is reviewed: (i) the nature and extent of the protected health information involved; (ii) who was the unauthorized person who accessed the information; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI had been mitigated.

Mr. McNulty highlighted, in summary, the following privacy incidents:

(i) one occurred at Harlem Hospital Center where several employees accessed the record of a patient inappropriately. Mr. McNulty informed the Committee that, as a result, nine employees were disciplined for improper access, and a breach notification was sent to the affected patient in early April. Ms. Youssouf asked if they all targeted one patient. Mr. McNulty responded that the patient was an employee, so they accessed the patient's records inappropriately and they were all suspended for those actions.

(i) another incident occurred at Coler Nursing Facility, which involved 27 residents whose medications were being transported from the Henry J. Carter Facility to the Coler Facility. Mr. McNulty informed the Committee that seven bags of medication fell off the back of the transporting van because the van door was open. He further informed the Committee that someone pulled the driver over and alerted the driver that the van door was open; hospital police later checked the security camera and confirmed the same. Mr. McNulty advised that, as a result, breach notification letters were scheduled to be sent before April 20th.

Mr. McNulty moved on to Section IV, the Monitoring of Excluded Providers. He explained that there were no excluded providers since the last time the Audit Committee convened. However, he stated that his office did uncover one vendor that was excluded from the General Service Administration list - the federal list for vendors - which was referred to the Office of Procurement for handling. He stated that the Office of Procurement determined that the vendor was inactive and was no longer used by HHC. As a result, Mr. McNulty explained, there were no potential overpayment issues that required addressing.

Ms. Youssouf said that a few years we had a lot of excluded providers and I want to congratulate everybody who is involved in really clearing this up. You all have done a great job.

Mr. McNulty continued with Section V, the Revision of Corporate Policies and Procedures, and provided a status update. As previously communicated, he said, his office would be revising Operation Procedure 50-1, which is the Corporate Compliance Program operating procedures, the HHC Corporate Compliance Plan, and HHC's Principles of Professional Conduct. He elaborated that, because of all these procedures touch on compliance and corporate governance issues, he would disseminate the same to the President and CEO for review and also to the Committee for review and comment before they were finalized and executed and approved by the President.

Dr. Boufford suggested that Mr. McNulty speak to the CEO of Maimonides Hospital on the Principles of Professional Conduct. Dr. Boufford commented that Maimonides has done some really interesting work in this area especially regarding the behavior of physicians relative to other staff. They have implemented something called a code of mutual respect and a number of other steps.

Mr. McNulty said that he will definitely give Maimonides a call. Currently, he stated, the Principles of Professional Conduct ("POPC") just covers basically fraud, waste and abuse and very little with regard to privacy. He stated that the POPC should cover a code of conduct and a way of doing business and it should cover issues that affect human resources and issues that affect conflicts of interest. He stated that his office would be expanding the same to cover those particular issues. He explained that he would be working with Carolyn Jacobs, Senior Vice President for Human Resources for input; he advised, in summary, that he would also seek input from the Executive Compliance Work Group and leadership before presenting the same to the Audit Committee and the President for review.

Dr. Boufford commented that I think it is a great opportunity for HHC because especially there are a number of organizations looking at sort of administrative checklists for issues of diversity, cultural competence, and there is a

lot of work that is been done in this area and I am glad to hear you thinking in broader terms because I think HHC can set a standard for a lot of things that other organizations are going to have deal with going forward. It is very exciting – look forward to tracking it with you.

Mr. McNulty continued on with Section VI, Compliance Training Update. He informed the Committee that Department of Social Services regulations require his office to provide training and education to all affected employees and persons associated with the Corporation, including executives and the governing body members, on compliance issues, expectations, and the compliance program operation. In summary, he further informed the Committee that his office has the following four modules: (i) one for physicians; (ii) one for all individuals that are licensed under the Title VIII if the Education Law, such as physical therapists, nurses and occupational therapists, as well as other individuals involved with patient-care activities; (iii) one for Group 11 employees; and (iv) one for the Members of the HHC Board of Directors.

He advised the Committee that his office revised the training modules for the physicians and healthcare providers. Those are currently live. He stated that Group 11 training module was being finalized and was expected to go live the next day. He stated that the training module for the Board of Directors was expected to go live sometime next week. He commented that he was working with Mr. Guido's office; Mr. Guido will try to make sure that the Board training will be available for all Board members on their iPads.

He informed the Committee that over 20,000 healthcare professionals were enrolled in the Healthcare Professionals Module. He reported that over 5,000 individuals completed the module, which is a 20 percent completion rate. He informed the Committee that there were 6,000 individuals enrolled in the Physicians Module, advising that over a thousand have completed the same - a 27 percent completion rate. He stated that outreach to all of the chiefs of services at the various location facilities and all the administrative heads at the various facilities has begun to ensure these numbers would go up; he stated that he was quite confident the next time he came before the Audit Committee that both of those rates will be somewhere between 75 and 85 percent. He stated that by the time June 30th rolls around, we will definitely be at least at 90 percent for both those modules.

Mr. McNulty discussed the Corporate-wide risk assessment process, stating that at some point in May, the OCC would begin conducting the Calendar Year 2015 Corporate-wide risk assessment. The results of this risk assessment, he added, would be used in pertinent part by the OCC to develop the Fiscal Year 2016 HHC Corporate Compliance Work Plan. He commented that the risk assessment process was expected to be completed by mid-July. He explained that the risk assessment was required under the Department of Social Services regulations and the Office of the Inspector General Guidance to Hospitals. Mr. McNulty stated that risk throughout the Corporation would be reviewed by, in sum and substance, taking the following three measures: (i) interviewing employees directly and asking them what risks do they observe in their daily work; (ii) conducting a survey of employees by asking them what three things keep them up at night or what three areas concerns them; and (iii) sending to all the various compliance committee and executive compliance work groups a predefined list of risks. He explained that the Office of Inspector General and the Office of the Medicaid Inspector General has send out fraud alerts, established work plans, and established a list of predefined risks that the OCC would assess to determine if they are applicable to the Corporation.

He continued by explaining that the OCC would then score and prioritize those risks and present the same to the Committee so that the Committee and the Board can accept the risk and develop risk tolerance and appetite strategies, which he further explained would be the last step of the risk-prioritization process. He reminded the Committee that KPMG mentioned the same in their last management letter just as an information item, thus, his office would definitely address the same..

Ms. Youssouf then called for the executive session at 1:34 pm. Once over, Ms. Youssouf stated that during the executive session, the Committee discussed confidential matters related to specific patient health information.

There being no further business, the meeting was adjourned at 2:00 P.M.

Submitted by,

Emily Youssouf
Audit Committee Chair

KPMG

cutting through complexity

New York City Health and Hospitals Corporation

Presentation of the 2015 Audit Plan to the Audit Committee

June 11, 2015

Overview of 2015 Audit Plan

KPMG Engagement Team

Engagement Team

- Maria Tiso - Lead Engagement Partner
- Mike Breen - Engagement Partner
- Sean Egan - MetroPlus / HHC Insurance Company Partner
- Joseph Bukzin - Lead Senior Manager
- Ryan Santonacita - Manager
- Chris Dominianni - Regulatory Reports Senior Manager
- Linda Baharestani - MetroPlus Health Plan Manager
- Kristen Cooper - HHC Insurance Company Manager
- Beatriz Mendoza - Lead Senior Associate
- Marlee Fisher - Senior Associate

Other Resources

- BCA Watson Rice Staff - Minority Business Enterprise
- Healthcare Management Solutions Staff - Women's Business Enterprise
- Internal audit assistance

Subject Matter Professionals

- Felicia Tucker - Partner, Tax
- Devin Duncan - Manager, Tax
- Rob Mishler - Senior Manager, Actuary
- Peggy Hermann - Director, Actuary
- Glennon Moyers - Partner, Compliance
- Kirk McNeil - Senior Manager, Reimbursement
- Anthony La Rocca – Director, IT

Other Partners

- Jim Martell - Healthcare Resource Partner
- Steve Reader - Concurring Review Partner
- Renee Bourget-Place - MetroPlus Concurring Review Partner
- Rich Catalano – HHC Insurance Concurring Review Partner
- John Hawryluk - Healthcare DPP Liaison
- Mark Jamilkowski – Managing Director, Insurance Resource

KPMG Deliverables and Other

- Auditor's report on the financial statements of:
  - HHC
  - MetroPlus Health Plan's (calendar year-end)
  - HHC Insurance Company, Inc. (calendar year-end)
  - HHC ACO, Inc.
- Management letter to Audit Committee and management on our recommendations regarding internal controls and other operational matters
- Auditor's report on the cost reports for:
  - Diagnostic and Treatment Centers
  - Skilled Nursing Facilities
  - Long-Term Home Health Care Program
- Annual Debt Compliance Letter

Other:

- 250 hours of Tax Advisory services over the contract period
- Provide five full days of continuing professional education (CPE) per year for up to 140 attendees per year

Objective of an Audit

- The objective of an audit of the financial statements is to enable the auditor to express an opinion about whether the financial statements that have been prepared by management with the oversight of the Audit Committee are presented fairly, in all material respects, in conformity with generally accepted accounting principles (GAAP)
- We plan and perform the audit to obtain reasonable assurance about whether the financial statements taken as a whole are free from material misstatement, whether from error or fraud.
- Our audit includes:
  - Performing tests of the accounting records and such other procedures, as we consider necessary in the circumstances, based on our judgment, including the assessment of the risks of material misstatement to provide a reasonable basis for our opinion(s)
  - Evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, and evaluating the overall presentation of the financial statements

Audit Responsibilities

Management is responsible for:

- Adopting sound accounting policies
- Fairly presenting the financial statements, including disclosures, in conformity with GAAP
- Establishing and maintaining effective Internal Control Over Financial Reporting (ICFR), including programs and controls to prevent, deter, and detect fraud
- Identifying and confirming that the Corporation complies with laws and regulations applicable to its activities and for informing the auditor of any known material violation of such laws and regulations
- Making all financial records and related information available to the auditor
- Providing unrestricted access to person's within the entity from whom the auditor determines it necessary to obtain audit evidence
- Adjusting the financial statements to correct material misstatements
- Providing the auditor with a letter confirming certain representations made during the audit that include, but are not limited to, management's:
  - Disclosure of all significant deficiencies, including material weaknesses, in the design or operation of internal controls that could adversely affect the Corporation's financial reporting
  - Acknowledgement of their responsibility for the design and implementation of programs and controls to prevent, deter, and detect fraud
  - Affirmation that the effects of any uncorrected misstatements aggregated by the auditor are immaterial, both individually and in the aggregate, to the financial statements taken as a whole

Audit Responsibilities (continued)

The Audit Committee is responsible for:

- Oversight of the financial reporting process
- Oversight of the establishment and maintenance by management of programs and internal controls designed to prevent, deter, and detect fraud

Management and the Audit Committee are responsible for:

- Setting the proper tone and creating and maintaining a culture of honesty and high ethical standards

The audit of the financial statements does not relieve management or the Audit Committee of their responsibilities.

Audit Responsibilities (continued)

KPMG is responsible for:

- Forming and expressing an opinion about whether the financial statements that have been prepared by management, with the oversight of the Audit Committee, are presented fairly, in all material respects, in conformity with GAAP
- Planning and performing the audit with an attitude of professional skepticism
- Conducting the audit in accordance with professional standards and complying with the Code of Professional Conduct of the American Institute of Certified Public Accountants, and the ethical standards of relevant CPA societies and relevant state boards of accountancy
- Evaluating ICFR as a basis for designing audit procedures, but not for the purpose of expressing an opinion on the effectiveness of the entity's ICFR
- Communicating to management and the Audit Committee all required information, including significant matters
- Communicating to the Audit Committee and management in writing all significant deficiencies and material weaknesses in internal control identified in the audit and reporting to management all deficiencies noted during our audit that are of sufficient importance to merit management's attention

Independence

KPMG maintains a comprehensive system of quality controls designed to maintain our independence

- Pre-approval of all worldwide engagements by the audit engagement team through Sentinel, a KPMG independence verification system
- Monitoring employment relationships
- Tracking partner rotation requirements using PRS, the firm's automated partner rotation tracking system
- Automated investment tracking system used by all KPMG member firms (KICS)
- Training and awareness programs
- Compliance testing programs
- Annual reporting to the Audit Committee

Financial Statement Audit Timetable

HHC:

April – June 2015

- Hold planning meetings with management
- Determine the audit strategy
- Perform analysis of business issues and identification of audit focus areas
- Hold audit team planning meeting
- Review of December 31, 2014 internal financial statements
- Communicate with management regarding IT related procedures
- Test IT General Controls
- Present 2015 Audit Plan to Audit Committee

June – July 2015

- Identify financial statement and assertion level fraud risks
- Perform test of operating effectiveness of controls
- Perform substantive audit procedures relative to interim account balances, including review of patient accounts receivable valuation utilizing data and analytics tool
- Review of non-routine transactions through June
- Perform SAS 99 fraud meetings
- Complete interim testwork at various facilities and at Central Office, which will include testing controls over various processes such as patient accounts receivable, procurement, fixed assets, and treasury.

Financial Statement Audit Timetable (cont'd)

August – September 2015

- Final phase of year-end audit to begin July 13, 2015 through September 25, 2015
- Perform remaining substantive audit procedures
- Perform procedures to roll forward interim account balances to year end
- Perform SAS 99 fraud meetings
- Financial statement audit closing meetings with management
- Form audit conclusions
- Discuss key issues and deficiencies identified with management (provide draft management letter)
- Attend Audit Committee meeting to review draft financial statements, management letter and perform required communications
- Finalize and issue audit opinion on financial statements

October 2015

- Issue debt covenant compliance letters

November 2015

- Present final management letter to Audit Committee

Financial Statement Audit Timetable (cont'd)

Other:

December 2015 – January 2016

- Complete interim testwork for Metroplus Health Plan audit
- HHC ACO audit and issuance of financial statements

February - March 2016

- Final phase of Metroplus Health Plan audit and issuance of financial statements

May - August 2016

- Issue auditor's reports on cost reports for the skilled nursing facilities (RHCF-4), diagnostic and treatment centers (ACHF) and long-term home health care facility (LTHHC)
- HHC Insurance Company audit and issuance of financial statements

Audit Matters

We identify audit matters that could have a material impact on the Corporation's financial statements. We then consider these matters when developing our audit approach and tailor our procedures to address these risks.

Significant Audit Areas

- Valuation of patient accounts receivable
- Third-party and pools receivables/ liabilities
- Postemployment benefit obligation other than pension (OPEB)
- Pension obligation
- Liquidity issues

Other Audit Areas

- Patient accounts receivable (completeness, existence and accuracy)
- Commitments and contingencies
- Related party transactions

Audit Matters, continued

Significant Non-Routine Transactions / Other Items

- Meaningful Use Incentive Payments
- Delivery System Reform Incentive Payment (DSRIP) Program
- Upper Payment Limit (UPL) Funding from CMS and NYS
- FEMA Awards
- Potential sale of dialysis services
- EPIC Implementation
- Gotham FQHC Look-a-Like

Information Technology Matters

- General information technology environment
- Review and test IT access controls
- Review and test the controls over changes to the IT system
- Verify that the Corporation's detection controls are functioning as intended
- Inform management of any performance improvement observations

Planned Use of Minority Business Enterprise (MBE) / Women's Business Enterprise (WBE) / Internal Audit

KPMG plans to utilize the MBE, WBE and internal audit in the following areas:

	MBE	WBE	Internal Audit
Third party payor liabilities		X	
Site visits			X
Grants receivable / Grant revenue			X
Capital assets			X
Cash			X
Debt / Deferred financing			X
Accounts payable / OTPS			X
Cost Reports (AHCF, RHCF-4, LTHHC)	X		

General Considerations – Fraud Approach (How Risks are Addressed)

Identification of fraud risks

Perform risk assessment procedures to identify fraud risks, both at the financial statement level and at the assertion level

Discuss among the audit team the susceptibility to fraud

Perform fraud inquiries of management, the Audit Committee, and others

Evaluate broad programs/controls that prevent, deter and detect fraud

Response to identified fraud risks

Evaluate design and implementation of antifraud controls

Test effectiveness of antifraud controls

Address revenue recognition and risk of management override of controls

Perform specific substantive audit procedures (incorporate elements of unpredictability)

Evaluate audit evidence

Communicate to management and the Audit Committee

Planned SAS 99 Fraud Interviews

We plan to perform the following SAS 99 fraud interviews for the annual audit ending June 30, 2015:

Emily Youssouf - Audit Committee Chair

Gordon Campbell- Acting Chairman of the Board

Dr. Ramanathan Raju - President and CEO

Marlene Zurack - Senior Vice President, Finance and CFO

Wayne McNulty - Corporate Compliance Officer

Ross Wilson - Senior Vice President, Quality and Corporate Chief Medical Officer

Julian John - Corporate Comptroller

Salvatore Russo - General Counsel

Chris Telano - Chief Internal Auditor and Assistant Vice President

Paul Albertson - Chief Procurement Officer

* Others may be identified during the course of the audit

Other Considerations

Liquidity

The Auditor's Responsibility under AU-C Section 570, The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern

- The auditor has a responsibility to evaluate whether there is substantial doubt about the entity's ability to continue as a going concern for a reasonable period of time….The auditor's evaluation is based on knowledge of relevant conditions and events that exist at or have occurred prior to the completion of fieldwork.
- The auditor's considerations should be based on knowledge of the entity, its business, and its management, and should include (a) reading of the prospective financial information and the underlying assumptions and (b) comparing prospective financial information in prior periods with actual results and comparing prospective information with the current period results achieved to date.

The following are going concern considerations:

- Net deficit position as of June 30, 2013, June 30, 2014, and March 31, 2015
- Loss from Operations for the years ending June 30, 2013 and June 30, 2014, and for the nine month period ending December 31, 2015
- Positive working capital as of June 30, 2013 and June 30, 2014
- Positive operating cash flow as of June 30, 2013, June 30, 2014, and March 31, 2015
- HHC was in compliance with financial debt covenants as of June 30, 2013 and June 30, 2014

Other Considerations (continued)

Liquidity (Continued)

KPMG will request information about management's plans

- Fiscal 2016 budgets and cash flow projections
- Written representation from management regarding plans
- Board and Finance committee meeting minutes
- Restructuring reports and findings, if applicable

Additionally, KPMG will review

- Fiscal 2015 budget to actual results (reliability of budgeting process)
- Working capital, operating income (loss) and cash flows from operations (liquidity)
- Continued support from the City of New York

New Accounting Pronouncements

- **GASB Statement 69, *Government Combinations and Disposals of Government Operations***
  - Effective for June 30, 2015
- **GASB Statement 70**, ***Accounting and Financial Report for Nonexchange Financial Guarantees***
  - Effective for June 30, 2015
- **GASB Statement 72, *Fair Value Measurement and Application***
  - Effective for June 30, 2016, Early adoption permitted

Audit Committee Resources

KPMG's Healthcare & Pharmaceutical Institute

The KPMG Healthcare & Pharmaceutical Institute has been established to provide an open forum for business leaders from across the industry to share perspectives, gain insight, and develop approaches to help balance risks and controls, and improve performance. To learn more about the HPI and become a member, please visit:

www.kpmginstitues.com/healthcare-life-sciences-institute/

KPMG's Audit Committee Institute

KPMG created the Audit Committee Institute (ACI) to serve as a resource for audit committee members and senior management. ACI's stated mission is to communicate with audit committee members and enhance their awareness, commitment, and ability to implement effective audit committee processes. The following link will take you to ACI website which contains information on upcoming seminars and publications available for download and also to become a member:

www.kpmginstitutes.com/aci/index.aspx

KPMG's Audit Committee Insights

KPMG's Audit Committee Insights is a biweekly e-mail alert that's designed to help audit committee members stay up to date on recent events. ACI editors review hundreds of respected business journals, industry publications, and association web sites to bring the information to your desktop in an easy to read email. You can click the articles that interest you. You can sign up for this e-mail at the following link or when you chose to become a member of the ACI:

http://www.kpmginsights.com/aci/insights/2012/kpmg-audit-committee-insights-newsletter.aspx

NEW YORK CITY HEALTH AND HOSPITALS CORPORATION

AUDIT COMMITTEE OF THE HHC BOARD OF DIRECTORS

Corporate Compliance Report

June 11, 2015

Table of Contents

Agenda

I. Interim 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 ("Sr. AVP/CCO"), 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"). HIPAA 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]

2) As the Audit Committee was previously informed, to meet HIPAA requirements, 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 a 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, store, 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 several of its applications,

[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 for 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).

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

OCC's Previous Recommendations

4) The OCC recommended to EITS that, among other things, any risk analysis performed by EITS to satisfy the Security Rule consists of and document the following eight steps:

(i) Outline the scope of the analysis (including the potential risks, threats, vulnerabilities to the confidentiality, availability and integrity of all EPHI that HHC creates, receives, maintains, or transmits);

(ii) Collect/gather data (identification of where data is stored);

(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 present; and

(viii) Document all findings and risk analysis conclusions.

April Audit Committee Status Update

5) During the April 2015 Audit Committee meeting, Sal Guido, Senior Assistant Vice President/Acting Chief Information Officer, provided the Audit Committee with the measures EITS planned to take to address the risk assessment requirements mentioned above. Mr. Guido informed the Audit Committee of the following:

- EITS issued a solicitation out to security vendors to provide services around application security risk assessments; preliminary perimeter security assessments; and to meet the HIPAA requirements from an audit standpoint;

- EITS has conducted an inventory of all of its applications and the PHI associated with it and has identified 131 applications that house or transmit PHI; and

- Over the next three years EITS will perform a risk assessment and remediation plans on approximately 40 applications per year.

Present State of Remediation Process

6) At the present state, a vendor has been selected to assist with the risk analysis process. EITS and OCC were part of the selection committee for the vendors that responded to the Request for Proposal. After a series of interviews and assessment sessions, a vendor has been selected to provide the services mentioned in the previous paragraph for a period of three years. Over the course of three years, the vendor will perform several assessments as detailed above. A kick-off call took place on 5/26/2015 at which time the selected vendor was directed to put together a comprehensive Statement of Work detailing all the activities they will undertake while performing audit functions throughout the Corporation..

II. External Audits – U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR"): *Status Report*

1) In April 2014, the OCC advised the Audit Committee that OCR was conducting a review of Metropolitan Hospital Center's ("Metropolitan or "MHC") compliance with certain federal civil rights and health information technology laws, including Metropolitan's policies, procedures, and practices related to: (i) meaningful access to services and programs for limited English proficient ("LEP") individuals; (ii) equal access to services and programs for individuals with HIV; and (iii) the privacy and security of individuals' protected health information "(PHI") and their rights with regard to such information.

2) The OCC, with the assistance from and information provided by Metropolitan executive and senior leadership, as well as senior leadership in Central Office, responded to OCR's query on April 30, 2014.

3) The OCR subsequently requested additional information regarding the scope of HHC's risk analysis process, specifically asking for a comprehensive risk analysis which identifies risks and vulnerabilities for the organization-wide EPHI systems and applications including, but not limited to, servers, applications, databases, desktops, mobile devices and media, or smartphones, that contain, process, or store EPHI, as well as MHC's corresponding remediation plan and targeted completion dates. On July 28, 2014, the OCC provided a supplement to its initial response. Therein, the OCC provided an overview of HHC's past and present data security activities including the following:

- findings from a vendor conducted information security and HIPAA assessment of MHC;
- a MHC Risk Registry and Remediation and Tracking report;
- a HIPAA Risk Analysis Report of MHC's Quadramed system; and

- the engagement of the services of an outside information technology vendor to perform a risk assessment and HIPAA gap analysis on all HHC acute care facilities, including MHC.

4) OCR has requested to perform a walkthrough of Metropolitan to review its LEP practices later this month.

5) OCR has requested to meet via telephone conference with HHC Sr. AVP/Chief Corporate Compliance Officer Wayne A. McNulty; HHC Sr. VP/General Counsel Salvatore Russo; and HHC Sr. AVP/CIO Sal Guido to discuss the HHC Risk Analysis process. The meeting is scheduled to take place on June 11, 2015.

III. Privacy Incidents and Related Reports

Background

1) The Office of HIPAA Privacy and Security within the OCC is responsible for reviewing, investigating, and responding to potential and confirmed breaches of PHI.

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.[3]

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.[4]

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:[5]

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

[3] 45 CFR § 164.402 ["Breach" defined].
[4] *See* 45 CFR § 164.402[2]; *see also* 78 Fed. Register 5565 at 5643 and 5695 [January 25, 2013]
[5] *See* 45 CFR § 164.402 [2][i-iv].

- 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.

Recent Breaches of PHI

5) Since the Audit Committee convened in April, the following breaches of PHI occurred requiring patient, HHS and media notification:

- Last week HHC began to notify 3,957 HHC patients who received services at Metropolitan about the disclosure of some of their personal and/or PHI when an e-mail file that contained PHI (including some sensitive patient information) was improperly sent by a Metropolitan employee to his personal email account. The employee responsible for sending the e-mail has been terminated from employment with Metropolitan. All affected patients were offered one year of credit free credit monitoring and identity protection services. In addition to the breach notification sent to all affected patients, HHC provided notification to the media and the U.S. Department of Health and Human Services.

- In late April HHC began to notify about 90,000 HHC patients about the possible disclosure of some of their PHI that may have occurred when a former employee at HHC Jacobi Medical Center in the Bronx improperly accessed and transmitted files containing PHI to her personal email account and her email account at her new employer, which is a New York City agency.

  There is no evidence to suggest that the subject files were received or viewed by anyone other than the former employee, and there is no evidence to suggest that the PHI contained in these files was misused or further disclosed in any manner. Based on actions taken by HHC, the PHI has been deleted from all known unauthorized sites and sources to which it was sent and there is no basis to believe that it was forwarded to any other site before it was deleted. HHC has taken decisive steps to protect the individuals who are potentially affected, and through third-party vendor ID Experts, Inc. offered free credit monitoring and identity protection services to all affected patients. In addition to the breach notification sent to all affected patients, HHC provided notification to the media and the U.S. Department of Health and Human Services.

- In late April HHC Center began to notify about 3,300 Bellevue patients about the possible disclosure of some of their protected health information (PHI). The incident in question occurred on January 15, 2015 and was discovered on February 27, 2015 when, in the course of HHC's monitoring of outgoing emails, ETIS identified an email attachment that a Bellevue employee improperly sent to her relative's e-mail account at the relative's place of employment. The e-mail attachment contained a spreadsheet that included the PHI of your PHI, as well as the PHI of other patients. According to the employee, she sent the spreadsheet to her relative for technical assistance in manipulating the spreadsheet data for Bellevue work purposes.

  Based on HHC's investigation into the unauthorized disclosure, the spreadsheet has been deleted from all known unauthorized sources to which it was sent and there is no basis to believe that it was forwarded to any other site before deletion. There is no evidence to suggest that the spreadsheet was received or viewed by anyone other than the single unauthorized recipient, and there is no evidence to suggest that the PHI contained in the spreadsheet was misused or further disclosed in any manner. Through a third-party vendor, free credit monitoring services was offered to all affected patients. In addition to the breach notification sent to all affected patients, HHC provided notification to the media and the U.S. Department of Health and Human Services. The employee responsible for the unauthorized disclosure has been disciplined.

6) All of the incidents described above were detected and discovered through HHC's information governance and security program, which includes data loss prevention ("DLP") software, that among other things, monitors and detects all email communications that contain PHI and other confidential information that are sent outside of HHC's information systems without proper authorization.

IV. Monitoring of Excluded Providers

1) On June 8, 2015, the OCC received a report regarding an excluded provider at the Northern Manhattan/Generations Plus Healthcare Network. This matter is currently under investigation. The OCC will evaluate all claims attributable to this provider and make the necessary self-disclosure to the appropriate regulatory oversight agencies and refund resulting overpayments, if any.

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

Overview

1) As reported to the Audit Committee in April, 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) The revision of these policies is consistent with compliance best practices that recommend the periodic assessment and revision of existing compliance policies and procedures. 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.

Additional Activities:

8) In addition to the above, the OCC has started to revise its Guide to Compliance, which will be discussed before the Audit Committee.

9) The OCC's development of a corporate-wide Code of Conduct is ongoing. As recommended by the Audit Committee in April 2015, the OCC reached out to Pamela S. Brier, President and Chief Executive Officer, Maimonides Medical Center, for her insight regarding the development of the same.

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…."[6]

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

Current training numbers

3) Current training numbers as of June 3, 2015 are as follows:

- Healthcare Professionals Module**:**
  - 20% completion rate (April 6, 2015)
  - 47% completion rate (June 3, 2015)

[6] 18 NYCRR § 521.3[c][3]

- Physicians Module

  - 27% completion rate (April 6, 2015)
  - 39% completion Rate (June 3, 2015)

Efforts made to increase training numbers:

4) 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.

5) 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

Follow up

1) The OCC started its CY2015 Corporate-wide Risk Assessment (the "Risk Assessment") process in May 2015, which will be used, in pertinent part, by the OCC to develop the fiscal year 2016 ("FY2016") HHC Corporate Compliance Work Plan.

2) Risk may be 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."[7] In simpler terms, "[r]isks are events or conditions that may occur and, if they do occur, would have a harmful effect" on HHC.[8]

3) The subject risk assessment process is still on schedule to be completed by mid-July 2015.

Status:

4) The following steps have been taken at this juncture as part of the risk assessment process:

- The OCC convened an Executive Compliance Workgroup on Compliance and Quality in May 2015 to review the risk assessment process;

[7] NIST, U.S. Dep't of Commerce, *Guide for Conducting Risk Assessments* (Special Publication 800-30) Information Security, September 2012, at 6.
[8] HCCA Professional's Manual, Risk Assessment Chapter, ¶ 40,105, at 41,001.

- The OCC expanded its list of predefined risks.

List of Predefined Risks

5) The following is the expanded list of predefined risks:

(i) Office of the Inspector General ("OIG")

- U.S. Department of Health and Human Services Office of the Inspector General *Fiscal Year 2015 Work Plan* (OIG FY15 Work Plan) and *Work Plan for Fiscal Year 2014* (OIG FY2014 Work Plan).
- OIG Special Fraud Alerts From 1994-2014.
- OIG Compliance Program Guidance for Various Types of Providers.
- OIG Special Advisory Bulletins.
- Other OIG Guidance.

(ii) Office of the Medicaid Inspector General ("OMIG")

- New York State Office of the Medicaid Inspector General *Fiscal Year 2015-2016 Work Plan* (OMIG FY15 Work Plan) and *Fiscal Year 2014-2015 Work Plan* (OMIG FY14 Work Plan)
- OMIG Compliance Program Guidance for General Hospitals (May 11, 2012).

(iii) Centers for Medicaid and Medicare Services:

- Conditions of Participation for Hospitals – Standards and Certification (42 CFR part 482).
- Requirements for States and Long Term Care Facilities (42 CFR Part 483).

(iv) New York State Department of Health ("DOH") Regulations:

- Hospitals –Minimum Standards (10 NYCRR part 405).
- Nursing Homes – Minimum Standards (10 NYCRR part 415).

- Treatment Center and Diagnostic Center Operation (10 NYCRR parts 750-759).

- Certified Home Health Agencies – Minimum Standards (10 NYCRR Part 763).

(v). New York State compliance program regulations found at 18 NYCRR § 521.3(a) – Compliance Risk Areas[9]:

- Required risk areas for an effective compliance program.

(vi) Office of the State Comptroller, Division of Local Government and School Accountability, Local Government Management Guide:

- The Practice of Internal Controls, (2010)[10] and Management's Responsibility for Internal Controls.

Risk Scoring Prioritization & Tolerance[11]

5) As previously reported, the OCC will lead the 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.

6) 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 overall risk tolerance and risk appetite.

[9] 18 NYCRR § 521.3[a]
[10] Office of the State Comptroller, Division of Local Government and School Accountability, The Practice of Internal Controls, Oct 2010, at 1 (discussing the examples of internal controls in the listed areas) accessed at: **http://www.osc.state.ny.us/localgov/pubs/lgmg/practiceinternalcontrols.pdf**
[11] *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).

VIII. Vendor/Contractor Management and Information Governance

Background

1) On May 1, 2015, the OCC convened within its offices a workgroup to discuss contractor/vendor management and governance (hereinafter the "Workgroup"). The Workgroup consisted of the following senior leaders, all of whom play important roles in contractor/vendor management and governance throughout the Corporation:

- Paul Albertson, Sr. AVP, Procurement (in person)
- Jeremy Berman, Deputy Counsel, Office of Legal Affairs ("OLA")(via telephone conference)
- Sal Guido, Sr. AVP/Acting Chief Information Officer, EITS (in person)
- Wayne A. McNulty, Sr. AVP/CCO, OCC (in person)
- Barbara Keller, Esq., Deputy Counsel, OLA (in person)
- Joseph Quinones, Sr. AVP, Contract Administration and Controls (via telephone conference)
- Marilyn Robertson, Risk Management (in person)
- Keith Tallbe, Esq., Associate Counsel, OLA (via telephone conference)
- Lisa Weinstein, First Deputy Corporate Compliance Officer, OCC (in person)

Scope of Discussion

2) The Workgroup discussed the privacy and data security requirements concerning vendor management including business associate agreements, vendor due diligence, vendor management, and the auditing of vendors.

Control Objectives for Information and Related Technology

3) As discussed during the Workgroup meeting, the Corporation's EITS has, in pertinent part, decided to follow the information governance principles outlined in the Control Objectives for Information and Related Technology ("COBIT"), which is an information management and control strategy framework published by the IT Governance Institute and the Information Systems Audit and Control Association ("ISACA"). The COBIT framework includes principles, practices, tools and models to help enterprises improve information and technology management processes.

Centers for Medicare and Medicaid Services

4) The Workgroup reviewed the Centers for Medicare and Medicaid Services ("CMS") regulations found under 42 CFR part 482, which sets forth requirements hospitals must follow as conditions for payment and participation in the Medicare and Medicaid programs.

5) 42 CFR § 482.12 (e), set forth the standard for contracted services, specifically the role of the governing body. Under § 482.12(e) and its corresponding interpretive guidelines, the governing body is responsible for services furnished throughout the Corporation's hospitals whether or not they are furnished under contracts. Specifically, the governing body must ensure that a contractor of services provides the same in a manner that: (i) permits the Corporation's hospitals to comply with all applicable conditions of participation and standards for the contracted services; (ii) is safe and effective. Additionally, § 482.12 requires the Corporation to maintain a list of all contracted services, including the scope and nature of the services provided.

6) Equally important, similar to services provided directly by hospitals, all contractors are subject to the Corporation's quality assessment and performance improvement program. This is further detailed under 42 CFR § 482.21, which provides that the Corporation's hospitals must "develop, implement, and maintain an effective, ongoing, hospital-wide, data-driven quality assessment and performance improvement program." Further, § 482.21 mandates that the hospital's governing body must ensure that the performance improvement program covers "those services furnished under contract or arrangement . . . ."

Department of Health Regulations

7) New York State Department of Health Regulations found at 10 NYCRR §§ 400.4 405.2(h), and 415.26 outline similar contractor requirements that hospitals such as HHC's facilities must follow.

8) Specifically, under § 400.4, hospitals operating under a certificate approved and issued by SDOH remain responsible for ensuring that all services provided by vendors are performed in a manner (i) that is safe and effective; and (ii) consistent with applicable law. Similarly, § 405.2(h) states that "[t]he governing body [of a hospital] shall be responsible for services furnished in the hospital whether or not they are furnished by outside entities under contracts. The governing body shall ensure that a contractor of services (including one for shared services and joint ventures) furnishes services that permit the hospital to comply with all applicable codes, rules and regulations."

9) Likewise, § 415.26 requires, among other things, that nursing facilities that use outside resources/vendors to provide residential services adhere to the requirements set forth under § 400.4.

Stark and Anti-kickback Statutes

10) The Workgroup also discussed strategies to ensure that proper controls are in place to ensure that the Corporation adheres to Stark and Anti-Kickback provisions.

- The Stark Law, which is codified at 42 U.S.C. § 1395nn, is also known as the physician self-referral law. In summary, unless an exception exists, the Stark Law prohibits physician referrals for designated health services payable by Medicare to an entity with which he or she or an immediate family member has an ownership, investment, compensation arrangement or other financial relationship.

- The federal Anti-Kickback Statute ("Anti-Kickback Statute") is a criminal statute that prohibits the exchange (or offer to exchange), of anything of value, in an effort to induce (or reward) the referral of federal health care program business. The Anti-Kickback Statute does not afford a private right of action; notwithstanding, via the False Claims Act, individuals may bring qui tam actions alleging violations of the Anti-Kickback Statute.

Business Associate Agreements

11) The Workgroup discussed the Corporation's compliance with the business associate provisions found under the HIPAA. The Office of Procurement reported that it has established a database of business associates as well as other contractor controls. The OCC, Office of Procurement, and OLA have been working to ensure that all business associates have agreements in place, and said agreements are all updated to meet the new business associate requirements promulgated under the HIPAA Omnibus rule, as well as meeting the contractor requirements set forth under Medicare and DOH regulations

Future Discussions of the Workgroup

12) The next time the Workgroup convenes the OCC will raise the notification requirements found under the Deficit Reduction Act of 2005 ("DRA"), which requires HHC to annually inform all vendors that provide healthcare products and services notice of its policies and procedures related to fraud waste and abuse. The OCC will work with the Office of Procurement, as well as the Office of Contract Administration and Controls, to ensure that vendors/contractors subject to the DRA can be readily identified.

IX. HHC ACO, Inc., Compliance Program

Background

Formation of HHC subsidiary to carry out accountable care activities

1) On June 12, 2012 the HHC Board of Directors by way of resolution approved the formation of HHC ACO Inc., a wholly owned subsidiary public benefit corporation in order to establish an Accountable Care Organization to meet the purposes and goals of the Medicare Shared Savings Program. The following individuals have since been designated to key leadership roles at HHC ACO:

- The Chief Executive Officer of the HHC ACO is Ross Wilson, M.D., who also serves as HHC's Senior Vice President, Quality/Corporate Chief Medical Officer
- The Medical Director of the HHC ACO is Nicholas Stine, M.D.; and
- The Director of Operations of the HHC ACO is Megan Cunningham.

The HHC ACO was selected by CMS to participate in the Medicare Shared Savings Program (MSSP) for a three-year term that began on January 1, 2013. Under the MSSP, the ACO is accountable for improving the quality of care for approximately 13,000 Medicare fee-for-service beneficiaries who receive primary care at HHC. In 2013, the only year for which performance data is currently available, the ACO met quality reporting standards and achieved a 7% reduction in Medicare expenditures for its population.

HHC ACO, Inc. participants

2) As of June 2015, the following entities and their employed providers will perform functions or services related to the ACO's activities:

- Coney Island Medical Practice Plan, P.C.
- Downtown Bronx Medical Associates, P.C.
- Harlem Medical Associates, P.C.
- Icahn School of Medicine at Mount Sinai
- Icahn School of Medicine at Mount Sinai, doing business as the Mount Sinai Elmhurst Faculty Practice Group
- Metropolitan Medical Practice Plan, P.C.
- New York University School of Medicine
- NYC Health & Hospitals Corporation
- Physician Affiliate Group of New York, P.C.

Overview of Accountable Care Organizations

3) Pursuant to the Patient Protection and Affordable Care Act ("PPACA"), "the Centers for Medicare & Medicaid Services (CMS) finalized the Medicare Shared Savings Program (MSSP) …. to help doctors, hospitals, and other health care providers better coordinate care for Medicare patients through [ACOs]." [12] "ACOs are groups of providers and suppliers of services (e.g., hospitals, physicians, and others involved in patient care) that agree to work together to coordinate care for the Medicare Fee-For-Service patients they serve."[13] The goal of an ACO is to ensure that patients, especially the chronically ill, get the right care at the right time, while avoiding unnecessary duplication of services and preventing medical errors. This improves patient outcomes and reduces overall cost of care. [14]

4) ACOs create incentives for health care providers to work together to treat an individual patient across care settings—including doctor's offices, hospitals, and long-term care facilities." The Goals of an ACO are as follows:[15]

- "[T]o deliver seamless, high-quality care for Medicare beneficiaries, instead of the fragmented care that often results from a Fee-For-Service payment system in which different providers receive different, disconnected payments."
- To maintain "a patient-centered focus . . . ."
- To develop "processes to: (i) promote evidence-based medicine; (ii) promote patient engagement; (iii) internally and publicly report on quality and cost; and (iv) and coordinate care.

Achievement of Quality Performance Standard

5) ACOs cannot share in savings unless the quality performance standard for that year is realized. The 2014 ACO quality standard consists of 33 quality measures, which can be separated into four key categories:[16]

- Patient/caregiver experience - 7 measures;
- Care coordination/patient safety - 6 measures;
- At-risk population - 5 measures and 2 composites consisting of an

[12] (CMS Accountable Care Organization 2014 Program Analysis Quality Performance Standards Narrative Measure Specifications, June 30, 2014, prepared by RTI International, accessed at: http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/sharedsavingsprogram/Downloads/ACO-NarrativeMeasures-Specs.pdf)
[13] *Id.; see also* 42 CFR §425.10 and 42 CFR § 425.20
[14] *See* http**://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/index.html**, (last accessed on June 8, 2015); *see also* 42 CFR § 425.10
[15] CMS Accountable Care Organization 2014 Program Analysis Quality Performance Standards Narrative Measure Specifications, *supra*, note 15.
[16] *Id.*

additional 7 measures; and

- Preventive Care – 8 measures.

Note that, the quality performance standards are expected to change in 2015.

The HHC ACO

6) The HHC ACO participates in the MSSP. Although the HHC ACO currently focuses on Medicare fee-for-service patients, the HHC ACO will drive broader transformation to a higher-performance health system, serving and ultimately benefiting all HHC patients.

7) All of the entities and providers that are part of the HHC ACO must agree to comply with the MSSP Regulations, which set forth the HHC ACO's requirements with respect to governance, operations, performance and compliance.

Accuracy of HHC ACO Data

8) The entities and providers that are part of the HHC ACO must ensure that any information documented in patient records and business applications is accurate, complete and truthful, including:

- Quality measure documentation; and
- Beneficiary notification tracking.

Participant information must remain updated

9) The entities and providers that are part of the HHC ACO must keep all required job licenses, registrations and/or certifications up to date. Providers must keep their National Provider Identifier (NPI) up to date and must notify CMS of any changes within 30 days.

HHC ACO Restrictions

Patient inducement

10) The entities and providers that are part of the HHC ACO must not give or offer any gifts or other remuneration to patients as inducement for receiving items or services at HHC.

Patient avoidance

11) The entities and providers that are part of the HHC ACO are prohibited from avoiding at-risk patients, including those patients who:

- Have a high risk score and/or more than one chronic condition(s);
- Are considered high cost due to hospital/ED utilization;
- Are dual eligible; or
- Have a disability, or mental health or substance abuse disorder.

Additional Regulatory Requirements

12) In addition to MSSP Regulations, entities and providers that are part of the HHC ACO must comply with all applicable laws, including Federal criminal law and the following:

- **False Claims Act.** This generally prohibits the knowing submission of false or misleading claims to the federal government (31 U.S.C. § 3729[a][2]).
- **Anti-Kickback Statute.** This generally prohibits the knowing and willful exchange of remuneration for the referral of patients for items or services covered by federal health care program (42 U.S.C. §1320a-7b[b]).
- **Civil Monetary Penalties Law.** This authorizes the imposition of penalties upon one who knowingly presents or causes to present an improper claim for a medical service (42 U.S.C. § 1320a–7a)
- **Stark Law (Physician Self-Referral Law).** This prohibits referrals by physicians to any entity with which the physician has a financial relationship that does not fit within any permitted exception (42 U.S.C. §1395nn).

Development of an ACO Compliance Plan

13) All ACOs, including HHC ACO, are required to establish and periodically update (to reflect changes in applicable laws) a compliance plan that encompasses several required elements. The development of a compliance plan serves the following key purposes:[17]

- Identifies and helps to prevent unlawful and unethical conduct;

[17] *See* 76 FR 67,802, 67,952 [2011]

- Provides a centralized source for distributing information on healthcare statutes and other program directives related to fraud, waste and abuse; and
- Fosters an environment that encourages employees and others to anonymously report potential problems.

14) The structure of an ACO's compliance plan may be determined by, among other things, the following factors:[18]

- The size of an ACO; and
- The business structure of an ACO.

Required Elements of an Effective ACO Compliance Program

15) To constitute an effective ACO compliance plan, the following five (5) elements are required:

- ***ELEMENT # 1*** - The appointment of a "designated compliance official or individual who is not legal counsel to the ACO and reports directly to the ACO governing body."[19];
  - **Note**: Attorneys can serve as compliance officers of an ACO, however, legal counsel for the ACO and the compliance officer of the ACO must be different individuals.[20] According to the enforcement agency commentary, this is necessary "in order to ensure independent and objective legal reviews and financial analyses of the organization's compliance efforts and activities by the compliance officer."[21] ACO's, *however,* can utilize the existing organization's compliance officer *provided that* the compliance officer *is not legal counsel* to the ACO or existing organization and *reports directly* to the *governing body* of the ACO.[22]
  - Wayne A. McNulty, HHC's Sr. AVP/CCO has being appointed CCO of HHC ACO.

[18] 76 FR 67,802, 67,952 [2011]
[19] 42 CFR § 425.300 [a][1];
[20] (*See* 76 FR 67,802, 67,952 [2011]
[21] *Id.*
[22] *See* 42 CFR § 425.300 [b][1]); *see also* (76 FR 67,802, 67,952-3 [2011]).

- ***ELEMENT # 2*** - The development and implementation of "mechanisms for identifying and addressing compliance problems related to the ACO's operations and performance."[23]

  - **Note**: "ACOs should consider implementing a system for identifying and addressing possible violations when designing their compliance plan."[24] Potential ACO risks include failure to comply with, among other things, the following:

    - ✓ Physician self-referral prohibition;
    - ✓ Civil monetary penalties (CMP) law;
    - ✓ Federal anti-kickback statute;
    - ✓ Medicare laws and regulations relevant to ACO operations; and
    - ✓ Record retention requirements under 42 CFR § 425.314[b].

  Other potential risks include the following:

    - ✓ Failure to record accurate specific financial and quality measurement data;
    - ✓ Improper coding;
    - ✓ Presence of beneficiary and provider complaints;
    - ✓ The engagement or practice of avoiding at risk beneficiaries; and
    - ✓ Failure to adhere to ACO governance requirements

- ***ELEMENT # 3*** - "A method for employees or contractors of the ACO, ACO participants, ACO providers/suppliers, and other individuals or entities performing functions or services related to ACO activities to anonymously report suspected problems related to the ACO to the compliance officer."[25]

  - **Note**: The ACO compliance program shall be constituted in a manner that "allows for the prompt and thorough investigation of possible misconduct

[23] 42 CFR § 425.300 [a][2]
[24] 76 FR 67,802, 67,953 [2011]
[25] 42 CFR § 425.300 [a][3]

by ACO participants, ACO providers/suppliers, other individuals or entities performing function or services related to ACO activities, corporate officers, managers, employees, and independent contractors, as well as early detection and reporting of violations . . . ."[26] Anonymous reporting mechanisms should be available to report suspected problems related to the ACO.[27]

- ***ELEMENT # 4*** - The provision of "[c]ompliance training for the ACO, the ACO participants, and the ACO providers/suppliers."[28]

  - **Note**: Compliance training is necessary to ensure that ACO participants, ACO providers/suppliers, and contractors are aware of potential compliance risks and how to report compliance concerns.[29] ACO compliance training should cover the legal obligations of every ACO participant, ACO providers/suppliers, and contractor "with respect to the ACO's operations and performance, as well as the requirements of the compliance program and the manner in which [the] ACO is implementing such requirements."[30]

- ***ELEMENT # 5:*** A requirement for the ACO to report "probable violations of law to an appropriate law enforcement agency."[31];

  - **Note**: The following guidance may be used to determine what violations must be reported:

    - ✓ Utilize the Medicare self-referral disclosure protocol for potential violations of the physician self-referral statute.[32]
    - ✓ Utilize the Office of the Inspector General guidance with regard to those activities that may rise to the level of a violation that may require reporting.[33]

[26] *See* 76 FR 67,802, 67,953 [2011]
[27] *See id* at 67,952
[28] 42 CFR § 425.300 [a][4].
[29] 76 FR 67,802, 67,952 [2011].
[30] *See* 76 FR 67,802, 67,953 [2011].
[31] 42 CFR § 425.300 [a][5]
[32] *See* 76 FR 67,802, 67,953 [2011]
[33] *See id.*

Updating the ACO Compliance Plan

15) ACO Compliance Plans must: (1) satisfy applicable law; and (2) be periodically updated "to reflect changes in the law and regulations."[34]

Reporting Compliance Issues

16) The entities and providers that are part of the HHC ACO are encouraged to report compliance issues related to the HHC ACO, including any suspected violation of law, in one of the following ways:

- By anonymously reporting through HHC's confidential Compliance Helpline at **1-866-HELP-HHC (1-866-435-7442)**;
- By e-mailing COMPLIANCE@nychhc.org;
- By following the link to Report Fraud or Abuse on the HHC Office of Corporate Compliance intranet site at http://compliance.nychhc.org; and/or
- By sending a letter through postal mail (or if you are located at HHC or one of its facilities, by interoffice mail) addressed to:

New York City Health and Hospitals Corporation/HHC ACO, Inc.
Office of Corporate Compliance
160 Water Street, Suite 1129
New York, NY 10016

Present Compliance Activities

17) The OCC will include the HHC ACO's operations as part of its CY2015 Risk Assessment process.

18) The OCC has enrolled ACO participants who are members of HHC's medical staff into its Healthcare Professional and Physician Compliance Training Modules. Both modules consist of, among other things, fraud, waste and abuse and general compliance training on ACO compliance consistent with that outlined in the forgoing paragraphs.

19) The OCC is presently developing audit and monitoring plans with regard to the HHC ACO.

[34] 42 CFR § 425.300 [b][2]

20) The OCC will work with the HHC Inspector General and other law enforcement officials as necessary and when appropriate with regard to meeting its reporting requirement if a circumstance arises where a probable violation of law regarding ACO operations exists.

X. Delivery System Reform Incentive Payments ("DSRIP") Compliance Program

Background of the Delivery System Reform Incentive Payments ("DSRIP")

1) In April 2014 the State of New York (the "State") finalized an agreement with the federal government to allow the State to reinvest $8 billion of the $17.1 billion in savings generated through Medicaid Redesign Team ("MRT") reforms. Of this, $6.42 billion was allocated for Delivery System Reform Incentive Payments ("DSRIP"), which is the main vehicle that the State will utilize to implement the savings generated through the MRT reforms. "DSRIP's purpose is to fundamentally restructure the health care delivery system by reinvesting in the Medicaid program, with the primary goal of reducing avoidable hospital use by 25% over 5 years."[35]

2) On December 18, 2014, the HHC Board of Directors (the "Board") approved via formal resolution the following Corporation actions as it relates to DSRIP:

- the submission of an application to the SDOH to participate in DSRIP;
- the execution of agreements with designated participants; and
- the repurposing of the wholly owned HHC subsidiary the HHC Assistance Corporation to function in the capacity of a centralized service organization ("CSO")(d/b/a One City Health Services) for the purpose of providing technical assistance to a single HHC-led Performing Provider System ("PPS"). As part of the resolution, the Board directed that the activities of the CSO under the DSRIP program be subject to HHC's compliance, procurement, and internal audit programs. HHC will serve as the PPS Lead, or fiduciary, of the PPS.

3) To satisfy Department of Social Services compliance program regulations, HHC, as a PPS Lead, is required to "dedicate resources toward implementing a compliance program that will assist in preventing and identifying Medicaid payment discrepancies related to DSRIP payments."[36] In simple terms, HHC is required to "[f]ollow the money."[37] To meet these requirements, "PPS Leads must dedicate resources and develop systems to take all reasonable

[35] New York State Department of Health, Frequently Asked Questions (FAQs), New York MRT Waiver Amendment Delivery System Reform Incentive Payment (DSRIP) Plan.
[36] New York State Department of Health Office of the Medicaid Inspector General Delvery System Reform Incentive Payment ("DSRIP") Program, DSRIP Compliance Guidance 2015-01, Special Considerations for Performing provider System ("PPS") Leads' Compliance Program. [DSRIP CG 2015-01, April 6, 2015].
[37] *Id.*

steps to ensure the Medicaid funds are distributed as part of the DSRIP program are not connected with fraud, waste and abuse."[38]

4) The Office of the Medicaid Inspector General advises that PPS Leads should focus risk identification strategies on "the current phase of the DSRIP program and payments made to it."[39]

5) With regard to the eight elements HHC must comply with to maintain an effective compliance program as required to participate in the Medicaid program, the following are special considerations, by element, that HHC must consider as a PPS Lead:

- ***ELEMENT # 1*** - The establishment of policies and procedures that outlined compliance expectations pertaining to DSRIP, including a mechanism for the reporting of compliance issues to HHC's Chief Corporate Compliance Officer ("CCO"), who is the PPS Lead Compliance Officer.[40] This may be accomplished with direct reports to the PPS Lead Compliance Officer or through "compliance liaisons within the [PPS] Network."[41]

- ***ELEMENT # 2*** – The compliance officer must report directly to the PPS Lead Chief Executive Officer (or other senior administrator) and report to the governing body of the lead PPS at least quarterly.

- ***ELEMENT # 3*** - The provision of training and education directly to the workforce members of the Lead PPS and indirectly to performing providers within the PPS Network. HHC can meet its obligations here by supplying training materials to the PPS providers provided or by implementing a control process that allows HHC to validate that said training took place. Training and education should cover DSRIP compliance expectations, the performing provider's role in DSRIP projects, and the procedure for reporting compliance violations as related to DSRIP funds.

- ***ELEMENT # 4*** – The establishment of a confidential reporting methodology to the PPS Lead compliance officer.

- ***ELEMENT # 5*** – The PPS Lead's disciplinary policies must facilitate the good faith reporting of compliance issues and it must cover the performing providers within the PPS Network.

[38] Id. a
[39] *Id.*at p.2.
[40] *See id*. at p. 2, Special Considerations by Element
[41] *Id.*

- ***ELEMENT # 6*** – The PPS Lead is required to perform a risk assessment on the distribution and use of DSRIP funds. Additionally, the PPS Lead should audit/monitor how PPS partners are using DSRIP funds. OMIG provides that "[t]his plan may coincide with DOH requirements for measuring performance and reporting on the flow of funds related to DSRIP projects.

- ***ELEMENT # 7*** – PPS Leads are required to respond to compliance issues, such as: (i) the misuse of DSRIP funds; (ii) and the false representations to obtain DSRIP funds. The PPS Lead must establish an auditing program that can reach and assess how network partners are utilizing DSRIP funds.

- ***ELEMENT # 8*** – The development of whistleblower protection policies must be undertaken. The PPS Lead will require assistance from the PPS partners to enforce this requirement.

DSRIP and Privacy-Related Matters

6) The New York State Department of Health ("DOH"), Office of Health Insurance Programs, requires that all PPS Leads receiving Medicaid data containing Protected Health Information ("PHI") originating from DOH ("DOH Medicaid Data") assess the need for two factor authentication when accessing DOH Medicaid Data whether it be for employee use within the PPS Lead's IT systems or when providing downstream entities (PPS Performing Providers and PPS Lead's contractors) access to DOH Medicaid Data through the PPS Lead's IT systems. This assessment requirement also applies to the Performing Providers and contractors if they desire to utilize DOH Medicaid Data, shared by the PPS Lead, on their IT systems.

Establishment of a DSRIP Compliance Committee

7) The OCC will establish a compliance committee to focus on DSRIP compliance issues, which will be co-chaired by Christina Jenkins, M.D., President and Chief Executive Officer of One City Health Services CSO, and Wayne A. McNulty, Sr. AVP/CCO.

XI. Gotham Health FQHC, Inc., and Compliance Oversight

Background

1) HHC applied to the Health Resources and Services Administration ("HRSA") for the designation of its six (6) Diagnostic and Treatment Centers ("D&TCs") and all of their respective satellite clinics — twenty (20) satellite clinics and thirteen (13) school-based health centers — as a Federally Qualified Community Health Center Look-Alike ("Health Center") pursuant to HRSA's regulations concerning the Public Entity/Co-Applicant governance model. A corresponding co-applicant agreement was executed between HHC ("public entity") and the Gotham Health FQHC, Inc., Board ("co-applicant").

- On February 2, 2015, HRSA designated the Health Center as a Federally Qualified Health Center Look-Alike for the time period of February 1, 2015 to January 31, 2018.

2) On April 7, 2015, Wayne A. McNulty, Sr. AVP/CCO, reported via telephone conference to members of the Gotham Board of Directors ("Gotham Board"): The following Gotham Board members were present via telephone conference:

- Dr. Dolores McCray, Chairperson, Gotham FQHC, Inc.
- Shena Elrington, Board Member, Gotham FQHC, Inc.
- Herman Smith, Board Member, Gotham FQHC, Inc.

3) During the telephone conference, Mr. McNulty informed the Gotham Board about the following FQHC compliance activities:

HHC's Compliance with the HIPAA Security Rule Risk Assessment Requirements.

- The CCO reported that the "Security Standards for the Protection of Electronic Protected Health Information" (the "Security Rule") requires that HHC implement a risk assessment program the purpose of which is to prevent, detect, contain and correct security violations affecting EPHI.

- The CCO stated that HHC is required to conduct periodic technical and nontechnical evaluations of HHC systems and applications that access, store and transmit EPHI to assess the extent to which HHC's security policies and procedures meet the requirements of the Security Rule. The CCO reported to the Gotham Health Board that he recommended to the HHC Audit Committee that HHC hire a third party expert to assist in the Security Rule risk assessment and immediately begin a risk assessment of the top 25 high-risk systems and applications. The CCO informed the Gotham Board that he would keep them appraised as the risk assessment proceeded.

Compliance and Privacy Reporting Index for the First Quarter of Calendar Year 2015 ("CY2014").

- The CCO reported to the Gotham Board that there were no compliance reports or privacy reports that originated from and/or occurred at any of the D & TCs during the first quarter of 2015.

Monitoring of Excluded Providers.

- The CCO reported that the OCC has not received or uncovered any reports of excluded providers at the D&TCs since the last time the CCO issued a report to the Gotham Board on February 13, 2015. The OCC did uncover one HHC vendor that was excluded on the GSA list and the Office of Procurement is addressing the same. Apparently, the vendor is not an active vendor and therefore there are no apparent overpayment issues to address.

Report on Ongoing Compliance Matters.

- The CCO stated that the Gotham Board will at future meetings be provided with an overview of: (i) the status of the revision of Operating Procedure 50-1 (Corporate Compliance Program); (ii) the HHC Principles of Professional Conduct; (iii) the HHC Corporate Compliance Plan; (iv) the status of OCC's review of 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 (v) the OCC's compliance and privacy training activities and corresponding compliance rates at the D & TCs.

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

- The CCO gave the Gotham Health Board a report on the compliance risk assessment process and discussed the following key points:

  - Risk Assessment Process - In June, 2015 the OCC will begin conducting the calendar year 2015 ("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") HHC Corporate Compliance Work Plan (the "Work Plan"). The CCO stated 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.

  - Identifying Risk - the Gotham Board was informed that HHC will incorporate the following three distinct approaches to identify its risk:

(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.

- Risk Scoring and Prioritization - the CCO reported to the Gotham Health Board that the OCC will work with stakeholders 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.

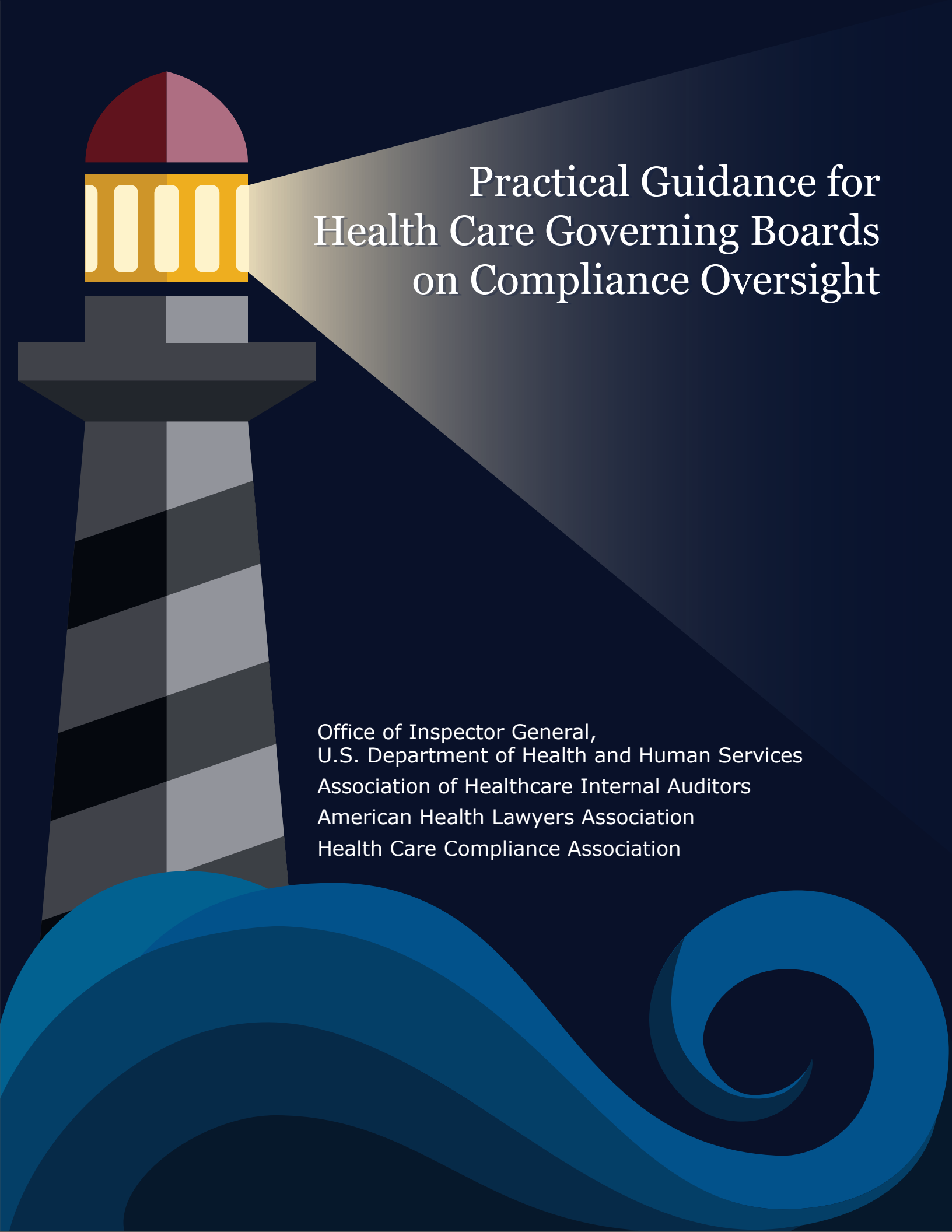
XII. Compliance Oversight Guidance for Healthcare Governing Bodies

1) A discussion regarding the recently issued Practical Guidance for Health Care Governing Boards on Compliance Oversight (*see* Attachment "1")(hereinafter the "Guidance") will take place. The Guidance was issued jointly by the HHS Office of Inspector General ("OIG"), the Association of Internal Auditors ("IAA"), the American Health Lawyers Association ("AHLA"), and the Health Care Compliance Association ("HCCA").

ATTACHMENT "1"

Joint Guidance from the HHS Office of Inspector General, Association of Internal Auditors, the American Health Lawyers Association, and the Health Care Compliance Association

"Practical Guidance for Governing Boards on Compliance Oversight."



Practical Guidance for Health Care Governing Boards on Compliance Oversight

Office of Inspector General,
U.S. Department of Health and Human Services
Association of Healthcare Internal Auditors
American Health Lawyers Association
Health Care Compliance Association

About the Organizations

This educational resource was developed in collaboration between the Association of Healthcare Internal Auditors (AHIA), the American Health Lawyers Association (AHLA), the Health Care Compliance Association (HCCA), and the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS).

AHIA is an international organization dedicated to the advancement of the health care internal auditing profession. The AHLA is the Nation's largest nonpartisan, educational organization devoted to legal issues in the health care field. HCCA is a member-based, nonprofit organization serving compliance professionals throughout the health care field. OIG's mission is to protect the integrity of more than 100 HHS programs, including Medicare and Medicaid, as well as the health and welfare of program beneficiaries.

The following individuals, representing these organizations, served on the drafting task force for this document:

Katherine Matos, Senior Counsel, OIG, HHS

Felicia E. Heimer, Senior Counsel, OIG, HHS

Catherine A. Martin, Principal, Ober | Kaler (AHLA)

Robert R. Michalski, Chief Compliance Officer, Baylor Scott & White Health (AHIA)

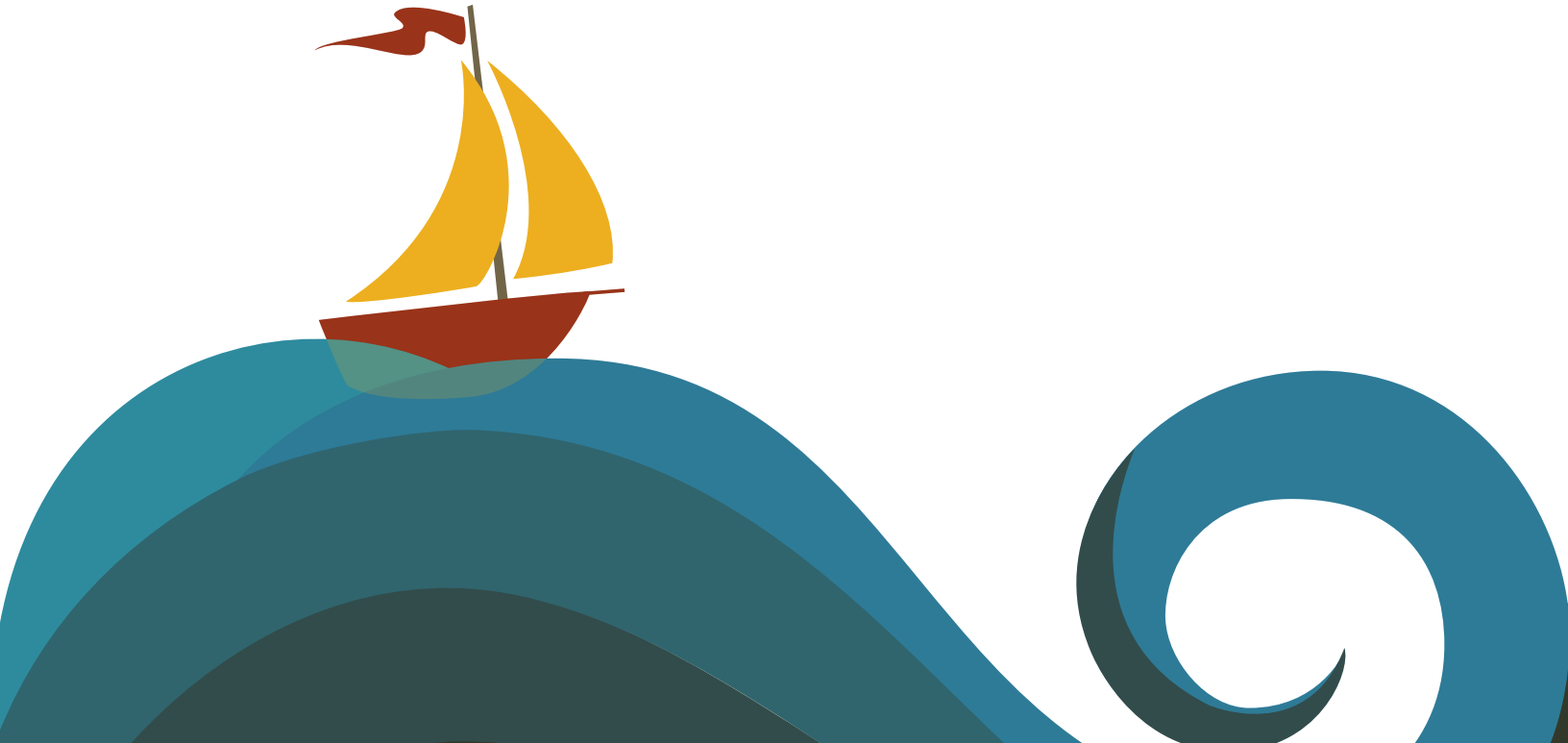
Daniel Roach, General Counsel and Chief Compliance Officer, Optum360 (HCCA)

Sanford V. Teplitzky, Principal, Ober | Kaler (AHLA)

Published on April 20, 2015.

This document is intended to assist governing boards of health care organizations (Boards) to responsibly carry out their compliance plan oversight obligations under applicable laws. This document is intended as guidance and should not be interpreted as setting any particular standards of conduct. The authors recognize that each health care entity can, and should, take the necessary steps to ensure compliance with applicable Federal, State, and local law. At the same time, the authors also recognize that there is no uniform approach to compliance. No part of this document should be taken as the opinion of, or as legal or professional advice from, any of the authors or their respective agencies or organizations.

Table of Contents



Introduction

Previous guidance[1] has consistently emphasized the need for Boards to be fully engaged in their oversight responsibility. A critical element of effective oversight is the process of asking the right questions of management to determine the adequacy and effectiveness of the organization's compliance program, as well as the performance of those who develop and execute that program, and to make compliance a responsibility for all levels of management. Given heightened industry and professional interest in governance and transparency issues, this document seeks to provide practical tips for Boards as they work to effectuate their oversight role of their organizations' compliance with State and Federal laws that regulate the health care industry. Specifically, this document addresses issues relating to a Board's oversight and review of compliance program functions, including the: (1) roles of, and relationships between, the organization's audit, compliance, and legal departments; (2) mechanism and process for issue-reporting within an organization; (3) approach to identifying regulatory risk; and (4) methods of encouraging enterprise-wide accountability for achievement of compliance goals and objectives.

A critical element of effective oversight is the process of asking the right questions....

1 OIG and AHLA, *Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors* (2003); OIG and AHLA, *An Integrated Approach to Corporate Compliance: A Resource for Health Care Organization Boards of Directors* (2004); and OIG and AHLA, *Corporate Responsibility and Health Care Quality: A Resource for Health Care Boards of Directors* (2007).

Expectations for Board Oversight of Compliance Program Functions

A Board must act in good faith in the exercise of its oversight responsibility for its organization, including making inquiries to ensure: (1) a corporate information and reporting system exists and (2) the reporting system is adequate to assure the Board that appropriate information relating to compliance with applicable laws will come to its attention timely and as a matter of course.[2] The existence of a corporate reporting system is a key compliance program element, which not only keeps the Board informed of the activities of the organization, but also enables an organization to evaluate and respond to issues of potentially illegal or otherwise inappropriate activity.

Boards are encouraged to use widely recognized public compliance resources as benchmarks for their organizations. The Federal Sentencing Guidelines (Guidelines),[3] OIG's voluntary compliance program guidance documents,[4] and OIG Corporate Integrity Agreements (CIAs) can be used as baseline assessment tools for Boards and management in determining what specific functions may be necessary to meet the requirements of an effective compliance program. The Guidelines "offer incentives to organizations to reduce and ultimately eliminate criminal conduct by providing a structural foundation from which an organization may self-police its own conduct through an effective compliance and ethics program."[5] The compliance program guidance documents were developed by OIG to encourage the development and use of internal controls to monitor adherence to applicable statutes, regulations, and program requirements. CIAs impose specific structural and reporting requirements to

---

2 *In re Caremark Int'l, Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

3 U.S. Sentencing Commission, *Guidelines Manual* (Nov. 2013) (USSG), http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2013/manual-pdf/2013_Guidelines_Manual_Full.pdf.

4 OIG, *Compliance Guidance*, http://oig.hhs.gov/compliance/compliance-guidance/index.asp.

5 USSG Ch. 8, Intro. Comment.

promote compliance with Federal health care program standards at entities that have resolved fraud allegations.

Basic CIA elements mirror those in the Guidelines, but a CIA also includes obligations tailored to the organization and its compliance risks. Existing CIAs may be helpful resources for Boards seeking to evaluate their organizations' compliance programs. OIG has required some settling entities, such as health systems and hospitals, to agree to Board-level requirements, including annual resolutions. These resolutions are signed by each member of the Board, or the designated Board committee, and detail the activities that have been undertaken to review and oversee the organization's compliance with Federal health care program and CIA requirements. OIG has not required this level of Board involvement in every case, but these provisions demonstrate the importance placed on Board oversight in cases OIG believes reflect serious compliance failures.

Although compliance program design is not a "one size fits all" issue, Boards are expected to put forth a meaningful effort....

Although compliance program design is not a "one size fits all" issue, Boards are expected to put forth a meaningful effort to review the adequacy of existing compliance systems and functions. Ensuring that management is aware of the Guidelines, compliance program guidance, and relevant CIAs is a good first step.

One area of inquiry for Board members of health care organizations should be the scope and adequacy of the compliance program in light of the size and complexity of their organizations. The Guidelines allow for variation according to "the size of the organization."[6] In accordance with the Guidelines,

6 USSG § 8B2.1, comment. (n. 2).

OIG recognizes that the design of a compliance program will depend on the size and resources of the organization.[7] Additionally, the complexity of the organization will likely dictate the nature and magnitude of regulatory impact and thereby the nature and skill set of resources needed to manage and monitor compliance.

While smaller or less complex organizations must demonstrate the same degree of commitment to ethical conduct and compliance as larger organizations, the Government recognizes that they may meet the Guidelines requirements with less formality and fewer resources than would be expected of larger and more complex organizations.[8] Smaller organizations may meet their compliance responsibility by "using available personnel, rather than employing separate staff, to carry out the compliance and ethics program." Board members of such organizations may wish to evaluate whether the organization is "modeling its own compliance and ethics programs on existing, well-regarded compliance and ethics programs and best practices of other similar organizations."[9] The Guidelines also foresee that Boards of smaller organizations may need to become more involved in the organizations' compliance and ethics efforts than their larger counterparts.[10]

Boards should develop a formal plan to stay abreast of the ever-changing regulatory landscape and operating environment. The plan may involve periodic updates from informed staff or review of regulatory resources made available to them by staff. With an understanding of the dynamic regulatory environment, Boards will be in a position to ask more pertinent questions of management

---

7 Compliance Program for Individual and Small Group Physician Practices, 65 Fed. Reg. 59434, 59436 (Oct. 5, 2000) ("The extent of implementation [of the seven components of a voluntary compliance program] will depend on the size and resources of the practice. Smaller physician practices may incorporate each of the components in a manner that best suits the practice. By contrast, larger physician practices often have the means to incorporate the components in a more systematic manner."); Compliance Program Guidance for Nursing Facilities, 65 Fed. Reg. 14,289 (Mar. 16, 2000) (recognizing that smaller providers may not be able to outsource their screening process or afford to maintain a telephone hotline).

8 USSG § 8B2.1, comment. (n. 2).

9 *Id.*

10 *Id.*

and make informed strategic decisions regarding the organizations' compliance programs, including matters that relate to funding and resource allocation. For instance, new standards and reporting requirements, as required by law, may, but do not necessarily, result in increased compliance costs for an organization. Board members may also wish to take advantage of outside educational programs that provide them with opportunities to develop a better understanding of industry risks, regulatory requirements, and how effective compliance and ethics programs operate. In addition, Boards may want management to create a formal education calendar that ensures that Board members are periodically educated on the organizations' highest risks.

Finally, a Board can raise its level of substantive expertise with respect to regulatory and compliance matters by adding to the Board, or periodically consulting with, an experienced regulatory, compliance, or legal professional. The presence of a professional with health care compliance expertise on the Board sends a strong message about the organization's commitment to compliance, provides a valuable resource to other Board members, and helps the Board better fulfill its oversight obligations. Board members are generally entitled to rely on the advice of experts in fulfilling their duties.[11] OIG sometimes requires entities under a CIA to retain an expert in compliance or governance issues to assist the Board in fulfilling its responsibilities under the CIA.[12] Experts can assist Boards and management in a variety of ways, including the identification of risk areas, provision of insight into best practices in governance, or consultation on other substantive or investigative matters.

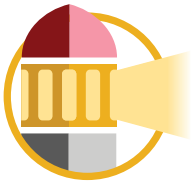
---

11 *See* Del Code Ann. tit. 8, § 141(e) (2010); ABA Revised Model Business Corporation Act, §§ 8.30(e), (f)(2) Standards of Conduct for Directors.

12 *See* Corporate Integrity Agreements between OIG and Halifax Hospital Medical Center and Halifax Staffing, Inc. (2014, compliance and governance); Johnson & Johnson (2013); Dallas County Hospital District d/b/a Parkland Health and Hospital System (2013, compliance and governance); Forest Laboratories, Inc. (2010); Novartis Pharmaceuticals Corporation (2010); Ortho-McNeil-Janssen Pharmaceuticals, Inc. (2010); Synthes, Inc. (2010, compliance expert retained by Audit Committee); The University of Medicine and Dentistry of New Jersey (2009, compliance expert retained by Audit Committee); Quest Diagnostics Incorporated (2009); Amerigroup Corporation (2008); Bayer HealthCare LLC (2008); and Tenet Healthcare Corporation (2006; retained by the Quality, Compliance, and Ethics Committee of the Board).

Roles and Relationships

Organizations should define the interrelationship of the audit, compliance, and legal functions in charters or other organizational documents. The structure, reporting relationships, and interaction of these and other functions (e.g., quality, risk management, and human resources) should be included as departmental roles and responsibilities are defined. One approach is for the charters to draw functional boundaries while also setting an expectation of cooperation and collaboration among those functions. One illustration is the following, recognizing that not all entities may possess sufficient resources to support this structure:



The compliance function promotes the prevention, detection, and resolution of actions that do not conform to legal, policy, or business standards. This responsibility includes the obligation to develop policies and procedures that provide employees guidance, the creation of incentives to promote employee compliance, the development of plans to improve or sustain compliance, the development of metrics to measure execution (particularly by management) of the program and implementation of corrective actions, and the development of reports and dashboards that help management and the Board evaluate the effectiveness of the program.

The legal function advises the organization on the legal and regulatory risks of its business strategies, providing advice and counsel to management and the Board about relevant laws and regulations that govern, relate to, or impact the organization. The function also defends the organization in legal proceedings and initiates legal proceedings against other parties if such action is warranted.

The internal audit function provides an objective evaluation of the existing risk and internal control systems and framework within an organization. Internal audits ensure monitoring functions are working as intended and identify where management monitoring and/or additional

Board oversight may be required. Internal audit helps management (and the compliance function) develop actions to enhance internal controls, reduce risk to the organization, and promote more effective and efficient use of resources. Internal audit can fulfill the auditing requirements of the Guidelines.

The human resources function manages the recruiting, screening, and hiring of employees; coordinates employee benefits; and provides employee training and development opportunities.

The quality improvement function promotes consistent, safe, and high quality practices within health care organizations. This function improves efficiency and health outcomes by measuring and reporting on quality outcomes and recommends necessary changes to clinical processes to management and the Board. Quality improvement is critical to maintaining patient-centered care and helping the organization minimize risk of patient harm.

Boards should be aware of, and evaluate, the adequacy, independence,[13] and performance of different functions within an organization on a periodic basis. OIG believes an organization's Compliance Officer should neither be counsel for the provider, nor be subordinate in function or position to counsel or the legal department, in any manner.[14] While independent, an organization's counsel and compliance officer should collaborate to further the interests of the organization. OIG's position on separate compliance and legal functions reflects the independent roles and professional obligations of each function;[15]

---

13 Evaluation of independence typically includes assessing whether the function has uninhibited access to the relevant Board committees, is free from organizational bias through an appropriate administrative reporting relationship, and receives fair compensation adjustments based on input from any relevant Board committee.

14 *See* OIG and AHLA, *An Integrated Approach to Corporate Compliance: A Resource for Health Care Organization Boards of Directors*, 3 (2004) (citing Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,997 (Feb. 23, 1998)).

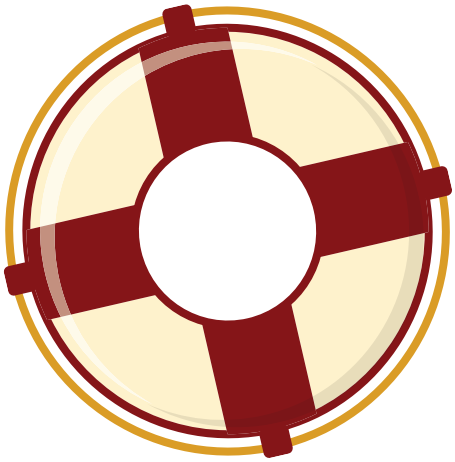
15 *See, generally, id.*

the same is true for internal audit.[16] To operate effectively, the compliance, legal, and internal audit functions should have access to appropriate and relevant corporate information and resources. As part of this effort, organizations will need to balance any existing attorney-client privilege with the goal of providing such access to key individuals who are charged with the responsibility for ensuring compliance, as well as properly reporting and remediating any violations of civil, criminal, or administrative law.

The Board should have a process to ensure appropriate access to information; this process may be set forth in a formal charter document approved by the Audit Committee of the Board or in other appropriate documents. Organizations that do not separate these functions (and some organizations may not have the resources to make this complete separation) should recognize the potential risks of such an arrangement. To partially mitigate these potential risks, organizations should provide individuals serving in multiple roles the capability to execute each function in an independent manner when necessary, including through reporting opportunities with the Board and executive management.

Boards should also evaluate and discuss how management works together to address risk, including the role of each in:

1. identifying compliance risks,
2. investigating compliance risks and avoiding duplication of effort,
3. identifying and implementing appropriate corrective actions and decision-making, and
4. communicating between the various functions throughout the process.



16 Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,997 (Feb. 23, 1998) (auditing and monitoring function should "[b]e independent of physicians and line management"); Compliance Program Guidance for Home Health Agencies, 63 Fed. Reg. 42,410, 42,424 (Aug. 7, 1998) (auditing and monitoring function should "[b]e objective and independent of line management to the extent reasonably possible"); Compliance Program Guidance for Nursing Facilities, 65 Fed. Reg. 14,289, 14,302 (Mar. 16, 2000).

Boards should understand how management approaches conflicts or disagreements with respect to the resolution of compliance issues and how it decides on the appropriate course of action. The audit, compliance, and legal functions should speak a common language, at least to the Board and management, with respect to governance concepts, such as accountability, risk, compliance, auditing, and monitoring. Agreeing on the adoption of certain frameworks and definitions can help to develop such a common language.

Reporting to the Board

The Board should set and enforce expectations for receiving particular types of compliance-related information from various members of management. The Board should receive regular reports regarding the organization's risk mitigation and compliance efforts—separately and independently—from a variety of key players, including those responsible for audit, compliance, human resources, legal, quality, and information technology. By engaging the leadership team and others deeper in the organization, the Board can identify who can provide relevant information about operations and operational risks. It may be helpful and productive for the Board to establish clear expectations for members of the management team and to hold them accountable for performing and informing the Board in accordance with those expectations. The Board may request the development of objective scorecards that measure how well management is executing the compliance program, mitigating risks, and implementing corrective action plans. Expectations could also include reporting information on internal and external investigations, serious issues raised in internal and external audits, hotline call activity, all allegations of material fraud or senior management misconduct, and all management exceptions to the organization's

The Board should receive regular reports regarding the organization's risk mitigation and compliance efforts....

code of conduct and/or expense reimbursement policy. In addition, the Board should expect that management will address significant regulatory changes and enforcement events relevant to the organization's business.

Boards of health care organizations should receive compliance and risk-related information in a format sufficient to satisfy the interests or concerns of their members and to fit their capacity to review that information. Some Boards use tools such as dashboards—containing key financial, operational and compliance indicators to assess risk, performance against budgets, strategic plans, policies and procedures, or other goals and objectives—in order to strike a balance between too much and too little information. For instance, Board quality committees can work with management to create the content of the dashboards with a goal of identifying and responding to risks and improving quality of care. Boards should also consider establishing a risk-based reporting system, in which those responsible for the compliance function provide reports to the Board when certain risk-based criteria are met. The Board should be assured that there are mechanisms in place to ensure timely reporting of suspected violations and to evaluate and implement remedial measures. These tools may also be used to track and identify trends in organizational performance against corrective action plans developed in response to compliance concerns. Regular internal reviews that provide a Board with a snapshot of where the organization is, and where it may be going, in terms of compliance and quality improvement, should produce better compliance results and higher quality services.

As part of its oversight responsibilities, the Board may want to consider conducting regular "executive sessions" (i.e., excluding senior management) with leadership from the compliance, legal, internal audit, and quality functions to encourage more open communication. Scheduling regular executive sessions creates a continuous expectation of open dialogue, rather than calling such a session only when a problem arises, and is helpful to avoid suspicion among management about why a special executive session is being called.

Identifying and Auditing Potential Risk Areas

Some regulatory risk areas are common to all health care providers. Compliance in health care requires monitoring of activities that are highly vulnerable to fraud or other violations. Areas of particular interest include referral relationships and arrangements, billing problems (e.g., upcoding, submitting claims for services not rendered and/or medically unnecessary services), privacy breaches, and quality-related events.

The Board should ensure that management and the Board have strong processes for identifying risk areas. Risk areas may be identified from internal or external information sources. For instance, Boards and management may identify regulatory risks from internal sources, such as employee reports to an internal compliance hotline or internal audits. External sources that may be used to identify regulatory risks might include professional organization publications, OIG-issued guidance, consultants, competitors, or news media. When failures or problems in similar organizations are publicized, Board members should ask their own management teams whether there are controls and processes in place to reduce the risk of, and to identify, similar misconduct or issues within their organizations.

The Board should ensure that management consistently reviews and audits risk areas, as well as develops, implements, and monitors corrective action plans. One of the reasonable steps an organization is expected to take

under the Guidelines is "monitoring and auditing to detect criminal conduct."[17] Audits can pinpoint potential risk factors, identify regulatory or compliance problems, or confirm the effectiveness of compliance controls. Audit results that reflect compliance issues or control deficiencies should be accompanied by corrective action plans.[18]

Recent industry trends should also be considered when designing risk assessment plans. Compliance functions tasked with monitoring new areas of risk should take into account the increasing emphasis on quality, industry consolidation, and changes in insurance coverage and reimbursement. New forms of reimbursement (e.g., value-based purchasing, bundling of services for a single payment, and global payments for maintaining and improving the health of individual patients and even entire populations) lead to new incentives and compliance risks. Payment policies that align payment with quality care have placed increasing pressure to conform to recommended quality guidelines and improve quality outcomes. New payment models have also incentivized consolidation among health care providers and more employment and contractual relationships (e.g., between hospitals and physicians). In light of the fact that statutes applicable to provider-physician relationships are very broad, Boards of entities that have financial relationships with referral sources or recipients should ask how their organizations are reviewing these arrangements for compliance with the physician self-referral (Stark) and anti-kickback laws. There should also be a clear understanding between the Board and management as to how the entity will approach and implement those relationships and what level of risk is acceptable in such arrangements.

Emerging trends in the health care industry to increase transparency can present health care organizations with opportunities and risks. For example, the Government is collecting and publishing data on health outcomes and quality measures (e.g., Centers for Medicare & Medicaid Services (CMS) Quality Compare Measures), Medicare payment data are now publicly available (e.g.,

---

17 *See* USSG § 8B2.1(b)(5).

18 *See* USSG § 8B2.1(c).

CMS physician payment data), and the Sunshine Rule[19] offers public access to data on payments from the pharmaceutical and device industries to physicians. Boards should consider all beneficial use of this newly available information. For example, Boards may choose to compare accessible data against organizational peers and incorporate national benchmarks when assessing organizational risk and compliance. Also, Boards of organizations that employ physicians should be cognizant of the relationships that exist between their employees and other health care entities and whether those relationships could have an impact on such matters as clinical and research decision-making. Because so much more information is becoming public, Boards may be asked significant compliance-oriented questions by various stakeholders, including patients, employees, government officials, donors, the media, and whistleblowers.

Encouraging Accountability and Compliance

Compliance is an enterprise-wide responsibility. While audit, compliance, and legal functions serve as advisors, evaluators, identifiers, and monitors of risk and compliance, it is the responsibility of the entire organization to execute the compliance program.

Compliance is an enterprise-wide responsiblity.

In an effort to support the concept that compliance is "a way of life," a Board may assess employee performance in promoting and adhering to compliance.[20] An organization may assess individual, department, or facility-level performance or consistency in executing the compliance program. These assessments can then be used to either withhold incentives or to provide bonuses

---

19 *See* Sunshine Rule, 42 C.F.R. § 403.904, and CMS *Open Payments*, http://www.cms.gov/Regulations-and-Guidance/Legislation/National-Physician-Payment-Transparency-Program/index.html.

20 Compliance Program Guidance for Nursing Facilities, 65 Fed. Reg. 14,289, 14,298-14,299 (Mar. 16, 2000).

based on compliance and quality outcomes. Some companies have made participation in annual incentive programs contingent on satisfactorily meeting annual compliance goals. Others have instituted employee and executive compensation claw-back/recoupment provisions if compliance metrics are not met. Such approaches mirror Government trends. For example, OIG is increasingly requiring certifications of compliance from managers outside the compliance department. Through a system of defined compliance goals and objectives against which performance may be measured and incentivized, organizations can effectively communicate the message that everyone is ultimately responsible for compliance.

Governing Boards have multiple incentives to build compliance programs that encourage self-identification of compliance failures and to voluntarily disclose such failures to the Government. For instance, providers enrolled in Medicare or Medicaid are required by statute to report and refund any overpayments under what is called the 60 Day Rule.[21] The 60-Day Rule requires all Medicare and Medicaid participating providers and suppliers to report and refund known overpayments within 60 days from the date the overpayment is "identified" or within 60 days of the date when any corresponding cost report is due. Failure to follow the 60-Day Rule can result in False Claims Act or civil monetary penalty liability. The final regulations, when released, should provide additional guidance and clarity as to what it means to "identify" an overpayment.[22] However, as an example, a Board would be well served by asking management about its efforts to develop policies for identifying and returning overpayments. Such an inquiry would inform the Board about how proactive the organization's compliance program may be in correcting and remediating compliance issues.

---

21 42 U.S.C. § 1320a-7k.

22 Medicare Program; Reporting and Returning of Overpayments, 77 Fed. Reg. 9179, 9182 (Feb. 16, 2012) (Under the proposed regulations interpreting this statutory requirement, an overpayment is "identified" when a person "has actual knowledge of the existence of the overpayment or acts in reckless disregard or deliberate ignorance of the overpayment.") disregard or deliberate ignorance of the overpayment."); Medicare Program; Reporting and Returning of Overpayments; Extensions of Timeline for Publication of the Final Rule, 80 Fed. Reg. 8247 (Feb. 17, 2015).

Organizations that discover a violation of law often engage in an internal analysis of the benefits and costs of disclosing—and risks of failing to disclose—such violation to OIG and/or another governmental agency. Organizations that are proactive in self-disclosing issues under OIG's Self-Disclosure Protocol realize certain benefits, such as (1) faster resolution of the case—the average OIG self-disclosure is resolved in less than one year; (2) lower payment—OIG settles most self-disclosure cases for 1.5 times damages rather than for double or treble damages and penalties available under the False Claims Act; and (3) exclusion release as part of settlement with no CIA or other compliance obligations.[23] OIG believes that providers have legal and ethical obligations to disclose known violations of law occurring within their organizations.[24] Boards should ask management how it handles the identification of probable violations of law, including voluntary self-disclosure of such issues to the Government.

As an extension of their oversight of reporting mechanisms and structures, Boards would also be well served by evaluating whether compliance systems and processes encourage effective communication across the organizations and whether employees feel confident that raising compliance concerns, questions, or complaints will result in meaningful inquiry without retaliation or retribution. Further, the Board should request and receive sufficient information to evaluate the appropriateness of management's responses to identified violations of the organization's policies or Federal or State laws.

Conclusion

A health care governing Board should make efforts to increase its knowledge of relevant and emerging regulatory risks, the role and functioning of the organization's compliance program in the face of those risks, and the flow and elevation of reporting of potential issues and problems to

---

23 *See* OIG, *Self-Disclosure Information*, http://oig.hhs.gov/compliance/self-disclosure-info.

24 *See id.*, at 2 ("we believe that using the [Self-Disclosure Protocol] may mitigate potential exposure under section 1128J(d) of the Act, 42 U.S.C. 1320a-7k(d).")

senior management. A Board should also encourage a level of compliance accountability across the organization. A Board may find that not every measure addressed in this document is appropriate for its organization, but every Board is responsible for ensuring that its organization complies with relevant Federal, State, and local laws. The recommendations presented in this document are intended to assist Boards with the performance of those activities that are key to their compliance program oversight responsibilities. Ultimately, compliance efforts are necessary to protect patients and public funds, but the form and manner of such efforts will always be dependent on the organization's individual situation.

Bibliography

Elisabeth Belmont, et al., "Quality in Action: Paradigm for a Hospital Board-Driven Quality Program," 4 Journal of Health & Life Sciences Law. 95, 113 (Feb. 2011).

Larry Gage, *Transformational Governance: Best Practices for Public and Nonprofit Hospitals and Health Systems*, Center for Healthcare Governance (2012).

Tracy E. Miller and Valerie L. Gutmann, "Changing Expectations for Board Oversight of Healthcare Quality: The Emerging Paradigm," 2 Journal of Health & Life Sciences Law (July 2009).

Tracy E. Miller, B*oard Fiduciary Duty to Oversee Quality: New Challenges, Rising Expectations*, 3 NYSBA Health L.J. (Summer/Fall 2012).

Lawrence Prybil, et al., *Governance in Nonprofit Community Health Systems: An Initial Report on CEO Perspectives*, Grant Thornton LLP (Feb. 2008).