

AUDIT COMMITTEE
MEETING AGENDA

June 13, 2017

1:00 P.M.

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

CALL TO ORDER

Ms. Emily A. Youssouf

- Adoption of Minutes April 04, 2017

Ms. Emily A. Youssouf

ACTION ITEMS

INFORMATION ITEMS

- KPMG 2017 Audit Plan
- Audits Update
- Compliance Update

Ms. Maria Tiso

Mr. Chris A. Telano

Mr. Wayne McNulty

EXECUTIVE SESSION

OLD BUSINESS

NEW BUSINESS

ADJOURNMENT

MINUTES

AUDIT COMMITTEE

MEETING DATE: April 4, 2017

TIME: 1:00 PM

COMMITTEE MEMBERS

Emily Youssouf, Chair
Stanley Brezenoff
Josephine Bolus, RN
Mark Page

STAFF ATTENDEES

Salvatore J. Russo, General Counsel, Legal Affairs
Colicia Hercules, Chief of Staff, Chairman's Office
Patricia Lockhart, Secretary to the Corporation, Chairman's Office
PV Anantharam, Senior Vice President/Corporate Chief Financial Officer
Wilson Ross, MD, Senior Vice President/Transformation Officer
Steven Bussey, Chief of Ambulatory Care
Jay Weinman, Corporate Comptroller
James Linhart, Deputy Corporate Comptroller
Wayne McNulty, Corporate Compliance Officer/Senior Assistant Vice President
Machelle Allen, MD Chief Medical Officer, Medical & Professional Affairs
Kim Mendez, Corporate Nursing Executive
Christopher A. Telano, Chief Internal Auditor/Senior Assistant Vice President
Robert Ashkenase, Assistant Vice President, Finance
Nelson Conde, Senior Director, Affiliations
Chelsea-Lyn, Rudder, Deputy Press Secretary
Alice Berkowitz, Assistant Director, Finance
Devon Wilson, Senior Director, Office of Internal Audits
Chalice Piña, Director, Office of Internal Audits
Delores, Rahman, Director, Office of Internal Audits
Carlotta Duran, Assistant Director, Office of Internal Audits
Frank Zanghi, Audit Manager, Office of Internal Audits
Armel Sejour, Senior Auditor, Office of Internal Audits
Melissa Bernaudo, Audit Manager, Office of Internal Audits
Gillian Smith, Auditor Manager, Office of Internal Audits
Jean Saint-Preux, Staff Auditor, Office of Internal Audits
Erica Nairne-Hamilton, Staff Auditor, Office of Internal Audits
Robert Hogan, Staff Auditor, Office of Internal Audits
Miriam Yeger, Staff Auditor, Office of Internal Audits
Conny Lizarazo, Executive Secretary, Office of Internal Audits
Alex Scoufaras, Associate Executive Director, NYC H + H/Jacobi
L.R. Tulloch, Senior Director, Office of Facilities Development
Edie Coleman, Controller, NYC H + H/Metropolitan
Ron Townes, Associate Director, NYC H + H/Kings County
Kim Walcott, Coordinating Manager, NYC H + H/Coney Island
Mohammad Adnan, Supervising Systems Analyst, Central Office

OTHER ATTENDEES

PAGNY: Luis Marcos, CEO; Mike Chambers, COO; Anthony Mirdita, Chief Financial Officer; Reginal Odom, Chief of Human Resources; Diana, Voigt, General Counsel; Sandra Maldonado, On-Site Administrator

**APRIL 4, 2017
AUDIT COMMITTEE MEETING
MINUTES**

A meeting of the Audit Committee was held on Tuesday, April 4, 2017. The meeting was called to order at 1:02 P.M. Ms. Youssouf stated that because we do not have a quorum, we are going to by-pass the minutes and I'm going to turn it over to Chris Telano to give us an update.

Mr. Telano saluted everyone and said that we will start with the on-going external audit, and just to give the Committee an update as to the audit of Epic that the New York City Comptroller's Office is conducting, it's still ongoing. They finally began their fieldwork on March 21st, and they were provided with the test environment to Epic, and everything seems to be going well.

Ms. Youssouf stated that we are all very glad to hear that.

Moving on to the completed internal audits. The first one was a review of the Physician Affiliate Group of New York known as PAGNY at New York City Health + Hospitals/Jacobi.

Ms. Youssouf asked for the appropriate representatives to come to the table and introduce themselves. They did as follows: Dr. Luis Marcos, CEO; Sandra Maldonado, Chief Affiliation Officer at Jacobi and North Central Bronx Hospital and Reggie Odom, Chief Human Resources Officer for PAGNY.

Mr. Telano stated that I will go over the issues that we noted during our review.

1. The first one had to do with the lack of oversight of the subcontractors that are hired in various departments.
2. We found that a physician in Rheumatology, his credentialing had expired on March 31, 2016, and continued to see patients. We can confirm that he saw patients during July 2016 until this was brought to their attention.
3. Due to a lack of communication, the PAGNY Human Resources Department was unaware that a Residency Director was hired in Neurology.
4. In addition, a Residency Director at OB/GYN received his paperwork, was sent to HR, but they did not process it timely. We also found subcontracted physicians did not have their annual medical clearance and other clearances were done late.
5. We found a clause within the contract not being adhered to.
6. Two departments were not maintaining schedules for their employees indicating their regular hours.
7. Two departments that did maintain schedules, and even though they did keep them updated, they did not reconcile them to their timesheets, resulting in two physicians being paid for days in which they did not work, and there was some other discrepancies between the timesheets and the schedules. Regarding other issues of the timesheets, the director for Pediatrics was signing and approving her own timesheets. Two timesheets were not signed by authorized individuals, and the time worked for one employee did not match the time paid, and employees that are required to work 160 hours a month in the Medicine Department, there was no confirmation by review of the timesheets that this was being adhered to.
8. We also noted that there was some issues related to system access of terminated employees, and in some instances the PAGNY HR Department sent notification to the Enterprise Service Desk, which is the Jacobi

Enterprise Information Technology Service Department, but they did not take any action in removing individuals from QuadraMed. We found 15 individuals that still had QuadraMed access, and we found 6 individuals, that had access to the Active Directory. One of these individuals had access to the Active Directory almost a year after they were terminated, and their account was accessed, and since they had access to QuadraMed, we had passed this on to the Office of Corporate Compliance to determine if a breach had occurred, so I'll let Mr. McNulty comment on that.

Mr. McNulty saluted everyone and introduced himself as Wayne McNulty, Chief Compliance Officer. That matter is still under internal investigation by the Office of Corporate Compliance. I will brief the Audit Committee in June on our findings.

Mr. Telano continued and stated that the last issue had to do with the timely deactivation of ID badges. We found in some cases that PAGNY HR was late in notifying Hospital Police and in other instances Hospital Police did not act timely in deactivating the terminated employees' ID badges.

Ms. Youssouf stated that there are a number of things. I'm sure you have the list in front of you, so perhaps we can go through it and tell us how you addressed or are planning to address the items Chris Telano and his team enumerated.

Dr. Marcos said that let me first thank you for inviting us to the table. I thank the auditors, although I really don't mean it. It's always an opportunity to improve our operations, and my personal feeling is that we have significantly improved over the years, but obviously we still need to work hard to ensure that everything works the way it's supposed to work. With the help of Reggie Odom and Sandra Maldonado, we will address each of the items. Let's start with the issue of subcontracted employees.

Mr. Odom reported that I think there were three departments that had issues regarding subcontracted employees, and I think in one particular instance the department, it was a situation where an individual was late in giving their credentialing information back. It was a known individual who was working at the facility for a period of time, and he was late. That resulted in the finding that Chris Telano articulated. In two other instances, they found that there was new residency directors brought in under the subcontract, so what typically happens under the subcontract is if there's a change there needs to be communication between the department and the HR Department so we can do all the necessary paperwork to get them on-boarded correctly and to make sure all the credentialing is in order. In that instance, unfortunately in two instances, two different departments never communicated they were making a change under the contract, so we were not aware in the PAGNY office that the changes had occurred, so these individuals came on, and because they are paid under a subcontract, it wasn't picked up until a later date.

Ms. Youssouf asked where does that lie in -- is that PAGNY's responsibility, or is that Jacobi's responsibility?

Mr. Odom responded that ultimately we take responsibility because of the departments. We need to engage the departments more and make sure that they know their responsibility and that they are pushing this information forward to us. Going forward, what we are planning to do is make sure in our regular meetings with the board, with the chairs of the departments, make sure they are clear about where they stand with their subcontracts. Also we are looking at a monthly report to make sure if there are any changes to make sure everything has been addressed appropriately from a paperwork standpoint.

On the other timesheets issue, the monitoring of timesheets, in response to that situation the departments are very focused on getting the

schedule filled and making sure they have the appropriate people needed to cover the schedule. What we found through this audit process, as Dr. Marcos indicated, these things are helpful to us to teach us where we need to focus our attention as well, is that a lot of departments don't close the loop. If during the process I was scheduled to work 3 to 11 on Thursday, and I called out sick, and Sandra picks up for me, what we found is some departments had not been good about going back and making that adjustment in the schedule, so what happens then is there appears to be when you look at my timesheet and Sandra's timesheet, there's an apparent discrepancy in terms of what I work compared to what's on the schedule. We need to work with our departments more closely to make sure that they are pushing forward changes at the end of the scheduling process, not just setting the schedule and leaving it to sit, but to go back and making the adjustments because adjustments always occur.

Mrs. Bolus asked how is the pay done?

Mr. Odom answered that the pay would be done based on the timesheet, and I think that's where there's some discrepancies.

Mrs. Bolus commented that that's where your problem is, there are people who are not there have been paid. Then asked how do you figure that out?

Mr. Odom stated that the pay is driven from the timesheet. What we need to do is make sure that the schedules in the departments actually match up with the timesheet. We believe, we have been paying people appropriately based on the timesheet, and we believe the timesheets are correct. Where we think the error is, people did not close the loop on the schedule to make any adjustments if someone was on or off. The schedules will appear that Reggie might have been off work when in actuality Reggie was not.

Ms. Youssouf commented that then Reggie would not have not have been paid.

Mr. Odom stated no, Reggie would be paid based on the timesheet. If Reggie completed a timesheet indicating Reggie worked, that is what's been paid on, so there needs to be a matching up of the schedule with the timesheet to make sure that they are accurate. Unfortunately, during the period of the audit, particularly in our Payroll Department at Jacobi, one payroll person was missing and that created some of the backups.

Mr. Russo stated that the question our Board members are getting at was somebody paid that should not have been paid and other people not paid that should have been paid.

Mr. Odom responded that we believe we have been paying people appropriately based on their timesheet. Mr. Russo asked why would they have filled the timesheet if they did not show up?

Mr. Odom answered no, we are saying that the timesheet is accurately reflecting when they work.

Mr. Russo added that theoretically if an individual was on a schedule but did not show up, they would not fill a timesheet as if they were there. To which Mr. Odom answered correct.

Mr. Russo said that if a salary or the money is based on timesheet, then there would be nobody paid for services they did not provide, and people who did show up would be paid, so the answer is if that's correct that no one got paid that should not have been paid and someone who should have been paid was paid. To which Mr. Odom responded that that is correct.

Mr. Telano stated that in one instance an employee did not come to work, it was on a holiday, and they filled out the timesheet as if they worked, and in another instance I believe they were sick and they filled out their timesheet as if

they worked, so those were two instances in which they were overpaid, and there was other instance in which they were underpaid.

Ms. Youssouf asked if it was a physician? To which Mr. Telano answered yes.

Ms. Yossouf asked who filled in a timesheet saying he worked, but was not there.

Ms. Maldonado responded that we went back and corrected the timesheets, so if they signed in and it was a holiday, we corrected.

Ms. Yossouf asked if you found out through this audit? Ms. Maldonado replied yes.

Ms. Youssouf stated that we are trying to get to the root of the issue- what are you doing to correct it so that it does not happen again?

Dr. Marcos answered that we are going to do at least two things. The first one that Mr. Odom has instituted, we are going to have our own audits on a quarterly basis.

Mr. Odom added yes, on a quarterly basis, we are going to do an audit of the schedules and compare those to the timesheets to make sure that these kind of issues that were brought up don't occur and that we are reinforcing in meetings with the department chairs the importance of making sure that the schedules are accurately updated or reflected on a regular basis.

Ms. Youssouf asked who is going to do the audit? Mr. Odom answered that our Chief Affiliate Officer, Ms. Maldonado. Dr. Marcos then said that the second thing is more of a long term, but in the next few months we are going to go to electronic timesheets. Mr. Odom said that we are very much looking forward to moving to the electronic timesheet process. Hopefully before the next fiscal year starts, we'll move to an electronic timekeeping process, which eliminates this and some of the other issues that were brought up when Chris Telano talked about a person signing their own timesheet. That would be impossible in an electronic system because it will have to go to the secondary approver and can't be signed off by the individual.

Mr. Odom continued on with the next issue, untimely deactivation of terminated employees. With respect to the process, when people are terminated, there is supposed to be immediate notification that the person's been terminated. That's been indicated to several members of the hospital staff, and that communication is then supposed to support their termination from all the appropriate systems. There were several instances that Chris Telano indicated that they discovered where we were untimely in submitting that notice, and in one instance the notice never occurred, so some of that was an individual error, and that's an error that we strongly addressed with the individual who was doing the process. We have taken appropriate action to address it, but going forward I guess we are going to continue to work on making sure that that process happens immediately and that we are also doing a backup check once a month just doing a quick scan and search to make sure that everybody has been terminated and not just when we send a note, we're going to follow up, as I think Chris and his group recommended, follow up to make sure that termination occurs. Typically we get a response back that will tell us it happened, and in the past we weren't really monitoring those

responses to make sure we checked off everybody who had gotten terminated, so now we are going to be more actively engaged and monitor that process to make sure the terminations have occurred.

Ms. Youssef asked if the termination notice is part of Jacobi's responsibility? To which Dr. Marcos responded that the actual turning off in QuadraMed or any system, that is the responsibility of the hospital, but we have to tell the hospital that this person is not working anymore.

Ms. Youssef asked if that was the thing that was missed. Dr. Marcos answered yes.

Mr. Telano stated that in most of these instances, we found that PAGNY HR did do the right thing and they did send the notification, but it looked like on our end, H + H's end, it was not acted upon.

Ms. Maldonado reported on the last issue, the ID badges. That is pretty similar to the one we just talked about where we did send either it was a late notification or we did send the notification to Hospital Police, but they did not do what they were supposed to do.

Ms. Youssef stated that it looks like some of these discussions should be with Jacobi. Mr. Telano said yes, and those discussions were held with the appropriate individuals there.

Ms. Youssef thanked them.

Mr. Telano continued on with the briefing and stated that we did a review of the Delivery System Incentive Payment Program (DSRIP) at OneCityHealth. He asked for the representatives to approach the table and introduce themselves. They did as follows: Christina Jenkins, MD, CEO; Ines Sieben, Chief Operating Officer.

Mr. Telano said that although the primary objective of this audit was to evaluate the operations of the DSRIP program for efficiency and effectiveness, a secondary objective was to recommend the scope of an audit if one was to be done by an external consulting firm. So overall our report consisted of two recommendations:

- One being that the partner portal, which is more or less the crux of the organization, which is the database that shows all the information related to the partners that are paid and also tracks the money coming in, we recommended going forward when there is more activity that an outside auditor should review this portal and especially the general application controls related to this portal to ensure that it is able to handle the higher activity they are expecting in the future.
- We also recommended that the information within the portal related to the funds being received and disbursed are reconciled with H + H Finance Department records. As the money is kept in the a bank account of H + H along with some other Medicaid funds, so this way we make sure that it is looked at regularly.

Dr. Jenkins stated like Dr. Marcos, we are very grateful to have been audited and I'm sincere. I and my management agree with the two recommendations that were made. You should know that we will proceed to have an external audit of the subsidiary with the recommendation of the management team, Internal Audit and also the Board, the CSO, Central Services Organization Board, we just met again a few hours ago, and we will define the scope and issue the RFP within the next few months. With respect to the partner portal, absolutely we expect higher volumes and would appreciate further auditing of those processes and controls. Particularly for our relationship with H + H Finance and the

Comptroller, we will continue to deepen those regular relationships, which have been ongoing since the establishment of the subsidiary.

Mr. Telano said that that is it. In the remaining pages of my briefing I list the audits we are currently working on and the status of our follow up.

Ms. Youssouf said thank you very much.

Mr. Bresenoff asked that on the Jacobi thing, is there any kind of a communication that not necessarily naming the institution, but just sharing what you found with other around the areas of vulnerability.

Mr. Telano said that within the entire organization, no.

Mr. Brezenoff said that these are things that are not confidential right? To which Mr. Telano answered that in the past I have addressed that, and the individual facilities, this is going back probably two, three years, frowned upon and I'll quote them "airing their dirty laundry" so while that is not correct, I agree it was a call above and beyond me.

Mr. Brezenoff stated that since the issue here is in some respect attentiveness to procedure and the like, it seems like lessons will be shared.

Ms. Youssouf added that I don't think you have to say who the hospital is.

Mr. Telano stated that it was agreed at the time this should be taken care of and I'm not just saying it's because he's not here, by Tony Martin. He had mentioned that he would coordinate the communication between all the facilities.

Ms. Youssouf suggested that this is something that we had previously talked about. Maybe you can take a look at the easiest way to do that because it could just be "From your Friends in Internal Audit, lessons learned".

Ms. Youssouf announced that before we move on to Compliance, we need to adopt the minutes of the February 10th meeting and asked for a motion. Motion was seconded.

Ms. Youssouf then turned the meeting over to Wayne McNulty for the Compliance Report.

Mr. McNulty saluted everyone and stated that I am going to provide the Committee with an update on the system's Human Subject Research Protection program activities. At the February 2017 Audit Committee of the Board of Directors, the OCC had noted that pursuant to an audit conducted by the OCC that it had found several deficiencies with respect to the Human Subject Research Protection program. Since then the Office of Corporate Compliance has been working very closely with the Office of Medical and Professional Affairs and Office of Research Administration to further develop the System's Human Subject Research Protection program.

On March 22, 2017, the OCC working with the System's Chief Medical Officer, Dr. Allen, met with all of the facility chief medical officers here in this boardroom and provided a PowerPoint presentation on the Human Subject Research Protection program. I provided an overview of the development of Operating Procedure 180-9, which is the System's

policies/procedures that govern Human Subject Research. We went through the responsibilities of the facility medical directors as it relates to research, went through the responsibilities of the principal investigators as it relates to research. We talked about the audit that was performed by the Office of Corporate Compliance and provided a brief overview of the audit performed by the Office of Internal Audits and told the Committee our findings of the medical directors, and then we also discussed the further development of the Human Subject Research Quality Improvement program.

Over the next couple of months, with the assistance of Dr. Allen, I'll be meeting with the Research Council to go over our findings, and I'll also be working with the Office of Medical Professional Affairs, Legal Affairs and Research Administration to further develop the Human Subject Research Quality Assurance Compliance program. Any questions on that?

The next topic of the report, privacy incidents and related reports for the fourth quarter of 2016, from October 1st to December 31, 2016. We received HIPAA complaints in that particular time frame. We confirmed that 11 were violations of the HIPAA or our internal policies and procedures. Out of those 11 violations, five of those violations were determined to be breaches of protected health information. Some of the incidents were:

- At Elmhurst where a business associate had sent a billing statement to the wrong patient. We had to send a breach notification in that particular incident.
- At Metropolitan Hospital Center we had an employee that disclosed the inpatient status of a patient who happened also to be an employee at Metropolitan to several of his coworkers. They were retrained with respect to that particular instance.
- At Lincoln Medical Center an appointment slip was given to the wrong patient.
- At Kings County Hospital a fax was sent to the wrong patient. We had since retrained the social worker with respect to appropriately send a fax to check the number before it is sent and always include a cover page with respect to the fax.
- At Bellevue Hospital Center we had an employee who improperly accessed a medical record of his or her child, which is a violation of HIPAA policies and procedures, and we are evaluating that employee with respect to disciplinary action.

Mr. McNulty asked if there were any question with respect to the privacy incident.

Ms. Youssouf responded, just one. The HIPAA violation with the child, if the child is very young, a minor, how did they access the records?

Mr. McNulty answered that if you are an employee and you generally have access to medical records as part of your duties and functions, and then you have a family member that is ill, and want to look at that record, you have to go to Medical Records like any other family member and try to get access through Medical Records. You can't because you have access for your duties and functions utilize that access for your personal use.

Moving on to the next item - monitoring of excluded providers, we have no excluded providers or vendors to report in this time period.

Next our review of the Office of Foreign Asset Control Screening, we have no vendors or workforce members or business partners to report that were on the Office of Foreign Asset Control Screening list, which is the screening list that reviews anyone that's involved with terrorist activities.

Moving on to next item, compliance-related reports for the fourth quarter Calendar Year 2016, October 1st to December 31, 2016, we had a total of 88 compliance reports that we received in that period. We received no priority A reports, and priority A reports would be the reports that a patient safety or health or an immediate employee is threatened. We had 34 priority B reports and 54 priority C reports. We received 20 emails and 38 or 43 percent were received by our confidential compliance hotline.

I am briefly going to discuss the next item – the compliance requirements for an effective compliance program under the Medicare and Medicaid program requirements for long-term care facilities. Under New York Law, Health + Hospitals is required to establish an effective compliance program, and that compliance program requirements generally cover eight specific elements. Long before New York promulgated its statute for effective compliance programs, the Office of the Inspector General for the Department of Health and Human Services, issued compliance program guidance for nursing homes in 2000 and in 2008. These compliance program requirements include written policies and procedures, on designation of a chief compliance officer, development of training and education, establishment of a compliance hotline, the implementation of internal audits, the performance of exclusion screening on workforce members and vendors, and systems in place to respond to compliance issues with respect to investigations and mitigation.

Finally, the Legislature, Congress passed the Affordable Care Act, and with respect to the Affordable Care Act, inside the Affordable Care Act there was a requirement for the establishment of a compliance program for nursing homes, and the Department of Health and Human Services finally promulgated a rule with respect to compliance programs for nursing homes, and the rule is very similar to the previous compliance program requirements that were issued by OIG, the elements are the same, the designation of compliance officer. This is new, to make sure that the compliance office has adequate resources. Employee sanction screening is still consistent, training education, audit and monitoring to make sure that you have a disciplinary policy and to make sure that you respond and mitigate any compliance deficiencies that you learn of.

Ms. Youssouf asked, when it says assignment of a specific individual within a high-level personnel of the operating organization, does that mean they want separate compliance officers or is this talking about your office.

Mr. McNulty responded that this is my office. You have to designate one individual to run the compliance organization as it relates to nursing home and long-term care facilities, and that individual has to report to the governing body of the organization, which I report to Mr. Brezenoff in his role, so that satisfies that particular requirement.

Ms. Youssouf asked if there any things in here that we are not currently doing?

Mr. McNulty answered no. We are doing everything that's in the eight elements, so we have long satisfied these eight elements years and years ago. Satisfying the New York requirements, they overlap, so we automatically have to satisfy these requirements here. The one area that's new here to the elements that are not in the New York elements is the adequate resources, but we already had that in our operating procedure that only the president can approve or

disapprove the budget of the Office of Corporate Compliance, so we've had that in place for seven or eight years already, long before this was promulgated.

There are additional requirements because we operate five nursing facilities, so they have certain requirements organizations that operate less than five and certain requirements organizations that operate more than five nursing facilities or five or more nursing facilities, so one would be that not only do you have to provide training education, but it must be on an annual basis, so we have to make sure that all training education is done on an annual basis. Second requirement and we already had this in place here, but other of my colleagues at other institutions don't have this in place, the compliance officer must report to the governing body and cannot report to the general counsel, the subordinate of the general counsel, the chief financial officer or the chief operating officer, so only to the governing body. The third requirement is that each nursing facility has to have a compliance liaison. That compliance liaison is not considered a compliance officer. It's just a person at the facility that will provide information to the compliance officer, and we have a compliance officer that is designated to cover all of our facilities as we speak. I will work with the facility CEOs to identify who the compliance liaisons will be, but one again compliance liaison per regulations is not someone who is expected to be a compliance officer or qualified to be a compliance officer. It is just merely someone that's going to provide assistance to the compliance officer as required.

Ms. Youssouf asked if they have any special duties? To which Mr. McNulty replied that other than that, to provide assistance that is all that's in the regulations. It's really to make sure that the compliance officer from the Office of Corporate Compliance is provided with information, so if they know of something, that they funnel that information to the compliance person.

Mrs. Bolus asked if that person can be anybody who works at that facility?

Mr. McNulty answered that it can be a risk manager. It would not be someone you are going to give this specific duty to. They would already be in risk management, quality management, somewhere in that area, and then they would be the designated liaison, and that will be it. I would like to come to the Committee in June and discuss the other requirements in this rule with respect to quality assurance, background screening, so I will be meeting with the facility CEOs and the senior vice president in charge of long-term care for the System within the next two months, and we will come back to the table. There are three different phases of to be implemented over the next years, so I'll just give an update on where we are at to make sure that we are in compliance when those different dates come in effect.

Continuing on to the last topic, DISRIP compliance attestation by OneCityHealth partners, the Office of Corporate Compliance disseminated to all of the PPS partners, all the partners from OneCityHealth that participate in the Delivery Incentive Payment Program an attestation to ascertain their compliance readiness to make sure that they have a compliance integrity program in place. So the attestation will ask several questions of our partners, one, have they done our compliance training which we provided to the partners back in December; two, have they followed our principles of professional conduct, which they are required to adhere to; three, have they certified with the Office of the Medicaid Inspector General that they are in an effective compliance program and have they certified with the Office of the Medicaid Inspector General that they're in compliance with the Deficit Reduction Act of 2005.

We sent out the attestations in February, out of 228 attestation sent out, we received 91 back. All 91 have certified of completing their DISRIP training education requirements. Out of the 91 returned, all have adopted the principles of

professional conduct. That includes the principles of professional conduct's core objectives and substantially similar compliance goals. Out of the 91 attestations, 71 had certified that they have provided a certification to OMIG that they have an effective compliance perform, and 55 have certified to OMIG that they are compliant with the Deficit Reduction Act of 2005. OneCityHealth sent out a reminder, I believe yesterday to the partners that they have to provide us with the attestations for the ones that have not, and we have reached out to every partner. We have contacted every single partner by telephone who has not yet provided us with an attestation, so we expect that to be forthcoming, and we'll update the Committee in June.

We were very pleased to hear that there was so many partners that are certified with the Office of Medicaid Inspector General. Per the Office of Medicaid Inspector General guidance, if once the partner is certified with them, those partners are considered of a lower risk as far as how they are going to utilize the DSRIP funds. That's why we have to do that.

Ms. Youssouf asked since the deadline was March 20th, is there any penalty, risk that these guys do not do their attestation?

Mr. McNulty answered no, not at this point, it wouldn't put us at any risk. If we get to around June, and then the Office of the Medicaid Inspector General, they ask how many do you have in compliance, they may ask that question, but as long as we have a continuous effort to ascertain compliance in this area, generally we should be okay. I expect that by June, we will be in a range of 90 percent, 95 percent would have been completed, and then we will make sure we wrap it up from there, but that's our target, by June to at least have 90/95 percent, and I will work with Dr. Jenkins to make sure we achieve that goal. That concludes my report.

Ms. Youssouf said thank you.

There being no further business, the meeting was adjourned at 1:43 P.M.



NYC Health + Hospitals

Audit plan

June 30, 2017

June 13, 2017

This presentation to the Audit Committee is intended solely for the information and use of the Audit Committee and management and is not intended to be and should not be used by anyone other than these specified parties. This presentation is not intended for general use, circulation or publication and should not be published, circulated, reproduced or used for any purpose without our prior written permission in each specific instance.

Agenda

1.0 Audit plan

- Scope
- Client service team
- Materiality
- Timeline

2.0 Involvement of Others - Planned use of subcontractors

3.0 Objectives of an audit

4.0 Responsibilities

5.0 Risk assessment

6.0 Planned meetings with management

7.0 Independence

8.0 KPMG's Audit Committee Institute

9.0 Appendix

- New accounting pronouncements



1.0 Audit plan

Audit plan - Scope

Scope of work

- Auditor's report on the financial statements of:
 - New York City Health and Hospitals Corporation (NYC Health + Hospitals, NYC H+H, or the Corporation);
 - MetroPlus Health Plan (calendar year end);
 - HHC Insurance Company, Inc. (calendar year end);
 - HHC ACO, Inc.

Note: An audit of the financial statements includes consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control over financial reporting.

- Management letter to the 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 and;
 - Skilled nursing facilities
- Annual debt compliance letter.
- Completeness and accuracy census data attestation (pension related deliverable) done on a periodic basis (every 3 years as requested by The City Pension Plan Auditors).

Audit Plan - Scope (continued)

Applicable financial reporting framework	<ul style="list-style-type: none">— U.S. GAAP— Governmental Accounting Standards Board (GASB)
Applicable auditing standards	<ul style="list-style-type: none">— U.S. Generally Accepted Auditing Standards (GAAS)— Government Auditing Standards (GAS)

Audit plan - Client service team

Engagement team

- Maria Tiso: Lead Engagement Partner
- Mike Breen: Engagement Partner
- Sean Egan: MetroPlus/HHC Insurance Company Partner
- Joseph Bukzin: Lead Senior Manager
- Camille Fremont: Senior Manager
- Dorothy Wright: HHC Insurance Company Manager
- Marlee Fisher: Lead Senior Associate

Subject matter professionals

- Felicia Tucker: Principal, Tax
- Devin Duncan: Manager, Tax
- Robert Mishler: Senior Manager, Actuary
- Alisa Widmer: Manager, Actuary
- Anthony La Rocca: Director, IT

Other resources

- BCA Watson Rice Staff: Minority Business Enterprise
- Healthcare Management Solutions Staff: Women's Business Enterprise

Other Partners

- Jim Martell: Healthcare Resource Partner
- Steve Reader: Concurring Review Partner
- Richard Catalano: MetroPlus and HHC Insurance Concurring Review Partner

Audit plan - Materiality

- Professional standards require that we exercise professional judgment when we consider materiality and its relationship with audit risk when determining the nature, timing, and extent of our audit procedures, and when evaluating the effect of misstatements.
- Information is material if its misstatement or omission could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.
- Judgments about materiality are made in light of surrounding circumstances and are affected by the size or nature of a misstatement, or a combination of both.
- Judgments about matters that are material to users of the financial statements are based on a consideration of the common financial information needs of users as a group. The possible effect of misstatements on specific individual users, whose needs may vary widely, is not considered.

Audit plan - Timeline

NYC H+H

May to June 2017

- Hold planning meeting with management.
- Determine audit approach.
- Perform risk assessment procedures and identify risks.
- Hold audit team planning meeting.
- Review March 31, 2017 internal financial statements.
- Test IT general controls.
- Present audit plan to Audit Committee.

June to July 2017

- Identify financial statement and assertion level fraud risks.
- Evaluate design and implementation of controls.
- Perform site visits including testing controls over various processes such as patient accounts receivable, procurement, payroll/HR, and fixed assets.
- Review of non-routine transactions through June.
- Hold meetings with senior management.

Audit plan - Timeline (continued)

August to October 2017

- Final phase of year-end audit begins August 7, 2017 through October 6, 2017.
- Perform substantive audit procedures.
- Review of financial statements, including disclosures.
- Hold meetings with senior management.
- Form audit conclusions.
- Discuss key issues and deficiencies identified with management (provide draft management letter).
- Attend Audit Committee meeting and discuss required communications.
- Obtain written communications from management
- Finalize and issue audit opinion on financial statements.

December 2017

- Present final management letter to Audit Committee.

Audit plan - Timeline (continued)

Other

December 2017 to January 2018

- Perform interim testwork for MetroPlus Health Plan audit.

February to March 2018

- Final phase of MetroPlus Health Plan audit and issuance of financial statements.

April to August 2018

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

Timing to be determined

- HHC ACO, Inc. audit (2016 and 2017)



2.0 Involvement of Others - Planned use of subcontractors

Involvement of Others - Planned use of subcontractors

KPMG plans to utilize the Minority Business Enterprise (MBE) and Women’s Business Enterprise (WBE) in accordance with our contract dated May 27, 2014 in the following areas:

	MBE	WBE
Third party payor liabilities		X
Site visits	X	
Grants receivable/grant revenue	X	
Capital assets	X	
Investment/assets limited as to use	X	
Human Resources/payroll	X	
NOTE: Internal audit will not be utilized during this year’s audit based upon our discussions with senior management.		



3.0 Objectives of an audit

Objectives of an audit

- The objective of an audit of 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 are free of material misstatement, whether caused by error or fraud. Although not absolute assurance, reasonable assurance is a high level of assurance.
- Our audit includes:
 - Performing tests of the accounting records and such other procedures as we consider necessary in the circumstances to provide a reasonable basis for our opinion.
 - Assessing the accounting principles used and significant estimates made by management, and evaluating the overall financial statement presentation.



4.0 Responsibilities

Responsibilities

Management is responsible for:

- Preparation and fair presentation of the financial statements, including disclosures, in conformity with generally accepted accounting principles (GAAP).
- For the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.
- Ensuring that the Corporation operations are conducted in accordance with the provisions of laws and regulations, including compliance with the provisions of laws and regulations that determine the reported amounts and disclosures in the Corporation's financial statements, and for informing the auditor of any known material violations of such laws and regulations.
- To provide access to all information of which management is aware that is relevant to the preparation and fair presentation of the financial statements, such as records, documentation, and other matters, additional information that we may request from management for the purpose of the audit, and unrestricted access to persons within the entity from whom we determine it necessary to obtain audit evidence.
- Adjusting the financial statements to correct material misstatements and affirming 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.

Responsibilities (continued)

Management is responsible for (continued):

- Providing the auditor with a letter confirming certain representations made during the audit that includes, but is 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.

The Audit Committee is responsible for:

- Oversight of the financial reporting process and oversight of Internal Control Over Financial Reporting (ICOFR).
- Oversight of the establishment and maintenance by management of programs and 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.

Responsibilities (continued)

KPMG is responsible for:

- Planning and performing our audit, with an attitude of professional skepticism, to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by fraud or error. Accordingly, there is some risk that a material misstatement of the financial statements will remain undetected. Although not absolute assurance, reasonable assurance is a high level of assurance. Our audit is not designed to detect error or fraud that is immaterial to the financial statements.
- Conducting the audit in accordance with professional standards and complying with the rules and regulations of 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.
- 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.
- An audit of the financial statements includes consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control over financial reporting.
- Communicating to the Audit Committee all required information, including significant matters, that are in our professional judgment, relevant to the responsibilities of those charged with governance in overseeing the financial reporting process.

Responsibilities (continued)

KPMG is responsible for (continued):

- Communicating to management and the Audit Committee in writing all significant deficiencies and material weaknesses in internal control identified during the audit and reporting to management in writing all deficiencies noted during our audit that, in our professional judgment, are of sufficient importance to merit management's attention. The objective of our audit of the financial statements is not to report on the Corporation's internal control and we are not obligated to search for material weaknesses or significant deficiencies as part of our audit of the financial statements.
- Communicating to the Audit Committee circumstances that affect the form and content of the auditors' report, if any.



5.0 Risk assessment

Risk assessment

Based on our preliminary risk assessment procedures, the following are significant risks/financial statement level risks that may result in a material misstatement (due to fraud or error) in the financial statements and our planned audit approach in response to such significant risks:

- Valuation of hospital patient accounts receivable.
 - Utilization of data and analytics tool
- Valuation of certain third party receivables/liabilities (UPL,DSH,IPRO).
 - Utilization of third party subject matter professional
- Valuation of MetroPlus claims payable.
 - Utilization of KPMG actuary
- *Risk of management override of controls:* For every company, it is presumed that management is in a unique position to perpetrate fraud because of management's ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively.

Risk assessment (continued)

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 hospital patient accounts receivable.
- Third-party and pools receivables/liabilities.
- Postemployment benefit obligation other than pension (OPEB).
- Pension obligation.
- Valuation of MetroPlus claims payable.
- Liquidity (see following slides).

— Other audit areas:

- Patient accounts receivable and Net Patient Service Revenue (completeness, existence and accuracy).
- Related party transactions with the City of New York.
- General Information Technology environment.

— Significant non-routine transactions/unusual/other items:

- Delivery System Reform Incentive Payment (DSRIP) program.
- Elimination of non-union staff positions
- Implementation of new GASB Standards (see appendix)

Risk assessment (continued)

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 areas are some liquidity considerations:

- Income (loss) from operations trends.
- Working capital trends.
- Cash flow trends.
- Net deficit position.
- Debt covenant compliance.

The engagement team will review the March 31, 2017 internal financial statements to preliminarily assess the liquidity of the Corporation.

Risk assessment (continued)

Liquidity (continued)

KPMG may request the information about management's plans:

- Fiscal 2018 budgets and cash flow projections.
- Written representation from management regarding plans.
- Board and Finance Committee meeting minutes.
- Transforming Health + Hospitals report (One New York: Healthcare for Our Neighbors).
- Other reports and findings, if applicable.

Additionally, KPMG may review:

- Fiscal 2017 budget to actual results (reliability of budgeting process).
- Working capital, operating income (loss) and cash flow from operations (liquidity).
- Continued support from the City of New York.



6.0 Planned meetings with management

Planned meetings with management

We plan to perform the following meetings with management for the annual audit ending June 30, 2017:

- Emily Youssouf: Audit Committee Chair
- Stanley Brezenoff: Interim President and CEO
- Plachikkat V. Anantharam: Senior Vice Present, Finance and CFO
- Wayne McNulty: Senior Assistant Vice President, Chief Corporate Compliance Officer
- Salvatore Russo: Senior Vice President, General Counsel
- Christopher Telano: Chief Internal Auditor and Assistant Vice President
- Jay Weinman: Corporate Comptroller
- John Cuda, Chief Financial Officer, MetroPlus

*Others may be identified during the course of the audit.



7.0 Independence

KPMG independence quality controls

KPMG maintains a comprehensive system of quality controls designed to maintain our independence and to comply with regulatory and professional requirements.

- Pre-approval of all worldwide engagements by the audit engagement team through Sentinel, a KPMG independence and conflict checking system (includes services for/relationships with the audit client, its affiliates, and its affiliated persons).
- 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, including a required annual independence training deployed globally.
- Annual independence confirmation required for all partners and employees and for all new joiners to the firm.
- Compliance testing programs.
- Formal disciplinary policy and process.
- Annual reporting to the audit committee regarding independence.



8.0 KPMG's Audit Committee Institute

KPMG resources

KPMG's Audit Committee Institute (ACI): Established in 1999

- KPMG's commitment to communicating with Audit Committee members and other participants in the financial reporting process.
- **www.kpmg.com/aci**
- Publications of the ACI
 - Audit Committee insights: **www.kpmginsights.com**
 - Audit Committee quarterly: **<http://www.kpmg.com/aci/quarterly.htm>**
 - Audit Committee institute roundtables: **www.kpmg.com/aci/roundtables.htm**
 - ACI Website: **www.kpmg.com/aci**
 - ACI mailbox: **auditcommittee@kpmg.com**
 - ACI hotline: **1-877-KPMG-ACI**
- Healthcare publications
- KPMG insiders, Healthcare: **www.kpmginsiders.com**
- Healthcare business briefing



9.0 Appendix

New accounting pronouncements

GASB 75, Accounting and Financial Reporting for Postemployment Benefits Other Than Pensions

— Effective for reporting periods beginning after June 15, 2017.

GASB 80, Blending Requirements for Certain Component Units: An amendment of GASB Statement No. 14

— Effective for reporting periods beginning after June 15, 2016.

GASB 82, Pension Issues: An amendment of GASB Statements No. 67, No. 68, and No. 73

— Effective for reporting periods beginning after June 15, 2016.

GASB 85, Omnibus 2017

— Effective for reporting periods beginning after June 15, 2017.



kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
NDPPS 678363

The KPMG name and logo are registered trademarks or trademarks of KPMG International.



**AUDIT COMMITTEE OF THE
NYC HEALTH + HOSPITALS
BOARD OF DIRECTORS**

Corporate Compliance Report

June 13, 2017

Table of Contents

I. Privacy Incidents and Related ReportsPages 3-4

II. Monitoring of Excluded ProvidersPages 4-6

**III. Summary of Compliance-Related Reports for the First Quarter of Calendar Year 2017
.....Pages 6-10**

**IV. Status Update - DSRIP Compliance Attestation of OneCity Health Partners
.....Pages 10-12**

**V. Status Update - NYC Health + Hospitals' Compliance with the HIPAA Security Rule
Risk Analysis Requirements Pages 12-17**

I. Privacy Incidents and Related Reports

Reportable Privacy Incidents for the First Quarter of Calendar Year 2017 (January 1, 2017 to March 31, 2017 (hereinafter “First Quarter”))

1) During period of January 1, 2017 through March 31, 2017, twenty-nine (29) complaints were entered in the ID Experts RADAR Incident Tracking System. Of the 29 complaints entered in the tracking system, nine (9) were found after investigation to be violations of NYC Health + Hospitals HIPAA Privacy Operating Procedures; six (6) were determined to be unsubstantiated; twelve (12) were found not to be a violation of NYC Health + Hospitals HIPAA Privacy Operating Procedures; and three (3) are still under investigation.

Of the 9 incidents confirmed as violations, one (1) was determined to be a breach.

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.¹

3) Pursuant to 45 CFR § 164.402 [2], the unauthorized access, acquisition, use or disclosure of PHI is presumed to be a breach unless NYC Health + Hospitals 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.²

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:³

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

¹ 45 CFR § 164.402 [“Breach” defined].

² See 45 CFR § 164.402[2]; see also 78 Fed. Register 5565 at 5643 and 5695 [January 25, 2013]

³ See 45 CFR § 164.402 [2][i-iv].

Reportable Breaches in the 1st Quarter

5) As stated above, there was one (1) reportable breach in the 1st Quarter. Below is a summary of said breach:

➤ *NYC Health + Hospitals/Coney (“Coney”) – March 2017*

Incident: This incident was discovered on March 10, 2017, and took place over a period of three months beginning in December 2016 until March 2017. The incident involved a volunteer who began working in the Phlebotomy department at Coney without appropriately being processed through Coney’s Human Resources Department. Nonetheless, a supervisor within the Phlebotomy department improperly arranged, under her supervision, for the volunteer to complete certain tasks within the department. These tasks involved, without limitation, logging patient names in a log book, cleaning up storage department areas, and transporting specimens within the Coney Island facility. In completing some of these tasks, the volunteer was permitted access to patient PHI such as name, medical record number, and date of birth when logging patient information into a log book and transporting specimens. However, because the volunteer was not appropriately processed by Coney’s Human Resources Department, she was not authorized to access patient PHI.

Breach Determination: Based upon the facts found during the investigation, the incident was determined to be a breach. Notification was sent to the affected individuals, a total of 3,494 individuals, on May 9, 2017. Because the number of affected individuals exceeded 500, a media notice was provided as well as the breach information was posted on the System’s public website. Additionally, the breach was also reported to the Office of Civil Rights (“OCR”) of the Department of Health and Human Services (“HHS”).

Mitigation: The supervisor of the department where the volunteer performed functions was immediately suspended as a result of the incident and is no longer employed at Coney. On May 10th, 2017, Wayne A. McNulty, Senior Assistant Vice President and Chief Corporate Compliance Officer, Office of Corporate Compliance (“OCC”), and several other OCC compliance personnel conducted training for the phlebotomy department staff on HIPAA compliance.

II. Monitoring of Excluded Providers

Overview of Regulatory Requirements

1) Federal regulations prohibit the allocation of Federal health care program (e.g., Medicaid, Medicare) payments “for any item or service furnished . . . by an excluded individual or entity, or at the medical direction or on the prescription of a physician or other authorized individual who is

OFFICE OF CORPORATE COMPLIANCE

excluded when the person furnishing such item or service knew or had reason to know of the exclusion.”⁴ Likewise, New York State (the “State”) has promulgated billing prohibitions related to services furnished by an excluded provider. Lastly, to maintain an active enrollment status in the Medicare program, NYC Health + Hospitals must certify that it does not employ or contract with individuals or entities that are “excluded from participation in any Federal health care programs for the provision of items and services covered under the programs.”⁵

Responsibilities of the System for Sanction List Screening

2) To adhere to these regulations, and consistent with the recommendations of the NYS Office of the Medicaid Inspector General (“OMIG”)⁶ and the United States Department of Health and Human Services Office of the Inspector General (“OIG”), each month the Office of Corporate Compliance (“OCC”) reviews the exclusion status of the NYC Health + Hospitals workforce (e.g., employees, board members, affiliates, personnel, volunteers, and medical staff members), vendors, and DSRIP partners.

Office of Foreign Asset Control (“OFAC”) Screening

3) To ensure that NYC Health + Hospitals does not conduct business with individuals or entities that are a threat to the security, economy, or foreign policy of the United States, the OCC also screens all NYC Health + Hospital Workforce members, vendors and DSRIP partners against the data bases of the U.S. Department of Treasury Office of Foreign Asset Control (“OFAC”).⁷

Exclusion and Sanction Screening Report for March 22, 2017 through June 1, 2017

4) Since the OCC last reported excluded provider activities at the April 4, 2017 Audit Committee, no new excluded providers have been identified.

⁴ Scope and Effect of Exclusion 42 CFR § 1001.1901 (b); *see also* 42 CFR § 1002 (the authority of State agencies to exclude on their own initiative, regardless of whether the OIG has excluded an individual or entity).

⁵ *See* 42 CFR § 424.516 (a) (3); *see also* 42 CFR § 424.535(a) (2) (regarding CMS’ option to revoke enrollment and billing privileges due to exclusion from Medicare, Medicaid or any federal program). *See also* 42 USC 1320c-5 (Regarding obligations of health care practitioners and providers and the Secretary of Health and Human Services ‘right to exclude a person or entity for failing to meet the obligations.)

⁶ DOH Medicaid Update April 2010, Vol.26, No. 6 and the NY OMIG webinar #22 OMIG Exclusion and Reinstatement Process, <https://omig.ny.gov/resources/webinars/811-omig-webinar-22> [Slide 20 (Sept 2014), accessed Feb. 2, 2017.]

⁷ *See* Frequently Asked Questions: **Who must comply with OFAC regulations?** United States Treasury website, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx [accessed Feb. 1, 2017.]

Death Master and NPPES Screening to Prevent Identity Theft

- 5) Center for Medicare and Medicaid regulations⁸ and the contractual provisions found managed care organization (“MCO”)⁹ provider agreements both require screening of NYC Health + Hospitals workforce members and certain business partners (collectively “Covered Persons”) to ensure that none of these Covered Persons are using the social security number (“SSN”) or National Practitioner Identification Numbers (“NPI”) of a deceased person in an effort to hide their true identity. This screening may be accomplished by vetting the SSNs and NPIs of Covered Persons through the Social Security Administration Death Master File (“DMF”) and the National Plan and Provider Enumeration System (“NPPES”), respectively.
- 6) The OCC currently screens the DMF and NPPES files as part of its sanction screening process.

III. Summary of Compliance-Related Reports for the First Quarter of Calendar Year 2017

Summary of Reports

- 1) For the first quarter CY2017 (January 1, 2017 to March 30, 2017) there were 96 compliance-based reports of which 2 (2.1%) were classified as Priority “A”; 41 (42.7%) were classified as a Priority “B”; and 53 (55.2%) were classified as a Priority “C”.¹⁰

Report Analysis

For purposes here, the term “reports” means compliance-based inquiries and compliance-based complaints. The breakdown of 1st quarter reports by subject, source and allegation are as follows:

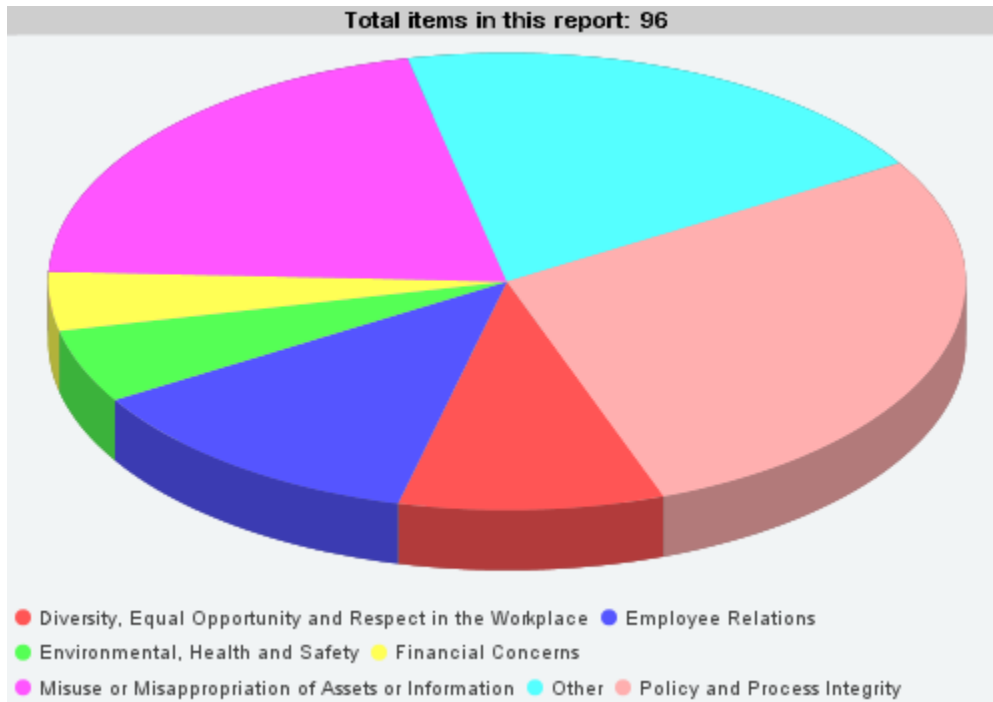
⁸See CMS’s Toolkit to Address Frequent Findings 42 CFR § 455.436 Federal Database Checks, <https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/FraudAbuseforProfs/Downloads/fftoolkit-federal-database-checks.pdf> (accessed June 1, 2017), see also generally, 42 CFR § 455.436;

⁹Provider ... agrees to monitor its employees and staff against the List of Excluded Individuals and Entities (LEIE), the Social Security Administration Death Master List, and the National Plan Provider Enumeration System (NPPES”).

New York State Department of Health Standard Clauses for Managed Care Provider/IPA Contracts, Appendix Revised April 1, 2017, at 4, available at: https://www.health.ny.gov/health_care/managed_care/hmoipa/docs/standard_clauses_revisions.pdf, (accessed June 1, 2017).

¹⁰ There are three (3) different report categories: (i) Priority “A” reports - matters that require immediate review and/or action due to an allegation of immediate threat to a person, property or environment; (ii) Priority “B” reports – matters of a time-sensitive nature that may require prompt review and/or action; and (iii) Priority “C” reports – matters that do not require immediate action.

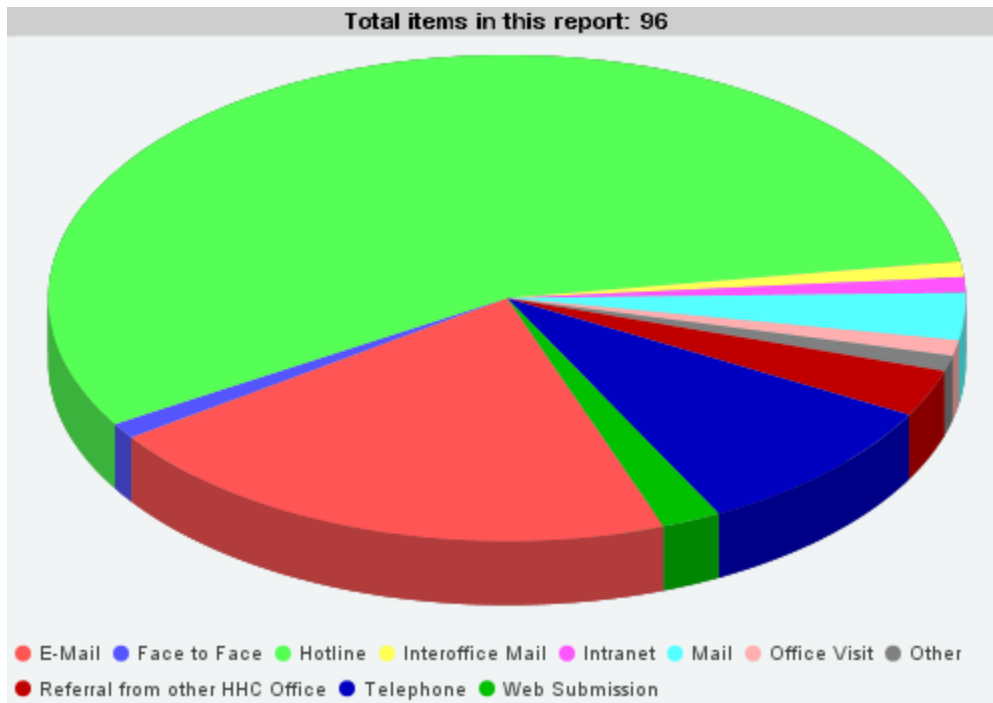
I. By Subject



PRIMARY ALLEGATION CLASS - CHART DATA

	Frequency (Percentage)
Diversity, Equal Opportunity and Respect in the Workplace	9.0 (9.4 %)
Employee Relations	12.0 (12.5 %)
Environmental, Health and Safety	5.0 (5.2 %)
Financial Concerns	4.0 (4.2 %)
Misuse or Misappropriation of Assets or Information	20.0 (20.8 %)
Other	19.0 (19.8 %)
Policy and Process Integrity	27.0 (28.1 %)
Totals	96.0 (100%)

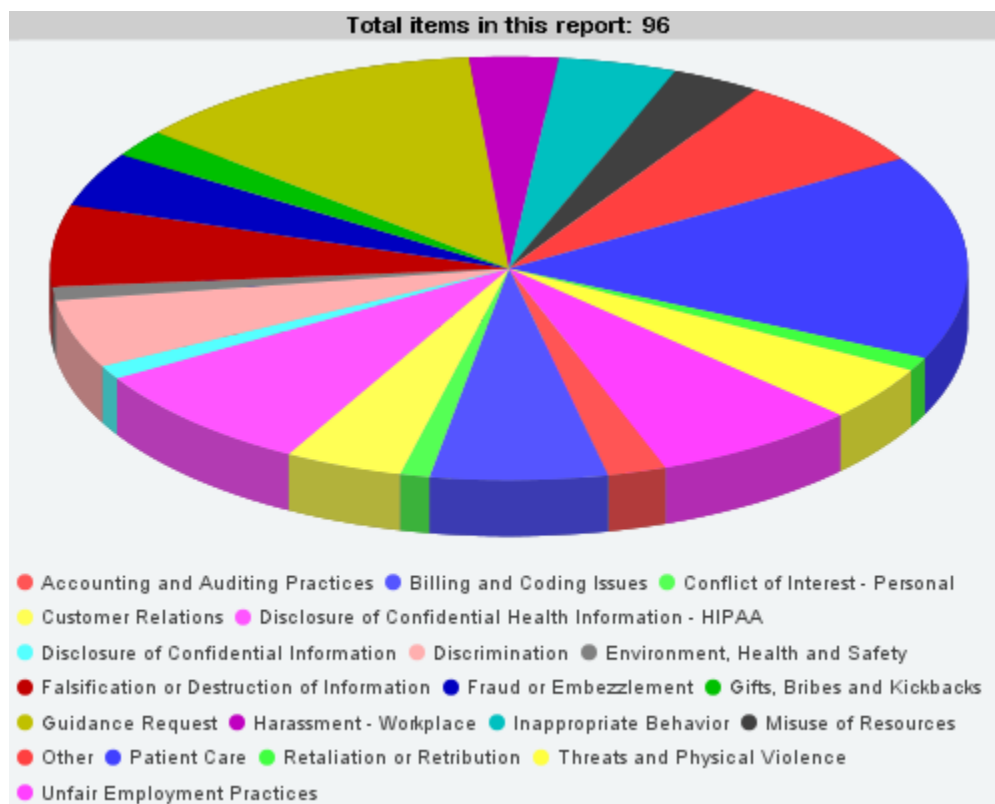
II. By Source



SOURCE - CHART DATA

	Frequency (Percentage)
E-Mail	20.0 (20.8 %)
Face to Face	1.0 (1 %)
Hotline	54.0 (56.2 %)
Interoffice Mail	1.0 (1 %)
Intranet	1.0 (1 %)
Mail	3.0 (3.1 %)
Office Visit	1.0 (1 %)
Other	1.0 (1 %)
Referral from other System Office	3.0 (3.1 %)
Telephone	9.0 (9.4 %)
Web Submission	2.0 (2.1 %)
Totals	96.0 (100%)

III. By Allegation



PRIMARY ALLEGATION TYPE - CHART DATA

	<u>Frequency (Percentage)</u>
<u>Accounting and Auditing Practices</u>	<u>2.0 (2.1 %)</u>
<u>Billing and Coding Issues</u>	<u>6.0 (6.2 %)</u>
<u>Conflict of Interest - Personal</u>	<u>1.0 (1 %)</u>
<u>Customer Relations</u>	<u>4.0 (4.2 %)</u>
<u>Disclosure of Confidential Health Information - HIPAA</u>	<u>8.0 (8.3 %)</u>
<u>Disclosure of Confidential Information</u>	<u>1.0 (1 %)</u>
<u>Discrimination</u>	<u>5.0 (5.2 %)</u>
<u>Environment, Health and Safety</u>	<u>1.0 (1 %)</u>
<u>Falsification or Destruction of Information</u>	<u>6.0 (6.2 %)</u>
<u>Fraud or Embezzlement</u>	<u>4.0 (4.2 %)</u>
<u>Gifts, Bribes and Kickbacks</u>	<u>2.0 (2.1 %)</u>
<u>Guidance Request</u>	<u>12.0 (12.5 %)</u>
<u>Harassment - Workplace</u>	<u>3.0 (3.1 %)</u>

OFFICE OF CORPORATE COMPLIANCE

<u>Inappropriate Behavior</u>	<u>4.0 (4.2 %)</u>
<u>Misuse of Resources</u>	<u>3.0 (3.1 %)</u>
<u>Other</u>	<u>7.0 (7.3 %)</u>
<u>Patient Care</u>	<u>15.0 (15.6 %)</u>
<u>Retaliation or Retribution</u>	<u>1.0 (1 %)</u>
<u>Threats and Physical Violence</u>	<u>4.0 (4.2 %)</u>
<u>Unfair Employment Practices</u>	<u>7.0 (7.3 %)</u>
<u>Totals</u>	<u>96.0 (100%)</u>

IV. Status Update - DSRIP Compliance Attestation of OneCity Health Partners

Background

1) As previously reported to the Audit Committee in April 2017, as a Performing Provider System (“PPS”) lead in the New York State Department of Health Delivery System Reform Incentive Payment (“DSRIP”) Program, NYC Health + Hospitals/OneCity Health (“OneCity Health”) is responsible for taking “reasonable steps to ensure that [M]edicaid funds distributed as part of the DSRIP program are not connected with fraud, waste, and abuse. It is reasonable for a PPS Lead to consider its network performing providers’ program integrity systems when dedicating resources and developing the PPS Lead’s systems.”¹¹ To satisfy its compliance obligations as the PPS Lead and to fulfill the requirements of the Office of Medicaid Inspector General (“OMIG”) DSRIP compliance guidance, OneCity Health developed a compliance Attestation form, which was designed to assess the compliance program integrity of its Partners.

The Attestation Form, Process and Results

- 2) On February 2, 2017, the Office of Corporate Compliance (“OCC”) distributed a Memorandum and a Compliance Attestation to be completed by all OneCity Health Partners.
- 3) In the Attestation, OneCity Health Partners were asked to provide the following information to the OCC:
- The status of their completion of DSRIP compliance training (a training PowerPoint had previously been previously provided to the Partners);
 - An acknowledgement that their workforce members have adopted the *NYC Health + Hospitals Principles of Professional Conduct (“POPC”)* or their own

¹¹ Office of the Medicaid Inspector General Delivery System Reform Incentive Payment (“DSRIP”) Program DSRIP Compliance Guidance 2015-01 –revised – Special Considerations for Performing Provider System (“PPS”) Leads’ Compliance Program available at:
https://www.omig.ny.gov/images/stories/compliance_alerts/20150901_DSRIP_CompGuidance_2015-01_Rev.pdf

OFFICE OF CORPORATE COMPLIANCE

organization's code of conduct that includes the POPC's core objectives or substantially similar compliance goals;

- Proof of New York State Office of Medicaid Inspector General ("OMIG") compliance program-related certifications by Partners that are required by law and/or OMIG policy to submit such certifications; and
- Confirmation that they were routinely screening their workforce members for exclusions from Federal healthcare programs and government contracting.

4) The two OMIG compliance certifications referenced in paragraph 3 of this section are as follows:

- New York Social Services Law § 363-d Certification; and
- The Deficit Reduction Act of 2005 ("DRA") Certification.

5) The answers provided by the Partners in the Attestation will be utilized by the OCC to:

- Assess the compliance program integrity of its Partners; and
- Satisfy OneCity Health's DSRIP Program compliance oversight obligations as they relate to the allocation of DSRIP funds.

Status of Compliance Attestations

Previous Partner Count

6) As noted in the April Audit Committee report, Attestations were sent to 228 Partners. The methodology utilized to count partners has since been revisited and revised.

Current OneCity Health Partner Count

7) For purposes of DSRIP contract execution, NYC Health + Hospitals OneCity Health counts partners at the system level. Moving forward, Attestations will be counted utilizing the same methodology. For example, Community Healthcare Network would count as 1 partner (system), comprising of > 5 sites. Thus, the number previously used by the OCC and reported to Audit Committee -- n = 228 -- was pulled from a OneCity Health newsletter distribution list, which contained duplications, or multiple contacts within same partner system. The de-duplicated number is n=203.

OFFICE OF CORPORATE COMPLIANCE

8) The OneCity Health team and the OCC have decided that the target group (or “denominator”) for attestations would be limited to those who would execute a Schedule B for time period of April 2017 to December 2017. The Schedule B is a contract that outlines performance requirements to earn DSRIP funding (“funds flow”).

- Of 203 who could potentially sign a Schedule B, 193 have completed the same; and
- As of June 8, 2017, of 193 who have actually signed the Schedule B, 157 (81%) have completed the compliance Attestation

OneCity Health Partner Outreach

9) With regard to the execution of Schedule B, as noted above, 193 partners of a potential 203 have signed a Schedule B (95%) as of June 6, 2017.

- The 10 who did not sign are partners that continue to be unresponsive despite outreach attempts and those that actively declined.
- Partner-cited reasons for declination include capacity concerns and organizational/legal changes due to M&A activities.

10) Partner outreach and engagement began well before April, 2017 contract issuance - -

- Monthly webinars, newsletters, and a Project Advisory Committee (PAC) meeting open to all OneCity Health stakeholders, with targeted follow up thereafter as needed.

11) For completion of compliance program Attestation, the OneCity Health team is including reminders to Partners in monthly webinars and newsletters. Additionally, the OCC has sent numerous email reminders to Partners and has communicated directly with Partners via telephone to encourage the expeditious completion of the Attestation.

V. Status Update - NYC Health + Hospitals’ Compliance with the HIPAA Security Rule Risk Analysis Requirements

Overview

1) On February 7, 2015, Wayne A. McNulty, Senior Assistant Vice President/Chief Corporate Compliance Officer, provided the Audit Committee with an overview of the System’s compliance with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA” or the “Act”) and

its implementing regulations (found at 45 CFR Parts 160 and 164, “The Security Standards for the Protection of Electronic Protected Health Information (the “Security Rule”)), which requires that the System implement a risk assessment program the purpose of which is to prevent, detect, contain, and correct security violations affecting electronic protected health information (“EPHI”).¹²

Security Rule Requirements

2) Specifically, the Security Rule requires that covered entities, such as NYC Health + Hospitals, perform periodic technical and non-technical evaluations of applications that access, house or transmit EPHI. More specifically, NYC Health + Hospitals 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 NYC Health + Hospitals’ information systems and applications. NYC Health + Hospitals is also required, at minimum, to conduct periodic technical and nontechnical evaluations of those systems and applications to establish the extent to which NYC Health + Hospitals security policies and procedures meet the requirements of the Security Rule.¹³

Status of NYC Health + Hospitals’ Compliance with Security Rule Risk Analysis Requirements as of February 2015

3) With regard to NYC Health + Hospitals compliance with the Security Rule risk analysis requirements, the OCC informed the Audit Committee that, in pertinent part:

- the inventory of the NYC Health + Hospitals information systems and applications that access, house, or transmit EPHI was a work in progress and therefore is not comprehensive at this juncture; and
- although Enterprise Information Technology Services (“EITS”) has taken numerous and significant measures to enhance and maintain the confidentiality, integrity, and security of NYC Health + Hospitals information systems including the formation of an information governance and security program, the implementation of security controls, and the performance of a formal risk analysis on a handful of its applications, it appears that further measures must be taken by

¹² Security Standards for the Protection of Electronic Protected Health Information (the “Security Rule”) found at 45 CFR Part 160 and Part 164, Subparts A and C, was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The HIPAA Security Rule is all about implementing effective risk management to adequately and effectively protect EPHI. The assessment, analysis, and management of risk provides the foundation of a covered entity’s Security Rule compliance efforts, serving as tools to develop and maintain a covered entity’s strategy to protect the confidentiality, integrity, and availability of EPHI; *see also, generally*, 18 NYCRR Part 521.

¹³ 45 CFR §164.308 (a)(8).

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

Recommendations

- 4) The OCC recommended that the following measures be taken by EITS:
- Identify and inventory, as a priority and no later than within 30-days, all NYC Health + Hospitals systems and applications that access, house or transmit EPHI;
 - Provide a written schedule that will specify date(s), over an 12-month period, by which all inventoried NYC Health + Hospitals systems and applications that access, house or transmit EPHI will have a completed risk analysis;
 - Provide a written schedule that will specify date(s), over a 12-month period, by which all inventoried NYC Health + Hospitals systems and applications that access, house or transmit EPHI will have been assessed as to the presence of the required implementation standards set forth in the Security Rule;
 - Provide a written schedule that will specify date(s), over a 12-month period, by which all systems and applications that access, house or transmit EPHI will have been assessed as to the presence of each addressable implementation standard set forth in the Security Rule or, in the alternative, documentation as to the reason(s) why the addressable specification was not implemented;
 - Immediately begin a risk analysis of the top 25 high-risk applications (based on criticality, amount of EPHI, impact etc.);
 - Inventory all remediation recommendations resulting from any completed risk analysis and document that the required remediation was completed or, if not completed, provide a date by which remediation was expected;
 - Ensure that, regardless of the methodology used to perform the required risk analyses, any risk analysis that is performed consists of and documents the following eight steps:

OFFICE OF CORPORATE COMPLIANCE

- Outline the scope of the analysis (including the potential risks, threats, vulnerabilities to the confidentiality, availability and integrity of all e-PHI that NYC Health + Hospitals creates, receives, maintains, or transmits);
 - Collect/gather data (identification of where data is stored);
 - Identify and document potential threats and vulnerabilities;
 - Assess current security measures;
 - Determine the likelihood of threat occurrence;
 - Determine the potential impact of threat occurrence;
 - Determine the level of risk present; and
 - Document all findings and risk analysis conclusion.
- Use a recommended best practice guide when performing a risk analysis to enhance the likelihood of compliance with the Security Rule. Such guides include, but are not limited to, the National Institute of Standards and Technology (NIST) Introductory Resource for implementing the Security Rule¹⁴ and HIPAA Guidance on Risk Analysis Requirements under the HIPAA Security Rule.¹⁵

Management's Response

- 5) In response to OCC's findings and recommendations, EITS announce the procurement of a third-party vendor to provide, among other things, the following services:
- HIPAA Risk Analysis (Application & EPHI);
 - HIPAA Compliance Assessment;

¹⁴NIST - An Introductory Resource for Implementing the Health Insurance Portability and Accountability Act ("HIPAA") Security Rule <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>; also see NIST Guide for Technology Systems at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf>

¹⁵ <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf>; see also Department of Health and Human Services. "Security Rule Guidance Material." at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html;

Department of Health and Human Services Standards for Privacy of Individually Identifiable Health Information; Final Rule." *Federal Register* 67, no. 157 (Aug. 14, 2002). at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-20554-filed.pdf and

National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995. Available online at <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>.

National Institute of Standards and Technology. "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." NIST Special Publication 800-66. October 2008. at <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>.

OFFICE OF CORPORATE COMPLIANCE

- Application Security – Penetration Test;
- Infrastructure Security – Internal Penetration Testing;
- Infrastructure Security – Internal Server Penetration Testing;
- Infrastructure Security- Perimeter/DMZ Penetration Assessment; and
- Vendor/Third Party Assessment.

6) Additionally, Sal Guido, then Senior Assistant Vice President/Acting Chief Information Officer, addressed the Audit Committee in April 2016 and, in summary, noted additional measures EITS had implemented to address the risk assessment requirements mentioned above. At the request of the Audit Committee, Mr. Guido stated that he would provide the Audit Committee with an update of EITS's risk assessment efforts in the future.

Status of Risk Assessment Activities and Remediation Efforts as of June 2017

7) Since the April 2015 Audit Committee Report, EITS has carried out numerous information governance-related activities pertaining to the performing risk analyses of NYC Health + Hospitals' information systems that house, store, and transmit PHI. Mr. Guido, Senior Vice President/Chief Information Officer, will provide the Committee with a brief overview of these activities, which include, in pertinent part, the implementation of risk assessment activities covering the following risk areas:

- HIPAA (Privacy, Security, and Breach Notification Rules);
- Configuration Review (Network, Server, Workstations, and Applications);
- Internal Penetration Assessment;
- External Penetration Assessment
- Application Security Assessment (29 applications); and
- Vendor Risk Management (29 vendors).

8) Additionally, EITS has reported that a full analysis of the biomed equipment at all System facilities has taken place. Specifically, the following measures have been taken:

OFFICE OF CORPORATE COMPLIANCE

- A plan has been developed to replace all non-conforming equipment and software;
 - EPHI will be automatically removed from biomed devices to conform with the regulation;
 - Biomedical equipment/software has been remediated at Coney Island.
 - Funding has been approved in the April 2017 City capital budget; and
 - Purchase order (“PO”) requests are being generated for OMB and City comptroller for funding approvals.
 - Once PO requests are approved, all remaining biomed environments will be remediated in 12 months.
- 9) The Audit Committee will be briefed in greater detail at the September 2017 Audit Committee regarding the risk analysis methodology, management, and activities regarding NYC Health + Hospitals’ biomedical equipment.
- 10) Annexed as to this report as Attachment “A” is a PowerPoint presentation prepared by Mr. Guido, which summarizes NYC Health + Hospitals recent risk analysis activities and future strategic plan as it relates to the same.

Attachment "A"



HIPAA & Security Risk Assessment Status

EITS Information Security & Risk Management

May 23, 2017



HIPAA Compliance and Annual Information Security Risk Assessment

- NYC Health + Hospitals entered into a three-year agreement in Year 2015 with a third-party vendor Solutionary, a Dimension Data and NTT Group Security Company (now known as NTT Security and defined in this document hereinafter as “NTT”), to perform, among other various information security services, functions, and duties, the following review at its facilities:
 - (i) a risk analysis on systems that house, store, and transmit electronic protected health information (“EPHI”);
 - (ii) HIPAA Privacy and Security Rule assessments. The following areas are covered by this comprehensive assessment:
 - All NYC Health + Hospitals facilities (including off-sites) covering:
 - HIPAA (Privacy, Security, and Breach Notification Rules)
 - Configuration Review (Network, Server, Workstations, and Applications)
 - Internal Penetration Assessment
 - External Penetration Assessment
 - Application Security Assessment (29 applications)
 - Vendor Risk Management (29 vendors)

Timeline: September 2015 – May 2016

Note: EITS Security manages HIPAA Security findings while Office of Corporate Compliance (OCC) manages HIPAA Privacy and Breach Notification findings. Status of findings on following slides are for EITS only.

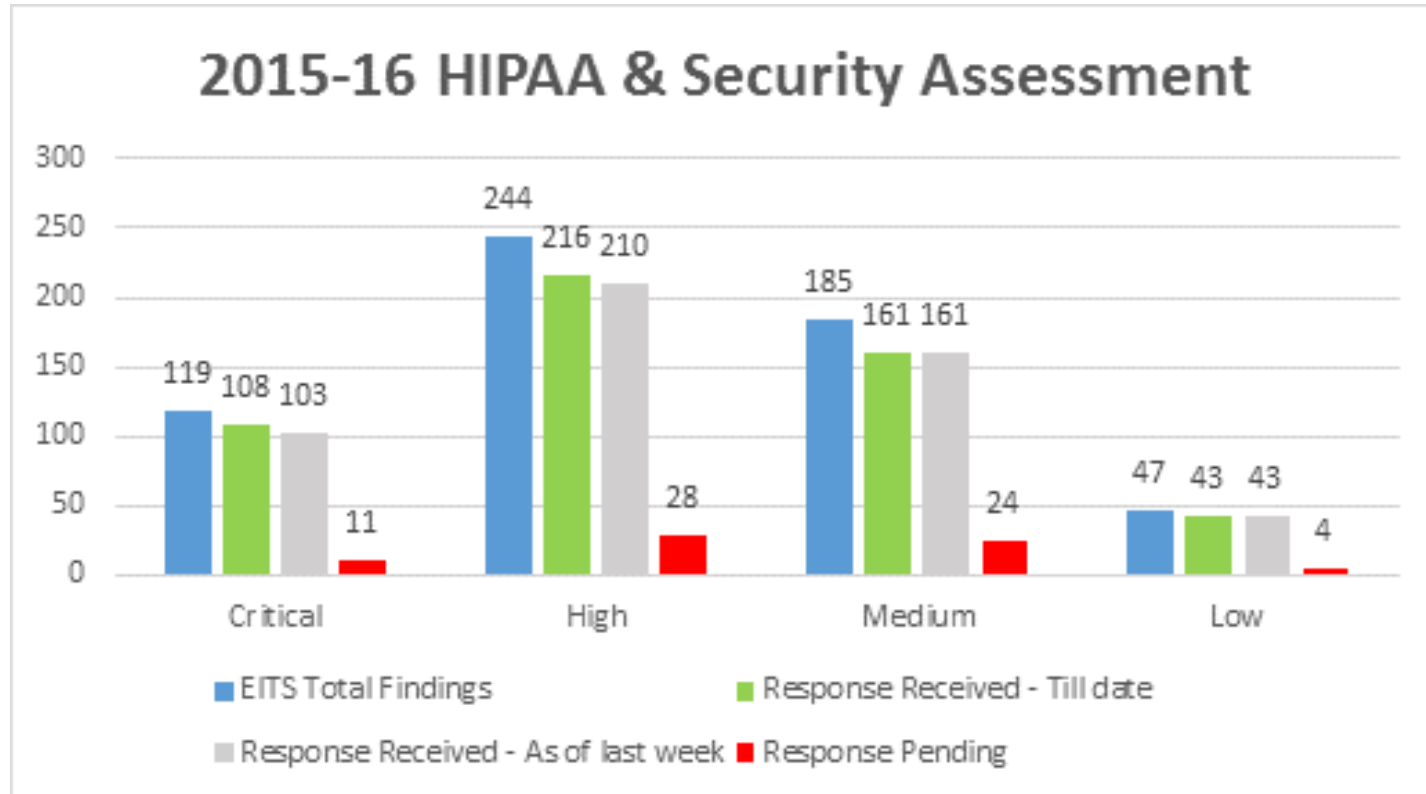
HIPAA Compliance and Annual Information Security Risk Assessment

- The Annual Risk Analysis & Security Assessment of NYC Health + Hospitals consisted of a high-level analysis and review of documentation, processes and procedures. The assessment represents a point-in-time review of the environment since information security is a moving target and threat vectors, known/unknown vulnerabilities, and the NYC Health + Hospitals environment is continuously changing.
- The assessment included policy and procedure reviews, interviews and observations, and a sampling of populations based on identified controls covering the following HIPAA Security-related areas:

Administrative Safeguard Requirements	Physical Safeguard Requirements	Technical Safeguard Requirements
<ul style="list-style-type: none"> • Security Management Process • Assigned Security Responsibility • Workforce Security • Information Access Management • Security Awareness & Training • Security Incident Procedures • Contingency Planning • Evaluation • BA Contracts and Other Arrangements 	<ul style="list-style-type: none"> • Facility Access Controls • Workstation Use • Workstation Security • Device and Media Controls 	<ul style="list-style-type: none"> • Access Controls • Audit Controls • Integrity • Transmission Security



EITS Remediation Status



As of 5/23/17

Information Governance Efforts around Bio-Medical Equipment:

- A plan has been developed to replace all bio-medical equipment and software that is not HIPAA-compliant from a point of view of security controls. EPHI will be automatically removed from biomed devices to conform to the regulation
- These efforts have already begun at NYC Health + Hospitals/Coney where Biomed equipment/software has been remediated.
- For enterprise-wide remediation efforts, additional funding has been approved in the April 2017 city capital budget. PO request are being generated for OMB and city comptroller for funding approvals
- Once PO are approved all remaining biomed environments will be remediated in 12 months.