NYC HEALTH + HOSPITALS

AUDIT COMMITTEE
MEETING AGENDA

April 9, 2019
11:00 A.M.

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

CALL TO ORDER — **Ms. Helen Arteaga Landaverde**

- **Adoption of Minutes February 14, 2019** — **Ms. Helen Arteaga Landaverde**
- **Adoption of Minutes December 13, 2018**

INFORMATION ITEMS

- **Audits Update** — **Mr. Chris A. Telano**
- **Compliance Update** — **Ms. Catherine Patsos**

EXECUTIVE SESSION

OLD BUSINESS

NEW BUSINESS

ADJOURNMENT

MINUTES

AUDIT COMMITTEE

MEETING DATE: February 14, 2019
TIME: 10:00 A.M.

COMMITTEE MEMBERS
Mitchell Katz, MD
Helen Arteaga Landaverde, MPH

STAFF ATTENDEES
Andrea Cohen, General Counsel, Legal Affairs
Colicia Hercules, Chief of Staff, Chairman's Office
Lisette Saravia, Senior Executive Secretary, Chairman's Office
Yvette Villanueva, Vice President, Human Resources
Jay Weinman, Corporate Comptroller
James Linhart, Deputy Corporate Comptroller
Catherine Patsos, Compliance Officer
Paul Albertson, Vice President, Supply Chain
Michelle Allen, Chief Medical Officer
Devon Wilson, Senior Director, Office of Internal Audits
Carlotta Duran, Assistant Director, Office of Internal Audits

NYC HEALTH + HOSPITALS

FEBRUARY 14, 2019
AUDIT COMMITTEE MEETING
MINUTES

Call to Order

Ms. Helen Arteaga Landaverde, Audit Committee Chair, called the meeting to order at 10:12 A.M. Ms. Arteaga Landaverde stated that since we do not have a quorum, we will not move to adopt the minutes of the Audit Committee meeting held on December 13, 2018.

INTERNAL AUDITS UPDATE

A. EXTERNAL AUDITS

1. Controls Over Equipment – Office of the State Comptroller

The objective of the audit included a physical verification of assets, and the review of the Fixed Asset System and asset disposal procedures. Testing was conducted at the following nine (9) facilities:

- NYC Health + Hospitals/Bellevue
- NYC Health + Hospitals/Elmhurst
- NYC Health + Hospitals/Jacobi
- NYC Health + Hospitals/Harlem
- NYC Health + Hospitals/Gotham Health, East New York
- NYC Health + Hospitals/Gotham Health, Belvis
- NYC Health + Hospitals/Gotham Health, Roberto Clemente
- NYC Health + Hospitals/Gotham Health, South Queens
- NYC Health + Hospitals/Sea View

They found that as of June 30, 2017, NYC Health + Hospitals had 203,659 assets with a net book value of $319 million. Pursuant to the audit of controls over movable equipment conducted by the NYS Comptroller's Office, which tested 338 pieces of movable equipment, only 18 pieces of equipment were not located (7%). These pieces of equipment had a total net book value of $17,924 as of June 30, 2017 (.006% of total net book value). Despite an audit revealing such a low number of equipment at issue, NYC Health + Hospitals agreed that some areas of tracking inventory could be strengthened and, as such, implemented a new mass retirement policy as well as committed to providing additional training to employees to mitigate any issues resulting from human error in recordkeeping.

2. Compliance with Federal Tax Requirements – Internal Revenue Service

After being on-hold during the government shutdown, this audit re-started on January 28, 2019. The objective of the audit is to ensure compliance with federal tax requirements as an exempt organization. All requested documents have been sent to the IRS. We are waiting their feedback.

B. OTHER AUDIT ACTIVITIES

a) Mayor's Office Communications

Periodically, the Office of Internal Audits receives status requests from the Audit Services function within the NYC Mayor's Office of Operations regarding audits being conducted by regulatory agencies of Health + Hospitals. OIA is responsible for regularly advising the individuals within Audit Services of the audits in progress, sending them draft/final reports and responses and inviting them to entrance and exit conferences.

A request regarding a Medicaid Audit was received and adequately responded to in January 2019.

b) Anonymous Letters

During Calendar Year 2018, 15 accusation letters were received by the Office of Internal Audits for their review, 5 alone in December. Most of the letters were found to be without merit or forwarded to other parties for review. Independent investigations were conducted of two anonymous letters received by the Office of the Chair. Internal Audits issued reports to the Chairman, President and Chief of Staff to the Board addressing the allegations within each letter.

c) Auxiliary Audits

An outside CPA firm (BKD, previously known as Loeb & Troper) conducts these financial statement certifications. The objective of these audits is to enable the auditors to express an opinion on the financial statements and provide reasonable, not absolute assurance, that the financial statements taken as a whole are free from material misstatement. Internal Audits responsibilities include:

- Meeting with BKD to develop the audit plan, issue notification letters to the Auxiliary representatives, and to assist the Auditors with any problems they may encounter.
- Reviewing the draft report, which includes comparing the numbers to the prior year's audit, requesting documentation to support certain financial information and inquiring about questionable numbers.
- Reviewing the final report to ensure it compares favorably to the draft report and issuing to the appropriate individuals at the Auxiliaries and NYC Health + Hospitals.

Twenty-one of twenty-two final reports were issued in 2018. The only audit not completed was of NYC Health + Hospitals/Queens. This was due to the Auxiliary not providing timely financial records needed to conduct the audit.

d) FOIL Request

A request for documents under the Freedom of Information Law was forwarded to Internal Audits on January 17, 2019. The New York Times made the initial request. The following documents were requested:

1) The results of any audits of spending by Health + Hospitals that were performed by outside agencies or third parties since 2014;
2) The conclusions of any internal investigations conducted by Health + Hospitals related to spending by the agency.

Five final reports from the NYC and NYS Comptroller's Offices were sent to H+H's FOIL Office in response to the first request. Only two were considered to be about Health + Hospitals spending.

The second request was not applicable as there were no internal investigations conducted.

CORPORATE COMPLIANCE UPDATE

I. Monitoring of Excluded Providers

Exclusion and Sanction Screening Report December 1, 2018 through January 31, 2019

During the period December 1, 2018 through January 31, 2019, there were no excluded individuals or providers.

As previously reported, on July 31, 2018, the OCC learned that a human resources administrator at NYC Health + Hospitals/Kings ("Kings), who was provided to NYC Health + Hospitals through a staffing agency, was an excluded individual. She worked at Kings from April 2018 through the end of July 2018. The OCC investigated the possibility of an overpayment for this individual and reported an overpayment to the OMIG, and the possibility of an overpayment to National Government Services. It was ultimately determined that an overpayment amount of approximately $9,000 was owed to the Medicaid program. That amount was fully repaid as of, December 24, 2018.

Death Master File and National Plan and Provider Enumeration System Screening

No providers were identified on the DMF or NPPES during the period December 1, 2018 through January 31, 2019.

II. Privacy Incidents and Related Reports

Reported Privacy Incidents for the period of December 1, 2018 through January 31, 2019

During the period of December 1, 2018 through January 31, 2019, seventeen (17) privacy incidents were entered into the RADAR Incident Tracking System. Of the seventeen (17) incidents, eight (8) were found after investigation to be violations of NYC Health + Hospitals HIPAA Privacy and Security Operating Procedures ("OPs"); six (6) were found not to be a violation of NYC Health + Hospitals HIPAA Privacy and Security OPs; and three (3) are still under investigation. Of the eight (8) incidents confirmed as violations, four (4) were determined to be breaches.

Reported Breaches for the Period of December 1, 2018 through January 31, 2019

NYC Health + Hospitals/Bellevue – December 2018

Incident: This incident was brought to our attention on December 24, 2018, and occurred when a patient contacted the Bellevue Administrator on Duty ("AOD") alleging that staff in the Comprehensive Psychiatric Emergency Program ("CPEP") had inappropriately provided medical records to an Administration for Children's Services' ("ACS") worker who subsequently used those records in a child custody court hearing.

Breach Determination: The OCC determined that a breach did occur, and that records were provided to the ACS worker without patient authorization. The staff involved in providing the records to the ACS worker was counseled and provided with targeted HIPAA remediation training, and administration distributed reminders regarding patient privacy to all staff within the department.

NYC Health + Hospitals/Kings – December 2018

Incident: This incident was brought to the attention of the OCC on December 27, 2018, when a patient reported that a Kings' employee videotaped her and her mother (who was also a patient) on October 29, 2018, while they were in a waiting area at Kings. The employee then posted the video on Facebook.

Breach Determination: After an investigation, it was determined that the employee took the video in the hospital waiting area; the patients' were identified in the video by name; and the information had been made available to thousands of people via Facebook. Breach notification will be sent to the affected individuals. The employee involved was counseled on the HIPAA privacy rights of patients. Labor Relations plans formal disciplinary action against the

employee and Kings' management would like to terminate the employee. Kings will also intensify HIPAA training for its staff.

NYC Health + Hospitals/Kings – December 2018

Incident: This incident was discovered on August 30, 2017, and occurred between December 20, 2014, and March 26, 2018. It involved a Kings employee who was misappropriating patient information and selling it to third parties. During the pendency of a joint investigation conducted by the United States Federal Bureau of Investigation ("FBI") and the NYC Health + Hospitals' Inspector General ("IG"), a law enforcement hold prevented NYC Health + Hospitals from providing notice to the affected individuals. As a result of the joint FBI and IG investigation, it was determined that the PHI of 419 patients was improperly disclosed by the Kings employee. This employee was terminated on April 9, 2018, and is being criminally prosecuted in Federal district court. The PHI disclosed included patients' names and telephone numbers. To the OCC's knowledge, no other information was disclosed. Although this incident occurred several months ago, the law enforcement hold was only lifted in December 2018, after which the System could send breach notifications to the affected individuals.

NYC Health + Hospitals/At Home – January 2019

Incident: This incident was brought to the OCC's attention on January 16, 2019, and involved a Health Home care coordinator who logged onto a non-secure web portal and shared PHI of a patient with the city's the Department of Homeless Services ("DHS"). Specifically, the care coordinator posted a complaint on DHS' web portal in an attempt to switch shelter accommodations for a patient, and in the process, shared the patient's PHI on the portal. The care coordinator had not been authorized to share that information, and had not informed her supervisor that she was making a complaint on the web portal. The patient information in the complaint included the patient's name, date of birth, and mental health and medical condition.

Mitigation: The Health Home care coordinator will be retrained on HIPAA, the importance of maintaining the confidentiality of patient information, and the need to safeguard such information. Further disciplinary action may be taken against the care coordinator based on additional information.

Office for Civil Rights ("OCR") Inquiries Regarding Privacy Incidents

There were no inquiries initiated by the OCR during the period December 1, 2018 through January 31, 2019.

III. Compliance Reports

Summary of Reports for the Period of December 1, 2018 through January 31, 2019

For the period December 1, 2018 through January 31, 2019, there were fifty-six (56) compliance reports, none of which were classified as Priority "A," fifteen (15) (27%) were classified as Priority "B," and forty-one (41) (73%) were classified as Priority "C" reports. For purposes here, the term "reports" means compliance-based inquiries and compliance-based complaints.

Priority B Report of Note: The OCC received a complaint filed by an employee at Gouverneur, who alleged inappropriate and unprofessional behavior, up to and including fraud, by NYC Health + Hospitals leadership, including a lack of monitoring of document verification by the Office of Medical and Professional Affairs ("OMPA"), missing signatures, falsified information on credentialing documents, and an inappropriate use of signature stamps for document approvals. The employee also alleged that there was targeted harassment toward her by the OMPA, resulting in her transfer to a different position and location at Gouverneur. Following an investigation by the OCC, however, it was discovered that this employee had in fact knowingly submitted unverified and possibly incorrect

credentialing information on her report to the OMPA, which detailed provider profile listings of the approval dates for the Gotham Health transitioned providers indicating that their credentialing files were verified as complete, when they were not. The employee admittedly altered the "Date" field in the electronic credentialing system (IntelliCred) so that it appeared that all of the required providers for that time period had been fully vetted. She further reported that not only was the credentialing information in the electronic record incomplete, but in some cases inaccurate.

In addition, the employee reported that she completed certain training courses for a physician, which were required for the physician's credentialing. The OCC's investigation revealed that the physician's assistant instructed the employee to "handle" certain credentialing items, including one of the training courses, on behalf of the physician. The investigation also revealed that the employee obtained additional credentialing information on the physician's behalf.

Based on the findings of its investigation, the OCC recommended that the employee be suspended or terminated. The OCC submitted its findings and recommendation to Human Resources, and the employee was subsequently terminated.

IV. Status Update - HHC ACO, Inc.

1) As reported at the June 2018 Audit Committee meeting, on October 5, 2017, HHC ACO, Inc. ("HHC ACO") submitted an application to the New York State Department of Health ("DOH") seeking approval for an "all payer" Accountable Care Organization ("ACO"), which includes Medicaid, commercial insurance, and Medicare Advantage. In December 2018, HHC ACO finally received a Certificate of Authority from DOH authorizing it to operate as an all payor ACO.

2) Prior to issuing the final rule, CMS announced that ACOs might elect to extend their participation agreements for six months. CMS permitted this extension to allow ACOs more time to implement two-sided risk arrangements. HHC ACO, therefore, elected to extend its participation agreement with CMS through June 30, 2019.

3) Currently, HHC ACO is applying to CMS for a contract to adopt the enhanced track of the MSSP, beginning July 1, 2019, which will involve potential shared losses, as well as shared savings. The shared savings, however, could potentially be as much as 75% of the savings to the Medicare program. Although the enhanced track provides for enhanced savings, it also carries the most risk – amounting to 40% to 75% of the losses to the Medicare program. The losses, however, are adjusted by HHC ACO's quality scores, and capped at 15% of the benchmark.

Aetna Desk Review

1) As previously reported, on January 31, 2018, the OCC received notification from Aetna of a Notice of Compliance Program Audit (the "Notice"), requesting information from NYC Health + Hospitals relating to its compliance with Medicare Parts C and D compliance program elements as required by CMS. The Notice stated that the review would include functions performed by the System (particularly the OCC) which are related to Aetna's Medicare Advantage, Prescription Drug Plans and/or Medicare – Medicaid Plan product lines. Aetna performs such reviews to ensure that the entities it contracts with, such as the System, meet their compliance program obligations. These reviews are conducted under the auspices of their "Delegated Vendor Oversight" responsibilities, as required by CMS.

2) On April 30, 2018, the OCC received Aetna's Compliance Program Elements Audit Report (the "Audit Report"), which included Aetna's conclusions regarding NYC Health + Hospitals' compliance with its audit. According to the Audit Report, NYC Health + Hospitals satisfied eight of the compliance requirements, but failed to satisfy four compliance requirements. The Audit Report also required NYC Health + Hospitals to submit corrective action plans to Aetna for the failed compliance requirements, which the OCC did on May 25, 2018.

3) On November 15, 2018, the OCC received an email from Aetna regarding its further review of the System's corrective action plans, stating that the System needs to revise its policies to meet a record retention requirement that the OCC believes does not apply to the System. The OCC conferred with the Office of Legal Affairs regarding the System's obligation to comply with this requirement, and responded that it continued to maintain its position that such requirement does not apply to the NYC Health + Hospitals.

4) On January 31, 2019, the OCC received another email from Aetna requesting that the OCC provide documentation to demonstrate the System's adherence to the CMS requirement related to retaining existing employee training records for a 10-year period. In addition, Aetna provided a random selection of five System employees with hire dates of 2009 and prior, which were identified from the System's original employee universe. Aetna requested that the OCC provide the necessary evidence demonstrating completion of these employees' Code of Conduct and Compliance training for the past ten years, by February 15, 2019.

Records Management

Prior Situation

1) As previously reported, in May 2018, a Records Task Force was formed to address the issue of more than 621,000 boxes of paper-based files in off-site storage at Iron Mountain, at an annual storage rate of more than $4,024,080.

2) In total, therefore, approximately 138,700 boxes were identified to be slated for destruction, which would save the System approximately $74,898 monthly and approximately $898,776 annually.

Next Steps & Future State of Records

1. The NY State Archives, which provides guidelines for the retention schedules for public agencies, such as NYC Health + Hospitals, published guidance in 2014 on imaging, including image resolution requirements for different types of documents, color and pixel depths, quality check methods and indexing procedures. The guidelines require a minimum of 300 Pixels Per Inch ("PPI") for most types of records. Over the years, however, the System has scanned its on-site records at a lower resolution than the required 300 PPI. Re-scanning these records to meet the 300 PPI requirement would be extremely cost-prohibitive. Also, given that the System's priority now is to implement digitization as a go-forward solution to the extent possible, expending resources toward this goal would be of the most benefit for its records management agenda.

2. Thus, for those documents scanned at the lower resolution, NYC Health + Hospitals needed to request a waiver from the NY State Archives of the 300 PPI resolution requirement and their approval to destroy all paper records that have been scanned at a lower resolution and thoroughly checked for quality issues.

3. Therefore, the RMO spoke with a representative of the NY State Archives to request such waiver and approval to destroy such paper records. The representative advised the RMO that, as long as the scanned records are operational and can be used for the System's business functions, and there is a documented memorandum in

the System's policies and procedures manual that includes the System's current state of digitized records with a strategy to approach digitization per NY State Archives' guidelines, the System would be able to destroy records scanned at the lower resolution. The Office of Legal Affairs concurred with this approach, in addition to memorializing the phone conversation with and emails received from the NY State Archives. Accordingly, the RMO has documented such memorandum

4. In early September, the RMO along with the Office of Supply Chain met with EITS to plan for digitization of records. In subsequent meetings, EITS presented the software solution OnBase to the Records Task Force, which can be used as an enterprise content management ("ECM") application. Among other things, an ECM application provides functionality such as indexing and labelling of digitized records, recording meta-data pertaining to the records, and manual or auto-purging of records past their retention period. Currently, OnBase is being used as an ECM application for Epic to store scanned patient records

5. On November 15, 2018, the RMO presented to the EITS Intake Meeting NYC Health + Hospitals' records digitization initiative as its future state for record retention. At the meeting, the EITS project management committee voted to advance the digitization initiative to the Health Information Technology ("HIT") Prioritization Committee, and assigned a project manager to the initiative. If the digitization initiative is accepted and voted upon as a "high priority" project at the upcoming HIT Prioritization Committee meeting, the initiative will become an "IT Project" which will be tracked and assigned technology resources.

There being no other business, the meeting was adjourned at 10:33 A.M.

MINUTES

AUDIT COMMITTEE

MEETING DATE: December 13, 2018
TIME: 12:00 P.M.

COMMITTEE MEMBERS

Mitchell Katz, MD
Gordon Campbell
Helen Arteaga Landaverde, MPH

STAFF ATTENDEES

Andrea Cohen, General Counsel, Legal Affairs
John Ulberg, Senior Vice President, Finance
Colicia Hercules, Chief of Staff, Chairman's Office
Lisette Saravia, Senior Executive Secretary, Chairman's Office
Paul Albertson, Vice President, Supply Chain
Kim Mendez, Chief Health Information Officer
Yvette Villanueva, Vice President, Human Resources
Jay Weinman, Corporate Comptroller
Janet Karageozian, Assistant Vice President, EITS
James Linhart, Deputy Corporate Comptroller
Catherine Patsos, Compliance Officer
Devon Wilson, Senior Director, Office of Internal Audits
Carlotta Duran, Assistant Director, Office of Internal Audits
Nicole Fleming, Controller, Central Office
Beverly Addai, Senior Accountant, NYC H+H/Metropolitan
John L. Cuda, Chief Financial Officer, MetroPlus

OTHER ATTENDEES

Grant Thornton: Tami Radinsky, Lead Engagement Partner; Dana Wilson, Insurance Audit Partner; Lou Feuerstein, Relationship Partner; Steven Dioguardi, Lead Audit Senior Manager.

Office of State Comptroller: Justine DeGeorge

NYC HEALTH+ HOSPITALS

DECEMBER 13, 2018
AUDIT COMMITTEE MEETING
MINUTES

Call to Order

The meeting was called to order at 12:07 P.M. by Mr. Gordon Campbell, Audit Committee Member. Mr. Campbell stated that as soon as Mr. Katz arrives, we will move to adopt the minutes of the Audit Committee meeting held on October 15, 2018.

Fiscal Year 2018 Draft Financial Statements

Mr. Campbell introduced the information item regarding the Fiscal Year 2018 Draft Management Letter.

Grant Thornton Management Letter

Ms. Radinsky presented by outlining the observations and recommendations.

Unlike a public company, we do not provide an opinion on internal control, under our professional standards noted on the Financial Statements issued in November 2018, we give an understanding of the control requirements, our processes and we do certain testing of the controls to support our process.

There are three levels of internal control deficiencies:

1. Control deficiency (lowest level) – exists when the design or operation of a control does not allow management or employee, in the normal course of performing their assigned functions, to prevent or detect and correct, misstatement on a timely basis.
2. Material weakness (highest level) – is a deficiency or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the System's financial statement will not be prevented or detected and corrected, on a timely basis.
3. Significant deficiency (middle category) – less severe than the material weakness, but it is important enough to warrant the attention of the Board and this Committee and those people in charge of governance.

Accounts Payable

Significant Deficiency – During fiscal 2018, New York City Health + Hospitals transitioned to PeopleSoft ERP for the general ledger function, including Vendor Accounts Payable. We noted that while the new PeopleSoft accounts payable system maintains adequate reports and did not reconcile to the general ledger old system.

We recommend that management put controls at an appropriate level of precision to prevent misstatement of the accounts payable balance and continue to work to find ways to reconcile balances for the old system for the remaining time it is in use. Any unusual reconciling items should be investigated and addressed in a timely manner.

Mr. Weinman added that this comment relates to the old system. Since the implementation of the ERP, at the end of this year, we are not going to have balances related to the old system. All vendor payables will be in the new system

as they are today and are already reconciled. We have accepted this comment, it is a long-standing comment that KPMG had for many years that the old system did not have adequate reports to reconcile. The adjustment made is immaterial to the financial statements and we recognized the need to move to a new system.

Patient Accounts Receivables and Net Patient Service Revenue – Credit Balances - we noted that credit balances in patient accounts receivable totalled approximately $80 million. We recommend that management develop a process to analyze the nature of the credit balances within patient accounts receivable and, on a monthly basis, record adjustments in the accounting records to reflect their proper disposition. In addition, management should investigate and determine the root cause for the credit balances while they are current. We understand that there is an EPIC system that the credit balances are being tracked electronically and routed to the appropriate people to investigate.

Dr. Katz asked what causes a credit balance in our system.

Mr. Weinman answered that for a single patient who has many visits, a payment for a visit was posted to a different visit that would cause an open balance for a visit and an overpayment to different visit.

Dr. Katz added that this should be routed to the appropriate department to make sure that the appropriate payment is applied to the account.

Patient Accounts Receivable and Net Patient Revenue – Patient revenue recorded after fiscal year-end for services prior to fiscal year-end.

We noted that patient service revenue is recognized for services based on the date those services are entered into the patient accounting system rather than as of the date the service was provided. As a result, the recording of revenue can occur up to several days subsequent to the date the service was provided. We noted that in fiscal 2017, revenue was recorded in a similar manner. Through audit procedures performed, we determined that the net impact of the improper cutoff of revenue between fiscal year 2017 to fiscal year 2018 was immaterial. This immaterial does not reflect the financial statements as a dollar value.

We recommend that management develop a process to determine the amount of revenue recorded in the month subsequent to the month that the service was provided and assess the net impact in order to determine if an adjustment to revenue is necessary.

Patient Accounts Receivable and Net Patient Service Revenue – Controls over manual data entry into the patient accounting system.

We noted two high dollar manual adjustments to patient account balances that were made in error. We recommended that NYC Health + Hospitals develop and formalize a policy consistent across all facilities, which requires periodic review of high dollar manual adjustments to patient account balances and high dollar patient account balances to ensure the accuracy of patient service revenue and accounts receivable. NYC H+H is in the process of building reports in Unity and Soarian to identify accounts with high dollar charges which will allow the facilities' Directors of Revenue Management to identify abnormal charges.

Information Technology

We performed systematic and automated controls that relate to the systems in place. We concentrated on the financial dependent systems; PeopleSoft, Unity and Sorian. We have a few comments related to information technology:

1. Unidentifiable Users – we identified one person having a Network administrator account that was not listed as an employee or outside consultant. We recommend that management reviews the active account listing to ensure that only appropriate and active users have access as a Network administrator. In addition, we recommend that management considers removing administrator responsibilities from personnel who are not part of the IT security group. If segregating security administration responsibilities is not feasible, personnel independent of the functional department should perform a periodic review of administrative users' activities to ensure that only authorized activities are performed. Evidence of this review should be retained. Management has verified that the identified person is a consultant and will update the active account listing to reflect that information. Additionally, the IT department already implemented a process which requires all staff seeking domain access to go through PeopleSoft's IdentityIQ which generates an active directory account.
2. Segregation of Duties – We noted that a couple of PeopleSoft security administrators have access to source code and to modify production. We recommend limiting program maintenance access to IT personnel who do not have security administrator privileges. If segregation of duties is not feasible, management should consider implementing mitigating controls (e.g., an activity log report of the administrators' actions reviewed by an independent party on a regular basis) to compensate for the lack of segregation around operating and security related functions. Management already has a process in place where all the migrations are done using a version control and migration tool called PHIRE. This tool maintains all the activity logs and every migration has an audit trail of who had performed a migration and what objects were migrated. Management will implement audits of these pre-existing logs going forward.
3. Sharing Account – we noted that 'sysadmin' account on the PeopleSoft database is shared by the PeopleSoft Administrators team and the Database Administrators team. We recommend that in order to promote accountability for activities performed using privileged accounts, management requires unique user IDs be utilized so that system activities are traceable to an individual. Management agrees with the recommendation and, moving forward, will request that all individuals associated with Database Administrator and/or PeopleSoft Administrator teams maintain individual accounts.
4. User Access Review – we noted that the System does not perform a formal periodic review of Network PeopleSoft, Unity, and Soarian user entitlements to ensure access changes were conducted in accordance with management's expectations. We recommend management performs a comprehensive review of user access entitlements on a regular basis (i.e., at least once per fiscal year).
5. User Administration: New Hires - although a ticketing system is in place, management was unable to provide adequate documentation for the new hire sample we selected for testing due to the switch from Remedy to ServiceNow. We recommend that IT maintain complete documentation regarding all newly hired personnel. In the event that application access was added post hire, any changes to user access rights should be documented and approved by appropriate stakeholders. Management responded that the ticketing interface between ServiceNow and SailPoint IdentityIQ is in progress. We are awaiting the purchase of the required software and, once purchased, the integration process will be in place by end of fiscal year 2019.

CORPORATE COMPLIANCE UPDATE

Ms. Patsos began her update with Monitoring Excluded Providers -

Exclusion and Sanction Screening Report October 1, 2018 through November 30, 2018

During the period October 1, 2018 through November 30, 2018, there was one excluded individual and follow up regarding a previously identified excluded individual.

On October 16, 2018, the OCC was notified that a patient care associate at NYC Health + Hospitals/Lincoln appeared on the System for Award Management ("SAM") list as having been excluded by the Department of Education. She was excluded due to her lack of business honesty or integrity, pending completion of an investigation/legal proceeding. The individual was terminated on October 16, 2018, and there is no overpayment issue for this individual because she has not been excluded by the Office of the Medicaid Inspector General or the Office of Inspector General from participation in the Medicare or Medicaid programs.

Death Master File and National Plan and Provider Enumeration System Screening

The Centers for Medicaid and Medicare Services' ("CMS") regulations and the contractual provisions found in managed care organization provider agreements require screening of the System's workforce members, certain business partners, and agents to ensure that none of these individuals are using the social security number ("SSN") or National Provider Identifier ("NPI") number of a deceased person. This screening may be accomplished by vetting the SSNs and NPIs of such individuals through the Social Security Administration Death Master File ("DMF") and the National Plan and Provider Enumeration System ("NPPES"), respectively. There no providers identified.

Reported Privacy Incidents for the period of October 1, 2018 through November 30, 2018

During the period of October 1, 2018 through November 30, 2018, thirteen privacy incidents were entered into the RADAR Incident Tracking System. Of the thirteen (13) incidents, four (4) were found after investigation to be violations of NYC Health + Hospitals HIPAA Privacy and Security Operating Procedures ("OPs"); two (2) were found not to be a violation of NYC Health + Hospitals HIPAA Privacy and Security Operating Procedures; and seven (7) are still under investigation. Of the four (4) incidents confirmed as violations, three (3) were determined to be breaches.

Reported Breaches for the Period of October 1, 2018 through November 30, 2018

NYC Health + Hospitals/ Jacobi – October 2018

Incident: On October 5, 2018, the OCC was notified of the incident, which occurred when NYC Health + Hospitals' vendor, CIOX, sent patient records, including information about the patient's medical history, diagnoses, medications, to the wrong courthouse. This incident occurred prior to CIOX's audit and Quality Assurance activities.

Breach Determination: Even though it is customary for the courthouse that received the misdirected records to transfer any such records to the correct courthouse, the courthouse that received the misdirected records could not confirm that the records were in fact received and appropriately transferred to the correct courthouse. The breach notice was sent on November 14, 2018. The records were subsequently sent to the appropriate requestor.

NYC Health + Hospitals/ North Central Bronx ("NCB") – October 2018

Incident: On October 2, 2018, the OCC was notified of an incident, which occurred on September 27, 2018, when a NCB care manager accessed the records of his friend/acquaintance. The care manager claimed that the patient requested his assistance, he accessed the records with the patient's consent, and the nature of his job as a care

manager would have allowed him to access the chart of any patient in that manner if the patient requested his assistance.

Breach Determination: It was determined after investigation that the employee was not working on the unit at the time of the incident, and did not have a legitimate business reason for accessing the patient's chart. The employee had a Step 1A disciplinary hearing before Labor Relations, which remanded the case to the department to issue a written warning, which was placed in the employee's personnel file.

NYC Health + Hospitals/Bellevue ("Bellevue") – October 2018

Incident: This incident was brought to our attention on October 11, 2018, and occurred when Patient Relations at Bellevue received a report from a patient stating that in 2017 he received medical records for another patient. After an investigation into the incident, it was determined that the patient had requested the records in 2015, that the envelope containing the records was not opened until 2017, and not reported until October 2018. It appears that the incorrect release of records occurred due to the similarity in last names.

Breach Determination: Of the four key factors described above, the nature and extent of the PHI involved, and the inability to completely mitigate the risk to the PHI contributed to the determination that there existed a greater than low probability that the PHI had been compromised. Therefore, notification was sent to the affected individual on November 2, 2018. The OCC worked with the patient who reported the incorrect disclosure to ensure that the records had been destroyed appropriately and that no other individuals had viewed or obtained any information from the records.

Office of Civil Rights ("OCR") Inquiries Regarding Privacy Incidents

There was one inquiry initiated by the OCR between October 1, 2018 and November 30. 2018. The inquiry pertained to an incident which occurred at NYC Health + Hospitals/Elmhurst ("Elmhurst"). On November 5, 2018, the OCC was notified via a letter from the OCR (Transaction 18-306394) that an individual filed a complaint with the OCR stating that he/she had been receiving documents, including bills and behavioral health appointment reminders, addressed to a patient from Elmhurst. The complainant also noted that attempts with Elmhurst's Patient Relations and Billing Departments to correct the issue went unresolved. After investigation by the OCC, it was determined that the patient to whom the records belonged had presumably provided an incorrect address, which was changed immediately in Elmhurst's records. Attempts to reach the patient have thus far been unsuccessful.

CIOX Audit Results

As reported at the October 2018 Audit Committee meeting, one of our vendors, CIOX, which responds to medical records requests on the System's behalf, was responsible for ten (10) HIPAA breaches this year. Consequently, the Chief Corporate Compliance Officer ("CCO") had a conversation with CIOX's Chief Privacy Officer to discuss what CIOX is doing to avoid further breaches. She informed the CCO that CIOX was implementing the following corrective actions.

- Performing a 100% quality assurance check on records requested from Bellevue and Jacobi, from which the majority of the breaches came, to ensure that the correct documents are being sent to the correct requester;
- Conducting unannounced on-site audits of their workforce at Bellevue and Jacobi to determine whether they are following proper policies and procedures, and HIPAA requirements; and
- Developing an action plan based on the results of the audits to bring their workforce into compliance.

In addition, the Office of Supply Chain engaged a consulting group to review CIOX's services and determine whether there are opportunities for improvement or change. Currently, the facility Health Information Management ("HIM") Directors oversee CIOX's services; however, we are in the process of centralizing this function. In the meantime, the Office of Supply Chain has identified a temporary point person to act as a liaison between CIOX and the HIM Directors until this function transitions to finance.

The OCC is awaiting for the resulting of the Quality Assurance review. Among the findings of the audits were the following:

- Staff need retraining on multi-factor patient identification when multiple names and dates of birth occur;
- Bellevue is a high risk site for sensitive patient information, and many of CIOX's staff at Bellevue have limited experience, including the site supervisor and area supervisor;
- The site supervisor at Bellevue appears to be unqualified for the position, due to lack of available candidates with qualifying experience in management and health care; additional training is being provided and CIOX will perform additional Quality Assurance on his work and review it with him;
- There is a printing issue at Bellevue that results in portions of prior print jobs printing in the middle of a subsequent print job, causing two patients' information to be combined into one print job;
- CIOX needs to continue to monitor both sites for Quality Assurance and potentially conduct another site audit at Bellevue in 2019; and
- NYC Health + Hospitals' unauthorized disclosure concerns, unqualified supervisor, and lack of further management oversight allowing the HIM Director to direct workflow and quality presents numerous risks associated with CIOX policy and compliance with regulations.

In addition, the Office of Supply Chain has attempted to meet with the consulting group, CIOX, and the HIM Directors to discuss the consultant's findings; unfortunately, two scheduled meetings had to be cancelled due to conflicts. The next meeting is scheduled for December 19, 2018.

<u>Update on Policy for Securing Biomedical Devices</u>

As previously reported, there was a breach of PHI at Harlem that resulted from the theft of a laptop from the hospital's Audiology Department. During the discussion regarding this breach, the OCC reported that it would be working with Enterprise Information Technology Services ("EITS") to develop a policy and procedure for documenting and securing biomedical devices that enter the System and connect to the System's network, as well as devices that do not connect to the System's network.

Since the October 15, 2018 Audit Committee meeting, a group comprised of representatives from EITS, Supply Chain, Acute Care Operations, and the OCC met to discuss the development of a Biomedical Device Operating Procedure ("OP"). As a result, a Draft Biomedical Device OP was prepared by the OCC, and circulated to the group for review. Following final review of the Draft OP, it will be distributed to the appropriate departments for review and comment, before the final version is sent to the President for approval and signature. If approved, additional resources will be required to implement.

The next step in this process is to identify an enterprise-wide Biomedical Task Force, as described in the Biomedical Device OP. The Biomedical Device Task Force will be a multidisciplinary group with responsibility for:

- Oversight and monitoring of all biomedical device management processes, including the Biomedical Device OP; and
- Oversight and management of all biomedical devices, including on-boarding, inventory, and encryption.

In addition, EITS is working on revising a 2010 Device and Media Control Plan, which addresses the receipt, movement, and removal of devices and electronic media that contain electronic health information into, within, and out of NYC Health + Hospitals. The revisions should be completed by the end of this week.

Summary of Reports for the Period of October 1, 2018 through November 30, 2018

For the period October 1, 2018 through November 30, 2018, there were seventy-nice (79) compliance reports, none of which were classified as Priority "A," 7 twenty-one (21) (27%) were classified as Priority "B," and fifty-eight (58) (73%) were classified as Priority "C" reports. Most of them had to do with employees' relations and a lot of them had to do with disgruntled employees.

Audit of OneCity Health DSRIP Program by Outside Auditor

As previously reported, OneCity Health engaged a third-party auditor, Bonadio & Co., LLP ("Bonadio"), to audit OneCity Health's internal processes, including Partner selection and contracting, quarterly reporting, funds flow, and the Partner portal. Bonadio completed its audit of OneCity Health, and submitted its final audit report to the Board of Directors of OneCity Health on October 9, 2018. During a subsequent internal meeting with the Comptroller's office, Internal Audits, and the OCC, it was determined that modifications should be made to two of Bonadio's findings in its report. Bonadio's final report has not yet been submitted to the OneCity Health Board of Directors. It should be noted that, on December 5, 2018, the New York State Department of Health ("DOH") broadcast an email to other PPSs acknowledging OneCity Health for conducting this audit, which DOH considered a best practice, and advising other PPSs that they should consider doing the same.

Status Update - HHC ACO, Inc.

1) As previously reported, on October 5, 2017, HHC ACO, Inc. ("HHC ACO") submitted an application to the New York State Department of Health ("DOH") seeking approval for an "all payer" ACO, which includes Medicaid, commercial insurance, and Medicare Advantage patients. That application is still pending.
2) On August 9, 2018, the Centers for Medicare and Medicaid Services ("CMS") issued a proposed rule for CY2019 of the Medicare Shared Savings Program ("MSSP"), which sets forth a number of proposed changes to the MSSP, including changes that encourage ACOs to take on greater risk. The final rule is expected to be released later this year.
3) Recently, CMS announced that the ACOs may elect to extend their participation agreements for six months. CMS is permitting this extension to allow ACOs more time to implement two-sided risk arrangements. HHC ACO has therefore elected to extend its participation agreement with CMS through June 30, 2019.
4) HHC ACO expects to move into a two-sided risk contract beginning July 1, 2019, and expects to know more information after CMS issues the final MSSP regulation in 2019.

Aetna Desk Review

As previously reported, on January 31, 2018, the OCC received notification from Aetna of a Notice of Compliance Program Audit (the "Notice"), requesting information from NYC Health + Hospitals relating to its compliance with Medicare Parts C and D compliance program elements as required by CMS. The Notice stated that the review would

include functions performed by the System (particularly the OCC) which are related to Aetna's Medicare Advantage, Prescription Drug Plans and/or Medicare – Medicaid Plan product lines. Aetna performs such reviews to ensure that the entities it contracts with, such as the System, meet their compliance program obligations. These reviews are conducted under the auspices of their "Delegated Vendor Oversight" responsibilities, as required by CMS.

On April 30, 2018, the OCC received Aetna's Compliance Program Elements Audit Report (the "Audit Report"), which included Aetna's final conclusions regarding NYC Health + Hospitals' compliance with its audit. According to the Audit Report, NYC Health + Hospitals satisfied eight of the compliance requirements, but failed to satisfy four compliance requirements. The Audit Report also required NYC Health + Hospitals to submit corrective action plans to Aetna for the failed compliance requirements, which the OCC did on May 25, 2018.

On August 27, 2018, the OCC submitted NYC Health + Hospitals' report on the implementation of its corrective actions plans, most of which involved changes to Operating Procedures. On September 18, 2018, the OCC received an email from Aetna requesting additional information in response to one of the System's corrective action plans, which the OCC provided on September 20, 2018.

On November 15, 2018, the OCC received an email from Aetna regarding its further review of the System's corrective action plans, stating that the System needs to revise its policies to meet a record retention requirement that the OCC believes does not apply to the System. The OCC is conferring with the Office of Legal Affairs regarding the System's obligation to comply with this requirement.

FY2018 Corporate Risk Assessment & FY2019 Corporate Compliance Work Plan

The Risk Assessment Process

The OCC identified various risks to the System, broken down by service line (*e.g*. acute care, post-acute care, etc.) and System-wide. These risks were presented to the Executive Compliance Workgroup ("ECW") in a Draft Risk Assessment on June 8, 2018, for review and potential revision and/or additions/deletions.

The risks described in the Draft Risk Assessment were derived from the OMIG's Work Plans, and the OIG's Work Plans and updates thereto, both of which identify risks that these agencies have determined to be areas of concern for overpayment and/or noncompliance. Other risks outlined in the Draft Risk Assessment were identified internally.

Following the ECW's review, the Draft Risk Assessment was presented to the Compliance Committees of the System's facilities, entities, and programs for their input and identification of additional risks pertinent to their facilities, units, entities, or programs. The Compliance Committees were asked to rank each of the relevant risks as high, medium or low.

The OCC then finalized the Risk Assessment and identified the impact, vulnerability, and current controls associated with the identified risks, and assigned a severity rating to each risk on a scale of 1 – 5, with 5 being the risks having the greatest impact. The OCC utilized a *Table of Risk Assessment Scoring Parameters,* adopted and derived, in pertinent part, from the Health Care Compliance Association, to score and prioritize the identified risks.

Once all the risks were prioritized, the OCC developed a Draft FY2019 Corporate Compliance Work Plan ("Draft FY2019 Work Plan"), which included the risks from the Risk Assessment with the highest risk prioritization scores in

each service line and System-wide. On September 10, 2018, the ECW met to review and discuss the draft FY2019 Work Plan. As a result, the ECW identified certain issues in the Draft FY2019 Work Plan for which follow-up was necessary.

On November 26, 2018, the ECW met to discuss the follow-up to the Draft FY2019 Work Plan, and to finalize the FY2019 Corporate Compliance Work Plan for submission to the System President and Chief Executive Officer and the Audit Committee for approval. The FY2019 Corporate Compliance Work Plan will be ready for submission to the President and to Audit Committee for approval on December 13, 2018.

Records Management

Current Situation

As previously reported, in May 2018, a Records Task Force was formed to address the issue of more than 621,000 boxes of paper-based files in off-site storage at Iron Mountain, at a monthly storage rate of more than $335,340, and annual storage rate of more than $4,024,080. The Records Task Force was comprised of the System's Corporate Records Management Officer ("RMO"), and representation from the OCC, the Office of Supply-Chain, the Office of Legal Affairs ("OLA") and EITS. The mandate for the Records Task Force was to deal with the immediate problem of the excessive storage at Iron Mountain, and to establish a plan for the future of records management for the System.

To date, 61,310 of the 621,000 boxes have been identified for destruction due to the age of boxes based on their in-take dates, and the type of records contained therein (*i.e*. non-clinical records excluding human resource records). The RMO will submit a request for destruction approval for these boxes to the System's senior leadership, explaining the analysis and the methodology used to determine the need for destruction, along with the costs associated with storing such boxes. Once approval is obtained, the RMO will work with Iron Mountain and the Office of Supply Chain to destroy these boxes.

In addition, 77,359 of the 621,000 boxes have an identified destruction date that was entered by a System workforce member. Destruction of these records will follow the standard destruction process outlined in OP 120-19, *Corporate Records Management Program and Guidelines for Corporate Record Retention and Disposal.* We are on track to order destruction of the majority of these boxes within the next couple of months.

In total, therefore, there are approximately 138,700 boxes that can be slated for destruction, which would save the System approximately $74,898 monthly, and approximately $898,776 annually.

Ms. Arteaga Landaverde asked if the 138,700 boxes slated for destruction are part of the annual destruction.

Ms. Patsos answered no that these boxes have been there for a long time. If these boxes are non-clinical records and non-HR records, they can be destroyed.

Dr. Katz commented that ideally if they all could be destroyed, because of the value of keeping unindexed boxes is very low. If they are all destroyed, there will not be any HIPAA issues. If someone requests a record and does not return it, then it becomes an issue. If they are not going to be destroyed, why we are renting space, we have lots of space. Maintaining records only requires a secured locked place.

Ms. Patsos stated that it has come up, but aside from the secured place, it needs the proper environment for the records.

Dr. Katz asked at what point we can have these records digitized.

Next Steps & Future State of Records

After a series of meetings with Iron Mountain, the RMO, in conjunction with the Office of Supply Chain, was able to put in place the following immediate steps to curb the mounting storage at Iron Mountain:

- No additional boxes will be sent to Iron Mountain.
- Restrict individual facility records management activities, including sending boxes off-site, to one or two Facility Records Officers per site, who will work with the RMO. Note that a total of over 600 NYC Health + Hospitals workforce members have been interacting with Iron Mountain regularly, often sending boxes off-site with no labelling and no retention dates.
- With the help of the Facility Records Officers, begin identifying records at Iron Mountain that have no retention requirements and/or are past their retention period.

In early September, the RMO along with the Office of Supply Chain met with EITS to plan for digitization of records. In subsequent meetings, EITS presented the software solution OnBase to the Records Task Force, which can be used as an enterprise content management system ("ECM"). Among other things, an ECM provides functionality such as indexing and labelling of digitized records, recording meta-data pertaining to the records, and manual or auto-purging of records past their retention period.

On November 15, 2018, the RMO presented to the EITS Intake Meeting NYC Health + Hospitals' records digitization initiative as the System's future state for records retention strategy. At the meeting, the EITS project management committee voted to advance the digitization initiative to the Health Information Technology ("HIT") Committee, and assigned a project manager to the initiative. If the digitization initiative is accepted and voted upon as a "high priority" project at the upcoming HIT Committee meeting, the initiative will become an "IT Project" which will be tracked and assigned technology resources.

Ms. Patsos added that we would like to scan all of the boxes and we are evaluating the cost.

Dr. Katz stated that it's an expensive solution relative to moving it out of storage and putting it on one of our hospitals' locked spaces. Going forward it makes sense, but going backwards, it makes no sense giving our clinical priorities.

Mr. Campbell asked Mr. Lynch going forward, how would they be stored digitally?

Mr. Lynch answered that it is still to be determined.

Updates to NYC Health + Hospitals' Compliance and HIPAA Training

Over the last year, the OCC has made significant revisions and updates to how the System provides Compliance and HIPAA training and education to its workforce members. The revisions and updates were designed to enhance and ease the training and education process, while simultaneously meeting regulatory requirements in a more efficient

and expeditious manner. The following is a brief summary of the OCC's efforts to enhance the training and education process:

- Combined previously separate annual courses (*i.e.* Compliance and HIPAA) into one Human Resources Annual Mandates training curriculum – making it easier for workforce members to meet regulatory requirements in one step;
- Developed a similar yet separate course for new workforce members, thus allowing a clear distinction of completed required orientation training, which is now maintained in their records;
- Developed "tracks" in both online courses which are more specific to the workforce member's role at NYC Health + Hospitals (*e.g.* physician track, non-clinical workforce member track, and volunteer/student track);
- Replaced previous in-person/live training with ELM training, which has allowed Compliance Officers to dedicate more time to other critical compliance activities;
- Worked with Human Resources Shared Services ("HRSS") and Workforce Development to produce a new online course for the purpose of remedial education of workforce members when a HIPAA incident and subsequent investigation warrants such. This online course, previously provided on paper, allows for better tracking, reporting and documenting of steps taken to mitigate future issues; and
- Worked with HRSS to offer, for the first time, in June and July 2018, a method of online training for the incoming class of resident physicians across the System. More than 1,800 residents were able to complete their training and education obligations prior to their start date, which lead to a faster and more seamless assignment of their clinical duties. This lead to a completion rate within the first week of on-boarding of close to 97%.

Mr. Campbell asked for a motion to hold an Executive Session to discuss potential legal implications, motion was made and seconded.

There being no other business, the meeting was adjourned at 1:04 P.M.

NYC HEALTH + HOSPITALS

OFFICE OF INTERNAL AUDITS

AUDIT COMMITTEE BRIEFING
APRIL 2019

Index

A. EXTERNAL AUDITS

1. *Compliance with Federal Tax Requirements – Internal Revenue Service*

Audit Notification Letter Received – August 30, 2018
Entrance Conference – October 30, 2018
Audit Status – On-going

After being on-hold during the government shutdown, this audit re-started on January 28, 2019. The objective of the audit is to ensure compliance with federal tax requirements as an exempt organization. During the entrance conference, the IRS requested the following documents:

a) Financial Assistance Plan (FAP) for each hospital facility – this document must apply to all emergency and other medically necessary care provided by the hospital facility and include:

- Eligibility criteria for financial assistance and whether such assistance includes free or discounted care.
- The basis for calculating amounts charged to patients.
- The method for applying financial assistance in the case of a hospital that does not have a separate billing and collection policy.
- The actions that may be taken in the event of nonpayment.
- The measures taken to widely publicize the FAP within the community served by the hospital.

b) Minutes from meetings describing the FAP during FY16, the billing and collection policy and actions taken in the event of nonpayment of fees.

c) Community Health Needs Assessment (CHNA) for FY16 - which is required to be conducted by each hospital facility once every three years in order to document the extent to which it understands the unique characteristics and needs of the local communities it serves, and responds to these means by delivering meaningful and effective benefit through clinical services.

The Financial Assistance Plan (FAP) for each hospital facility was provided to the IRS on November 1, 2018 by Revenue Management. Based on the FAP that was provided, a second 'Information Documentation Request' was submitted to the Office of Internal Audits (OIA) on December 3, 2018. Responses to the second Information Documentation Request was submitted by Revenue Management to OIA on December 20, 2018 and then forwarded to the IRS.

For the minutes from meetings describing the FAP, the IRS was advised in a written document from Revenue Management that the minutes are available on the NYC Health + Hospitals website (https://www.nychealthandhospitals.org/public-meetings-notices/).

The FY16 Community Health Needs Assessment (CHNA) reports were coordinated by the Office of Internal Audits and mailed to the IRS on December 3, 2018.

A copy of the Bad Debt policy was provided to the IRS on November 1, 2018. However, Revenue Management did not have a written Billing and Collection Policy as of that date. Responses to the second Information Documentation Request was received from Revenue Management on December 20, 2018.

On February 7, 2019 the written Billing and Collection Policy, which was updated for the current EPIC environment, was submitted to OIA and forwarded to the IRS the next day.

We are in continuous communication with the IRS. On March 12, 2019 we were advised that the review of the documentation submitted was not done because of the back log from the government shutdown. The status did not change as of March 26, 2019. The Auditor is hoping to start the review sometimes next week.

2. ***Children of Bellevue Auxiliary – NYC Comptroller's Office***

Audit Notification Letter Received – March 21, 2019
Preliminary Entrance Conference – April 4, 2019
Audit Status – Pending

The Audit Engagement Letter stated that the audit was of Children of Bellevue's (CoB) financial and operating practices.

The twenty-two Auxiliaries that exist within the various facilities of NYC Health + Hospitals are separate 501c3 not-for-profit corporations whose primary function is to enhance the quality of patient care. They do this by receiving and administering funds received from fund raising activities, gifts, and donations and distributing those funds for activities or projects which enhance the quality of patient care and for selected amenities not otherwise available to patients.

The audit objectives are to determine whether CoB:

- Has adequate controls over and accurately reports its revenues and expenses.
- Is complying with applicable rules, regulations, policies and procedures.
- Has computerized systems controls to ascertain the integrity, validity and reliability of its data.

It should be noted that the most recent audited financial statements of CoB, for Calendar Year 2017, shows Cash and Investments totaling over $1.25 million.

B. OTHER AUDIT ACTIVITIES

1. Report Received from the Office of Inspector General

A report was received from the Office of Inspector General (IG) regarding their review of the Inventory Controls within the Facilities Management Department at NYC Health + Hospitals/ Queens. The report noted the following findings:

1. There were no policies or practices for maintaining inventory control.
2. Work Orders were completed without the cost of materials indicated.
3. Annual inventory counts were not conducted.
4. Valuable power tools were not tagged and their usage was not monitored.
5. The area in which the inventory was held lacked cameras, Hospital Police presence or other security measures.

Discussions were held with the CEO from Queens, the Corporate Vice President of Facilities and other interested parties regarding the report. It was determined that the deficiencies found by the IG existed at the other facilities in the System. Hence, the responses to the findings would be at the System-wide level instead of from one facility.

The responses first addressed an incorrect comment made within the report. The IG stated that there was approximately $1.6 million in inventory purchased in fiscal years 2017 and 2018. However, their totals included various maintenance contracts (i.e. elevators) and service repair contracts. It was found that only $287,000 was spent for inventory in FY18 and a comparable amount was spent for 2017.

The other responses were as follows:

- Procedures will be developed once inventory controls, such as a baseline and par levels, are established.
- NYC Health + Hospitals will work toward achieving the recommendations to include the material cost option for all work orders and requiring supervisory approval before closing them. Resources need to be identified to ensure adherence before this is implemented.
- NYC H+H is working towards a computerized inventory system that parallels the current system used for medical supplies. Annual inventories can then be performed in a digital fashion with increased accuracy.
- A review will begin regarding a scanning program for expensive tools used by trades' personnel. A policy will be written requiring a reporting of missing tools.
- Cameras and card swipes will be installed at NYC Health + Hospitals/Queens within the next six months in all areas that are designated for storage and/or equipment.

2. Anonymous Letters

Since the last Committee meeting, the Office of Internal Audits was forwarded two anonymous letters received by the President's Office. The first letter included complaints about the management within the Medical Records Department at NYC Health + Hospitals/Kings. Further inquiry revealed that this was not the first letter received regarding this matter. As a result, the IG had already begun an investigation; OIA would then defer to them to avoid duplication of efforts.

The second letter involved the purchasing habits of the Facilities Manager at NYC Health + Hospitals/Gouverneur. Discussions were held with Corporate Facilities Management to obtain some background information. An evaluation of the purchasing history within this department is currently underway. This investigation is on-going.

AUDIT COMMITTEE OF THE NYC HEALTH + HOSPITALS BOARD OF DIRECTORS

Audit Committee Meeting

Corporate Compliance Report

April 9, 2019

AUDIT COMMITTEE OF THE
NYC HEALTH + HOSPITALS
BOARD OF DIRECTORS
Corporate Compliance Report
125 Worth Street, Room 532
New York, NY 10013
April 9, 2019 @ 11:00 AM

TABLE OF CONTENTS

AUDIT COMMITTEE OF THE
NYC HEALTH + HOSPITALS
BOARD OF DIRECTORS
Corporate Compliance Report
125 Worth Street, Room 532
New York, NY 10013
April 9, 2019 @ 11:00 AM

I. Monitoring Excluded Providers

Responsibilities of the System for Sanction List Screening

1) To comply with Federal and state regulations, and consistent with the recommendations of the NYS Office of the Medicaid Inspector General ("OMIG")[1] and the U.S. Department of Health and Human Services Office of Inspector General ("OIG"), each month the Office of Corporate Compliance ("OCC") reviews the exclusion status of the System's workforce members, vendors, and New York State Department of Health ("DOH") Delivery System Reform Incentive Payment ("DSRIP") program Partners.

2) To ensure that NYC Health + Hospitals (the "System") 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 + Hospitals workforce members, vendors and DSRIP Partners against the databases of the United States Department of Treasury Office of Foreign Asset Control ("OFAC").[2]

Exclusion and Sanction Screening Report February 1, 2019 through March 31, 2019

3) During the period of February 1, 2019 through March 31, 2019, there was one disciplined individual and one sanctioned vendor identified.

4) On February 28, 2019, the OCC was notified by its vendor that a registered nurse within NYC Health + Hospitals/At Home had a two-month actual suspension, twenty-two-month stayed suspension, and twenty-four-month probation on her license. The OCC is looking into whether there could be an overpayment related to her suspensions and probation. On March 22, 2019, however, she was terminated due to inappropriate behavior and interactions with shelter administrators.

5) On March 13, 2019, the OCC was informed that a vendor possessed a sanction through the Environmental Protection Agency due to a violation of the Clear Water

[1] *See* DOH Medicaid Update, April 2010, Vol.26, No. 6; OMIG webinar #22, OMIG Exclusion and Reinstatement Process, available at https://omig.ny.gov/resources/webinars/811-omig-webinar-22, (Slide 20 (Sept. 2014)).
[2] *See* Frequently Asked Questions: Who must comply with OFAC regulations? United States Treasury website available at, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx.

Act. The OCC is in the process of determining whether this sanction would cause an overpayment issue.

Death Master File and National Plan and Provider Enumeration System Screening

6) The Centers for Medicaid and Medicare Services' ("CMS") regulations[3] and the contractual provisions found in managed care organization provider agreements[4] require screening of the System's workforce members, certain business partners, and agents to ensure that none of these individuals are using the social security number ("SSN") or National Provider Identifier ("NPI") number of a deceased person. This screening may be accomplished by vetting the SSNs and NPIs of such individuals through the Social Security Administration Death Master File ("DMF") and the National Plan and Provider Enumeration System ("NPPES"), respectively.

7) No providers were identified on the DMF or NPPES during the period February 1, 2019 through March 31, 2019.

II. Privacy Incidents and Related Reports

Breach Defined

8) A breach is an impermissible use, access, acquisition or disclosure (collectively referred to as "use and/or disclosure") under the Health Insurance Portability and Accountability Act ("HIPAA") of 1996 Privacy Rule that compromises the security and privacy of protected health information ("PHI") maintained by the System or one of its business associates.[5]

9) Pursuant to 45 CFR § 164.402(2), unless an exception applies, the unauthorized use and/or disclosure of PHI is presumed to be a breach unless the System can

[3] *See* 42 CFR § 455.436; *see also*, CMS' Toolkit to Address Frequent Findings 42 CFR § 455.436 Federal Database Checks, available at https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/FraudAbuseforProfs/Downloads/fftoolkit-federal-database-checks.pdf.
[4] *See* 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, ("Provider … 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)").
[5] *See* 45 CFR § 164.402.

demonstrate, through a thorough, good faith risk assessment of key risk factors, that there is a low probability that the PHI has been compromised.[6]

Reported Breaches for the Period of February 1, 2019 through March 31, 2019

10) During the period of February 1, 2019 through March 31, 2019, sixteen (16) incidents were entered in the RADAR Incident Tracking System. Of the sixteen (16) incidents, nine (9) were found after investigation to be violations of NYC Health + Hospitals' HIPAA Privacy and Security Operating Procedures; six (6) were found not to be a violation of NYC Health + Hospitals' HIPAA Privacy and Security Operating Procedures; and one (1) is still under investigation.

11) Of the nine (9) incidents confirmed as violations, none were determined to be a HIPAA breach.

Update on Incidents Previously Under Investigation:

12) Two (2) previously discovered incidents that had been under investigation, were found to be breaches.

- **NYC Health + Hospitals/McKinney ("McKinney") – November 2018**

Incident: On November 30, 2018, the OCC was informed by the Deputy Inspector General of NYC Health + Hospitals Office of the Inspector General ("IG") that the PHI of 260 McKinney residents was mistakenly released by NYC Health + Hospitals to two potential vendors of NYC Health + Hospitals. The information was inadvertently released in September 2016 by Post-Acute Care leadership to Omni Care Inc. and Pharm Script, LLC to calculate potential savings that could result from outsourcing NYC Health + Hospitals' post-acute pharmacy services. The PHI that was released included patients' names, insurance, and medications.

Breach Determination: Although the information disclosed was limited in nature, the inability to mitigate the risk to the PHI and the length of time since the occurrence contributed to the determination that there existed a greater than low

[6] *See* 45 CFR § 164.402(2); *see also* 78 Fed. Reg. 5565, 5643 & 5695 (Jan. 25, 2013).

probability that the PHI may have been compromised. Therefore, the OCC sent breach notifications to the affected individuals.

Mitigation: The OCC reviewed this incident with the Post-Acute Care leadership, and reminded them of the need to safeguard PHI.

- **NYC Health + Hospitals/Lincoln ("Lincoln") – November 2018**

Incident: This incident occurred on November 2, 2018, when a social worker at Lincoln mistakenly faxed referral documents containing PHI to the wrong home care agency. The PHI disclosed included the patient's name, date of birth, home address, medical history, complaints, diagnoses, treatment, and insurance information.

Breach Determination: Even though the entity that received the PHI is a home care agency, and is therefore required to protect the privacy of any PHI it receives, the agency would not give the OCC written assurance that the PHI had been properly disposed of and had not been used or further disclosed for any purpose. The OCC, therefore, determined that there was more than a low probability that the security of the information had been compromised, and sent a breach notification to the affected individual.

Mitigation: In response to this incident, the social worker involved was counseled and reeducated on HIPAA privacy requirements, and a refresher training was provided to the entire Lincoln Social Work Department.

Office for Civil Rights ("OCR") Inquiries Regarding Privacy Incidents

13) There were no inquiries initiated by the OCR during the period February 1, 2019 through March 31, 2019.

14) Although there were no such inquiries, on February 22, 2019, the OCR met with OCC and Enterprise Information Technology Services ("EITS") leadership, along with in house and outside counsel, to discuss NYC Health + Hospitals' compliance with HIPAA, including the System's safeguards of its ePHI. During this meeting, the OCC and EITS explained to the OCR that the System has many controls in place to safeguard its ePHI, in compliance with HIPAA requirements. The OCR requested that the System document such current controls, as well as additional

planned controls, in a letter to the OCR. The OCC submitted such letter to the OCR on March 4, 2019, with follow-up documentation on March 18, 2019. The OCC will continue providing the OCR with additional documentation of its compliance with HIPAA as outlined in the letter.

III. Compliance Reports

Summary of Reports for the Period of February 1, 2019 through March 31, 2019

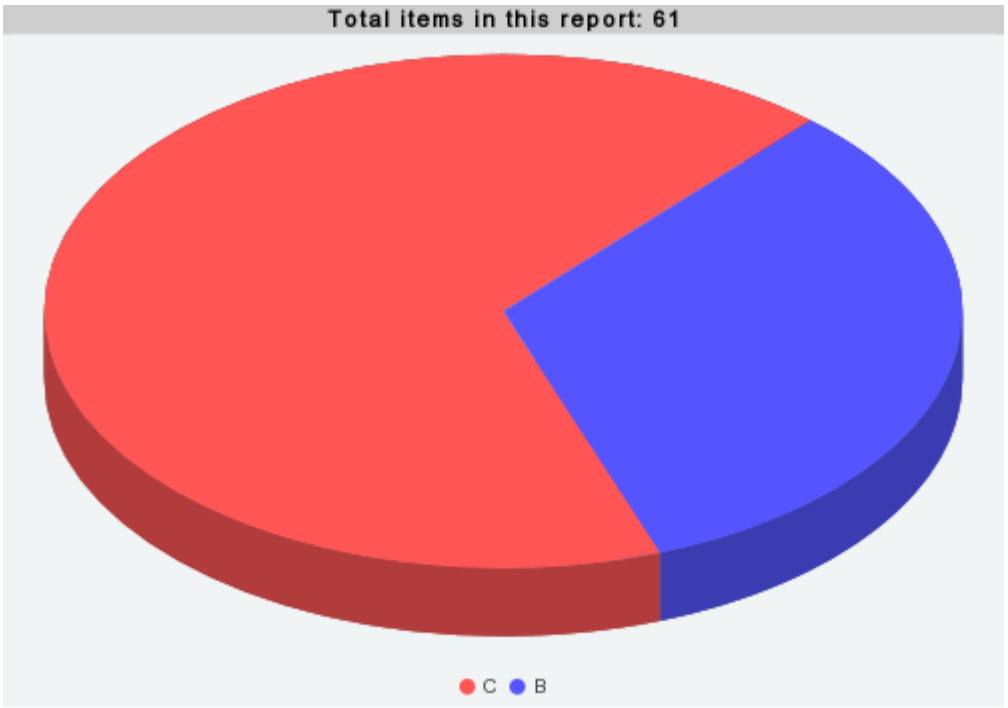
15) For the period February 1, 2019 through March 31, 2019, there were sixty-one (61) compliance reports, none of which were classified as Priority "A," [7] twenty (20) (33%) were classified as Priority "B," and forty-one (41) (67%) were classified as Priority "C" reports. For purposes here, the term "reports" means compliance-based inquiries and compliance-based complaints.

16) On March 18, 2019, the Director of Human Resources at NYC Health + Hospitals/Coney ("Coney") forwarded an email to the OCC which contained a statement from a physician assistant in Occupational Health Service ("OHS") that a laboratory employee from Coney was seen in OHS for her annual health assessment in November 2018. During that assessment, the employee asked the physician assistant to order additional blood work pertaining to iron deficiency; however, the physician assistant advised the employee that this was not permissible. According to the physician assistant, on February 13, 2019, she received laboratory work results for six tests that the employee had previously requested. The physician assistant reported that the employee had admitted that she ordered the tests on herself and that "everybody does that." An investigation of this matter is underway, and NYC Health + Hospitals laboratory leadership is aware of and will assist with the investigation. In the meantime, the Medical Director of the laboratory has begun retraining staff on who is permitted to order tests.

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

a. PRIORITY CLASSIFICATION

PRIORITY - CHART DATA	
	Frequency (Percentage)
B	20.0 (32.8 %)
C	41.0 (67.2 %)
Totals	61.0 (100%)



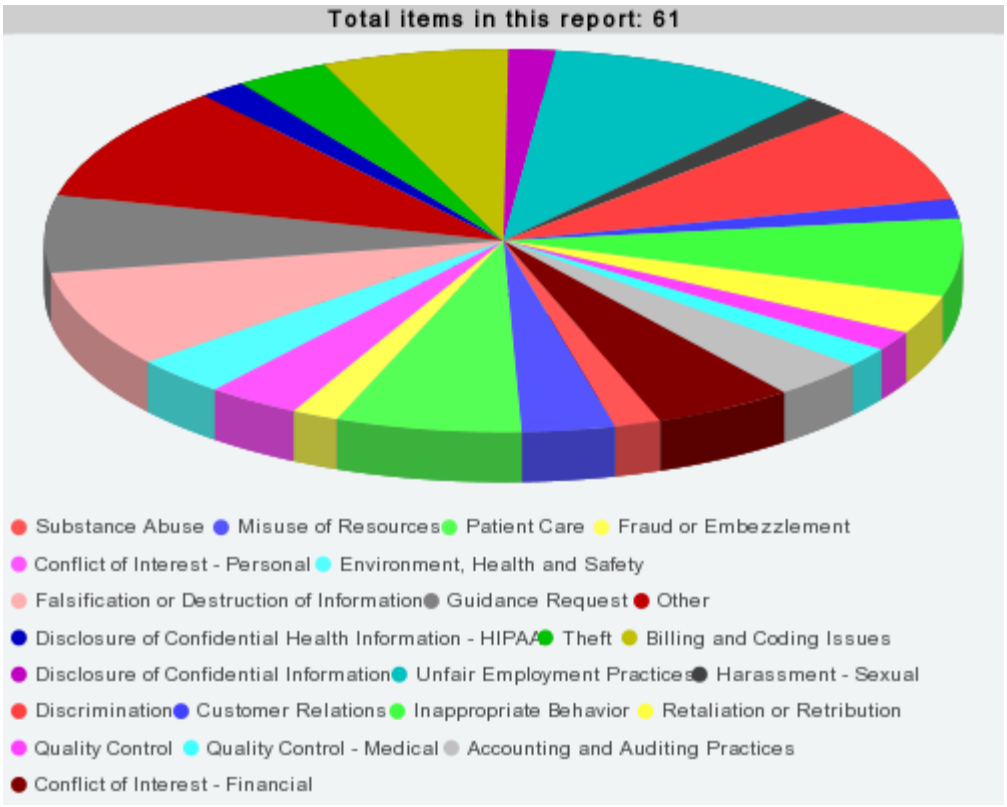
b. PRIMARY ALLEGATION CLASS

PRIMARY ALLEGATION CLASS - CHART DATA	
	Frequency (Percentage)
Diversity, Equal Opportunity and Respect in the Workplace	8.0 (13.1 %)
Employee Relations	12.0 (19.7 %)
Environmental, Health and Safety	3.0 (4.9 %)
Financial Concerns	5.0 (8.2 %)
Misuse or Misappropriation of Assets or Information	8.0 (13.1 %)
Other	10.0 (16.4 %)
Policy and Process Integrity	15.0 (24.6 %)
Totals	61.0 (100%)

c. PRIMARY ALLEGATION TYPE

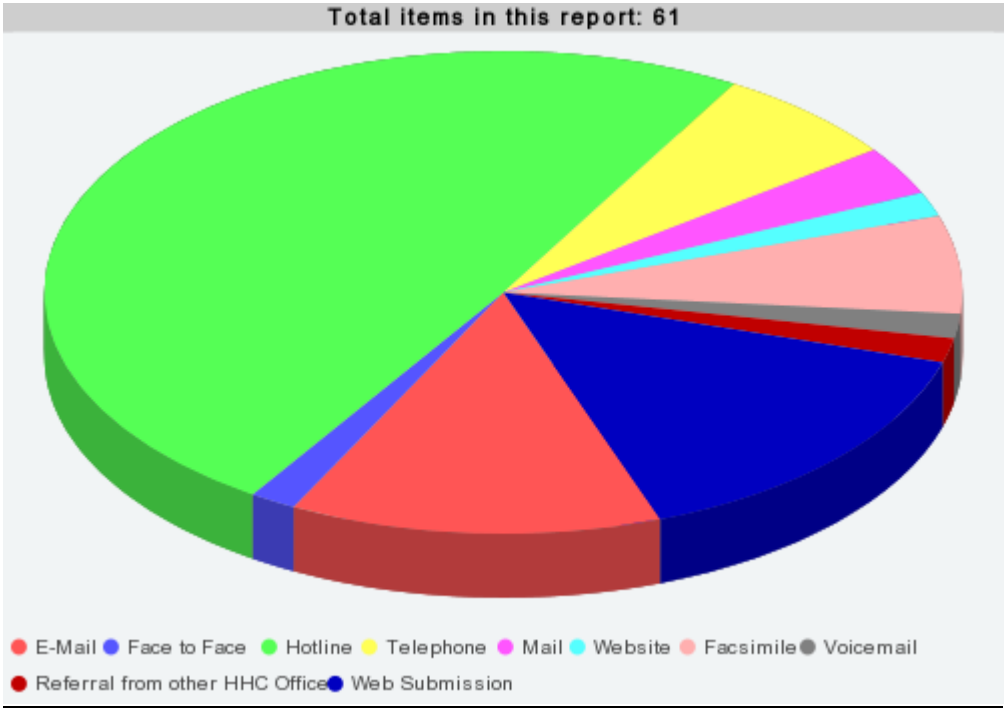
PRIMARY ALLEGATION TYPE - CHART DATA	
	Frequency (Percentage)
Accounting and Auditing Practices	2.0 (3.3 %)
Billing and Coding Issues	4.0 (6.6 %)
Conflict of Interest - Financial	3.0 (4.9 %)
Conflict of Interest - Personal	2.0 (3.3 %)
Customer Relations	1.0 (1.6 %)
Disclosure of Confidential Health Information - HIPAA	1.0 (1.6 %)
Disclosure of Confidential Information	1.0 (1.6 %)
Discrimination	5.0 (8.2 %)
Environment, Health and Safety	2.0 (3.3 %)
Falsification or Destruction of Information	5.0 (8.2 %)
Fraud or Embezzlement	1.0 (1.6 %)
Guidance Request	4.0 (6.6 %)
Harassment - Sexual	1.0 (1.6 %)
Inappropriate Behavior	4.0 (6.6 %)
Misuse of Resources	2.0 (3.3 %)
Other	6.0 (9.8 %)
Patient Care	4.0 (6.6 %)
Quality Control	1.0 (1.6 %)
Quality Control - Medical	1.0 (1.6 %)
Retaliation or Retribution	2.0 (3.3 %)
Substance Abuse	1.0 (1.6 %)
Theft	2.0 (3.3 %)
Unfair Employment Practices	6.0 (9.8 %)
Totals	61.0 (100%)

AUDIT COMMITTEE OF THE
NYC HEALTH + HOSPITALS
BOARD OF DIRECTORS
Corporate Compliance Report
125 Worth Street, Room 532
New York, NY 10013
April 9, 2019 @ 11:00 AM



d. PRIMARY ALLEGATION SOURCES

SOURCE - CHART DATA	
	Frequency (Percentage)
E-Mail	8.0 (13.1 %)
Face to Face	1.0 (1.6 %)
Facsimile	4.0 (6.6 %)
Hotline	30.0 (49.2 %)
Mail	2.0 (3.3 %)
Referral from other HHC Office	1.0 (1.6 %)
Telephone	4.0 (6.6 %)
Voicemail	1.0 (1.6 %)
Web Submission	9.0 (14.8 %)
Website	1.0 (1.6 %)
Totals	61.0 (100%)



IV. Status Update – OneCity Health

NYS Department of Health's Approval of OneCity Health's Attestation Form

17) The New York State Department of Health ("DOH") Security and Privacy Bureau ("Bureau") conducted a review of NYC Health + Hospitals/OneCity Health's ("OneCity Health") Performing Provider System ("PPS'") System Security Plan Controls Attestation Form for OneCity Health's internally hosted environment, and, on March 6, 2019, determined that it met the Bureau's criteria. As a result, OneCity will be able to derive and share insight from sensitive DOH data with its Partners to support better outcomes for NYC Health + Hospitals and other OneCity Health Partners' patients. This includes individual patient lists prioritizing care gaps to close, and summary analyses highlighting programmatic opportunities.

OneCity Health's Partner Compliance Attestation

18) OneCity Health, as a PPS Lead in the DSRIP Program, it 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."[8] To satisfy its compliance obligations, and to fulfill the requirements of the OMIG DSRIP compliance guidance, OneCity Health developed a compliance Attestation form, which is designed to assess its Partners' compliance with the program requirements.

19) OneCity Health Partners must certify annually to OneCity Health that they have met their DSRIP compliance training obligations and certain other compliance-related obligations. Accordingly, last week, OneCity Health distributed a Memorandum from the OCC to OneCity Health Partners with a link to a *Compliance Attestation of OneCity Health Partners* ("Attestation"). The Attestation, which provides OneCity Health and the OCC with a critical snapshot of the compliance foundation of its DSRIP Partners, must be completed by all

[8] 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.

OneCity Health Partners and returned to the OCC by close of business April 30, 2019.

V. Status Update - HHC ACO, Inc.

20) HHC ACO, Inc. ("HHC ACO") is in the process of submitting its application to renew its contract with CMS for the 2019-2024 agreement period. HHC ACO is applying to participate in the Enhanced track of the Medicare Shared Savings Program ("MSSP"), beginning July 1, 2019. The Enhanced track is a two-sided track, which will involve shared savings as well as potential shared losses. The shared savings could be as much as 75% of the savings to the Medicare program, adjusted by HHC ACO's quality score, and capped at 20% of total benchmark expenditure. Although the Enhanced track provides for the most allowed shared savings, it also carries the most risk – amounting to 40% to 75% of the losses to the Medicare program. The losses, however, are also adjusted by HHC ACO's quality scores, and capped at 15% of the total benchmark expenditure imposed by CMS. The final submission date for the round of requested documentation to CMS for this agreement is May 2, 2019.

VI. HIPAA Risk Analysis and Security Assessment

21) To ensure the System's compliance with the requirements of HIPAA and HIPAA regulations, the System had previously engaged a third party vendor to conduct HIPAA Risk Analyses and Security Assessments. The previous vendor's contract ended in August 2018, after which the OCC and the Information Security Risk Management ("ISRM") team of EITS issued a Request for Proposals ("RFP") to solicit proposals from vendors for the next round of HIPAA Risk Analyses and Security Assessments.

22) The Evaluation Committee for the RFP, which was comprised of individuals from the OCC and ISRM, received proposals from ten vendors, and selected four of them to provide presentations on their proposals. Of those four vendors, Coalfire Systems, Inc. ("Coalfire") received the highest score from the Evaluation Committee by a large margin, and its proposal was the one most closely aligned with the objectives of the RFP.

23) Coalfire's initial cost proposal for a three-year contract was more than $7 million above the RFP budgeted expense; however, following negotiations with Coalfire, they were able to provide the OCC and ISRM leadership with five proposed options at significantly reduced expense. Of the five options, the one that most closely aligns with the objectives of the RFP, and produces the minimal amount of risk of non-compliance with HIPAA requirements, is approximately $900,000 more that the budgeted expense for the three-year contract.

24) The OCC, therefore, outlined the budget difference to the System's Chief Information Officer ("CIO") and the rationale for choosing Coalfire over the next highest scoring vendor, and requested additional funding from EITS to cover the difference. Such funding was granted.

25) The Evaluation Committee therefore chose Coalfire to conduct the System's HIPAA Risk Analyses and Security Assessments for the next three calendar years. Coalfire held a two-day kick-off meeting with members of the OCC and ISRM in March, and work is underway for the 2019 Risk Analysis and Security Assessment.

VII. Aetna Desk Review

26) As previously reported, on January 31, 2018, the OCC received notification from Aetna of a Notice of Compliance Program Audit (the "Notice"), requesting information from NYC Health + Hospitals relating to its compliance with Medicare Parts C and D compliance program elements as required by CMS. The Notice stated that the review would include functions performed by the System (particularly the OCC) which are related to Aetna's Medicare Advantage, Prescription Drug Plans and/or Medicare – Medicaid Plan product lines. Aetna performs such reviews to ensure that the entities it contracts with, such as the System, meet their compliance program obligations. These reviews are conducted under the auspices of their "Delegated Vendor Oversight" responsibilities, as required by CMS.

27) On April 30, 2018, the OCC received Aetna's Compliance Program Elements Audit Report (the "Audit Report"), which included Aetna's final conclusions regarding NYC Health + Hospitals' compliance with its audit. According to the Audit Report, NYC Health + Hospitals satisfied eight of the compliance requirements, but failed

to satisfy four compliance requirements. The Audit Report also required NYC Health + Hospitals to submit corrective action plans to Aetna for the failed compliance requirements, which the OCC did on May 25, 2018.

28) On August 27, 2018, the OCC submitted NYC Health + Hospitals' report on the implementation of its corrective actions plans, most of which involved changes to Operating Procedures. On September 18, 2018, the OCC received an email from Aetna requesting additional information in response to one of the System's corrective action plans, which the OCC provided on September 20, 2018.

29) On November 15, 2018, the OCC received an email from Aetna regarding its further review of the System's corrective action plans, stating that the System needs to revise its policies to meet a record retention requirement that the OCC believes does not apply to the System. The OCC conferred with the Office of Legal Affairs regarding the System's obligation to comply with this requirement, and responded that it continued to maintain its position that such requirement does not apply to NYC Health + Hospitals.

30) On January 31, 2019, the OCC received another email from Aetna requesting that the OCC provide documentation to demonstrate the System's adherence to the CMS requirement related to retaining existing employee training records for a 10-year period. In addition, Aetna provided a random selection of five System employees with hire dates of 2009 and prior, which were identified from the System's original employee universe. Aetna requested that the OCC provide evidence demonstrating completion of these employees' Code of Conduct and Compliance training within the past ten years, by February 15, 2019. The OCC provided information to Aetna on February 15, 2019, and is waiting for their response.