KPMG
cutting through complexity

Commonwealth Health Insurance Connector Authority

Performance Audit of Centers for Medicare and Medicaid Services (CMS) Rule 9957 Requirements

For the Year Ended December 31, 2014

May 28, 2015

KPMG LLP
Two Financial Center
60 South Street

Contents

KPMG LLP
Two Financial Center
60 South Street
Boston, MA 02111

May 28, 2015

Louis Gutierrez
Executive Director
Commonwealth Health Insurance Connector Authority
100 City Hall Plaza
Boston, Massachusetts 02108

Dear Mr. Gutierrez:

This report presents the results of KPMG LLP's (KPMG) work conducted to address the performance audit objectives of Work Order 2014-02, related to the Commonwealth Health Insurance Connector Authority's ("the Authority," "the Connector" or "CCA") compliance with CMS Rule 9957 (45 C.F.R. §155) requirements. We conducted our testwork during the period February 3, 2015 through May 28, 2015 and our results, reported herein, are as of the calendar year ended December 31, 2014.

We conducted this performance audit in accordance with Government Auditing Standards (GAS) issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our Findings, Observations and Recommendations based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our Findings, Observations and Recommendations based on our audit objectives.

We have evaluated GAS independence standards for performance audits and affirm that we are independent of CCA and the relevant subject matter to perform this engagement.

Attached to this letter is our report detailing the background, objective, scope, approach, findings, recommendations and limitations as they relate to the performance audit.

Our fieldwork and testing were subject to overall limitations due to inability to access documents and data from the initial Health Information Exchange (HIX) system and documents and data relating to successor HIX system controls. These limitations applied to select control areas and individual controls over Eligibility, Enrollment, Financial Processing and IT Privacy and Security functions.

Based upon the audit procedures performed and the results obtained, we have met our audit objectives. Due to the exceptions noted in detail in this report, we documented findings which could increase CCA's risks of ineffective oversight and program integrity practices.

This audit did not constitute an audit of financial statements in accordance with Government Auditing Standards or U.S. Generally Accepted Auditing Standards. KPMG was not engaged to, and did not, render an opinion on the Authority's internal controls over financial reporting or over financial management systems.

Mr. Louis Gutierrez
Executive Director
Commonwealth Health Insurance Connector Authority
May 28, 2015

This report is intended solely for the information and use of the Authority and CMS, and is not intended to be, and should not be, used by anyone other than these specified parties.

Sincerely,

KPMG LLP

Executive Summary

Executive Summary

Over the next several pages of the Executive Summary, we provide you with the background, objective, scope, approach, and summary of results as it relates to the performance audit. The remainder of this document details the audit methodology as well as the Findings, Observations, and Recommendations that resulted from our test work.

Background

The Patient Protection and Affordable Care Act (ACA) was enacted by the U.S. Congress on October 23, 2010 and established the framework for the operation of health insurance exchanges. Specific regulations were further detailed in the Centers for Medicare and Medicaid Services (CMS) Final Rule 9957, published July 19, 2013 and incorporated into 45 C.F.R. §155. In accordance with general program integrity and oversight requirements, 45 C.F.R. §155.1200 requires entities operating as state-based marketplaces (SBM) to engage an independent qualifying auditing entity which follows generally accepted governmental auditing standards (GAGAS) to perform an annual independent external programmatic audit. The SBM must ensure that the programmatic audit addresses compliance with Rule 9957 generally and specifically with program integrity and oversight requirements; processes and procedures designed to prevent improper eligibility determinations and enrollment transactions; and identification of errors that have resulted in incorrect eligibility determinations. The SBM is required to provide the results of the audit to CMS and publish a public summary of the results.

CCA was created in 2006 pursuant to Massachusetts General Laws (MGL) Chapter 176Q and is an independent public authority responsible for facilitating the availability, choice and adoption of private health insurance plans to eligible individuals and groups. With major ACA provisions going into effect as of January 1, 2014, CCA was designated as the SBM for Massachusetts. CCA administers ACA programs for Qualified Health Plans (QHPs) and Qualified Dental Plans (QDPs) for eligible individuals, performs eligibility determinations for federal and state subsidies and cost-sharing reductions, administers a Small Business Health Options Program (SHOP) program for small businesses, and a Navigator program providing grants to community organizations that assist individuals and small businesses with enrollment.

CCA personnel perform various business administration, program oversight and support functions (e.g., finance, legal, communications, public policy and outreach, plan management, operations and information technology, member appeals). CCA contracts a significant amount of its operations to private vendors (e.g., customer service and call center operations, select financial processing activities, some IT development and maintenance) and relies on other public agencies and their private vendors to provide other key services relating to core IT systems.

CCA experienced significant IT challenges during its development and rollout of its initial Health Information Exchange (HIX) system in October 2013. As a result of CCA-identified operational issues with the initial HIX system and CCA's customer-facing website, CCA suspended member transition and enrollment into subsidized QHP coverage and obtained CMS approval to place individuals into temporary Medicaid coverage through the end of calendar year 2014. CCA developed manual workaround procedures to perform various processes and controls as a result of deficiencies within the initial HIX system. In 2014, development of a successor HIX system began with an initial rollout during November 2014 for the 2015 plan year.

Executive Summary (continued)

Objective

The objective of this audit was to assess CCA's compliance with 45 C.F.R. § 155 regulations for the calendar year ended December 31, 2014.

KPMG was responsible for performing the programmatic audit in accordance with Government Auditing Standards and preparing a written report communicating the results of the audit, including relevant observations and recommendations. These results include deficiencies in internal controls that are significant within the context of the objectives of the audit, any identified instances of fraud or potential illegal acts (unless they are inconsequential within the context of the audit objectives), significant violations of provisions of contracts and grant agreements, and significant abuse that was identified as a result of this engagement.

Scope

Program areas subject to review included processes and controls over:

- IT Privacy and Security
- Eligibility
- Enrollment
- Financial Processing
- General Exchange Functions, including:
  - Call Center
  - Governance and Oversight Functions
  - Data and Records Management
  - Qualified Health Plan Certification
  - Navigators and Assisters

Our audit procedures were limited in certain situations due to a variety of issues. These issues included, but were not limited to:

- Inability to access certain documents and data from the initial HIX system, which impacted select elements of our audit program for testing Eligibility, Enrollment and Financial Processing controls.
- Inability to access certain data sources for the successor HIX, which impacted our testing of IT Privacy and Security, Eligibility and Enrollment controls.

Approach

The audit was conducted in the following phases: Audit Planning, Information Gathering and Analysis, Audit Execution, and Reporting. Each phase is described below and in the following pages.

Audit Planning: Our audit planning included meeting with representatives of the CCA to begin the project, introduce the core team, validate our understanding and the overall scope of the audit, confirm functional areas to be included in the audit, and develop a tailored audit program.

Executive Summary (continued)

Information Gathering and Analysis: This phase included meeting with CCA process owners to initiate the audit, refine our understanding of CCA's activities, processes and controls during the audit period, obtain supporting documentation and conduct preliminary test work.

Audit Execution: This phase consisted of reviewing and testing specific procedures to assess CCA's compliance with regulatory criteria and design and operating effectiveness of supporting controls within the IT Privacy and Security, Eligibility, Enrollment, Financial Processing and General Exchange Functions.

Validation and Reporting: This phase consisted of validating the draft findings with CCA process owners, developing observations and recommended improvements, and discussing CCA's plans for corrective action.

Summary of Results and Findings

As a result of our audit procedures, KPMG identified findings relating to specific controls and processes that were subject to review. These findings are detailed further below and organized by condition, criteria, cause, effect and recommendation.

CMS Rule 9957 generally requires State Exchanges to perform oversight and financial integrity activities over exchange operations, keep an accurate accounting of receipts and expenditures and perform monitoring and reporting activities on Exchange-related activities. These requirements align with model internal control framework concepts such as those identified in the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s 2013 *Internal Controls – Integrated Framework*, which identifies fundamental internal control principles for the control environment, specific control activities, and monitoring.

Government Auditing Standards, i.e., the Government Accounting Office (GAO) Yellow Book, further define internal controls to include the processes and procedures for planning, organizing, directing, and controlling program operations, and management's system for measuring, reporting, and monitoring program performance KPMG identified controls through our walkthroughs with CCA process owners and identified gaps based on process objectives and associated risks. We tested identified controls and oversight activities within the audit scope and identified several findings indicating deficiencies in internal control activities. These deficiencies could increase CCA's risks of ineffective oversight and program integrity practices. For example, CCA was unable to provide select documentation and data from its initial HIX system to support testing of certain controls over enrollment, eligibility and financial processing activities. CCA did not exercise rigorous oversight of a key vendor performing customer service, financial processing and some IT development functions, and experienced a number of performance challenges as a result. CCA did not exercise effective oversight of IT privacy and security controls due to poorly defined governance responsibilities among CCA and other state agencies responsible for administering key elements of the successor HIX system. These conditions contributed to weaknesses in executing control activities.

Limitations

Our scope of procedures was subject to limitations due to inability to access data from the initial HIX system, and CCA's inability to provide access to certain documents relating to a third party service provider performing key services relating to the successor HIX system. The inability to access data from the initial HIX system impacted select elements of our audit program for testing Eligibility controls (e.g.,

Executive Summary (continued)

system interface functions, verification activities), Enrollment controls (e.g., customer account changes, QHP enrollment transactions), and Financial Processing controls (e.g., premium billing and receipt activities, customer refund activities). The inability to access certain documents relating to a third party service provider's key services relating to the successor HIX system impacted select elements of our audit program for testing IT Privacy and Security controls (e.g., ongoing monitoring activities, incident response activities).

Background

Background

The Patient Protection and Affordable Care Act (ACA) was enacted by the U.S. Congress on October 23, 2010 and established the framework for the operation of health insurance exchanges. Specific regulations were further detailed in the Centers for Medicare and Medicaid Services (CMS) Final Rule 9957, published July 19, 2013 and incorporated into 45 C.F.R. §155. In accordance with general program integrity and oversight requirements, Rule 9957 requires entities operating as state-based marketplaces (SBM) to engage an independent qualifying auditing entity which follows generally accepted governmental auditing standards (GAGAS) to perform an annual independent external programmatic audit. The SBM must ensure that the programmatic audit addresses compliance with Rule 9957 generally and specifically with program integrity and oversight requirements; processes and procedures designed to prevent improper eligibility determinations and enrollment transactions; and identification of errors that have resulted in incorrect eligibility determinations. The SBM is required to provide the results of the audit to CMS and publish a public summary of the results.

CCA was created in 2006 pursuant to Massachusetts General Laws (MGL) Chapter 176Q and is an independent public authority responsible for facilitating the availability, choice and adoption of private health insurance plans to eligible individuals and groups. CCA is governed by an eleven-member public/private Board, comprised of four ex-officio members from Massachusetts government (the Secretary of Administration and Finance, who serves as Chair of the Board; the Director of Medicaid; the Executive Director of the Group Insurance Commission; and the Commissioner of Insurance) and seven members of the general public (four appointed by the Governor and three appointed by the Attorney General). By law, public Board appointees encompass a range of interests and expertise including organized labor, employee health benefits, consumers, small business, actuarial science, health economics and health insurance brokerage.

With major ACA provisions going into effect as of January 1, 2014, CCA was designated as the SBM for Massachusetts. CCA's programs during 2014 included:

- Qualified Health Plans (QHPs) and Qualified Dental Plans (QDPs) for eligible individuals. Individuals with income up to 400% FPL may be eligible for federal tax credits, and individuals with income up to 250% FPL may be eligible for federal cost-sharing reductions.
- Small Business Health Options Program (SHOP), QHP and QDP programs for small businesses. Small businesses may be eligible for ACA Small Business Tax Credits with up to 50% of the cost of health insurance for businesses with fewer than 25 full-time equivalent employees, who earn on average $50,000 a year or less in 2014.
- ACA-required Navigator program, to provide grants to community organizations that assist individuals and small businesses with enrollment.
- Commonwealth Care, a subsidized program.

CCA personnel perform various business administration, program oversight and support functions (e.g., finance, legal, communications, public policy and outreach, plan management, operations and information technology, member appeals). CCA employed approximately 58 full-time equivalent personnel as of December 31, 2014. CCA contracts certain operations to private vendors (customer service and call center operations, select financial processing activities, some IT development and maintenance) and relies on other public agencies and their private vendors to provide other key services relating to core IT systems.

Background (continued)

45 C.F.R. §155.1200(c) – (d) requires CCA to engage an independent qualified auditing entity which follows generally accepted governmental auditing standards (GAGAS) to perform an annual independent programmatic audit. Federal regulations require that this audit address CCA's compliance with 45 C.F.R. §155 requirements, including oversight and program integrity, processes and procedures designed to prevent improper eligibility determinations and enrollment transactions, and identification of errors that have resulted in incorrect eligibility determinations. CCA is required to provide the results of the annual programmatic audit to HHS; make public a summary of the results of the external audit; and develop and inform HHS of a corrective action plan.

CCA experienced challenges during its development and rollout of its initial Health Information Exchange / Integrated Eligibility and Enrollment System (HIX) in October 2013. Among system failures, CCA was unable to perform eligibility determinations and enrollments for subsidized QHP coverage and experienced challenges with applying customer account changes and performing downstream financial transactions. As a result of identified failures with the initial HIX system and CCA's customer-facing website, CCA suspended member transition and enrollment into new ACA-compliant programs. The Commonwealth of Massachusetts (the "Commonwealth") obtained CMS approval to place individuals into temporary Medicaid coverage through the end of calendar year 2014. CCA developed manual workaround procedures to perform various processes and controls as a result of deficiencies within the initial HIX system. In 2014, development of a successor HIX system began with an initial rollout during November 2014 for the 2015 plan year open enrollment period.

Objectives, Scope, and Approach

Objectives, Scope, and Approach

Objectives

KPMG was engaged to perform a programmatic audit in accordance with both 45 C.F.R. §155.1200(c) and Government Auditing Standards to assess the Commonwealth Health Insurance Connector Authority's compliance with 45 C.F.R. §155 regulations for the calendar year ended December 31, 2014.

KPMG was responsible for preparing a written report communicating the results of the audit, including relevant observations and recommendations. These results include deficiencies in internal controls that are significant within the context of the objectives of the audit, any identified instances of fraud or potential illegal acts (unless they are inconsequential within the context of the audit objectives), and significant abuse that was identified as a result of this engagement.

In accordance with Government Auditing Standards, KPMG was also required in certain circumstances to report fraud, illegal acts, and violations of provisions of contracts or grant agreements, or abuse that we may detect as a result of this engagement, directly to parties outside the auditee.

Scope

KPMG was engaged to assess CCA's compliance with 45 C.F.R. §155 regulations for the calendar year ended December 31, 2014.

Audit Area	Representative Tasks	Sample Documentation
IT Privacy and Security	» Interview IT privacy and security process owners and review process control documentation. » Conduct process walkthroughs to identify and classify key controls for testing including: - Personally Identifiable Information (PII) and the confidentiality, disclosure, maintenance and use of information. - Incident management/reporting procedures. - Data loss and security breach incidents. » Select samples to test design and effectiveness of key controls and document any findings and recommendations.	» Internal IT control documentation – such as relevant IT security policies, application business rules, physical security provisions » Reports – incident reporting, user access, etc.

Objectives, Scope, and Approach (continued)

Audit Area	Representative Tasks	Sample Documentation
Eligibility	» Interview process owners and review process control documentation. » Conduct process walkthroughs to identify and classify key controls for testing including verification of basic applicant data, MAGI eligibility, account update procedures, exemption requests, appeals, and reporting to federal and state agencies. » Select samples to test design and effectiveness of key controls and document any findings and recommendations. » NOTE: Inability to access data from the initial HIX system limited our ability to perform control tests in this audit area.	» Internal control documentation – such as policies and procedures for eligibility determinations, account updates and terminations, etc. » Management Reports – applications and eligibility determinations activity » Member Applications – paper, electronic
Enrollment	» Interview process owners and review process control documentation. » Conduct process walkthroughs to identify safeguards over enrollment actions such as: - Enrolling individuals in QHP offerings. - Generating and correctly populating Forms 834. - Reporting (e.g., providing enrollee data to the CCA's Risk Adjustment entity as well as to CMS for Risk Corridor computation. » Select samples to test design and effectiveness of key controls and document any findings and recommendations. » NOTE: Inability to access data from the initial HIX system limited our ability to perform control tests in this audit area.	» Internal control documentation - such as policies and procedures for new members, terminations, status changes, etc. » Reconciliations with QHP issuers and CMS

Objectives, Scope, and Approach (continued)

Audit Area	Representative Tasks	Sample Documentation
Financial Processing	» Interview financial process owners and review process control documentation. » Conduct process walkthroughs to review and understand the calculations and reporting of QHP premiums and payments; federal and state APTC/CSR calculations, payments and associated reconciliation activity, and related reporting. » Select samples to test design and effectiveness of key controls and document any findings and recommendations.	» Internal financial policies and procedures » Financial reports– such as billing reports, CMS APTC/CSR reconciliations, etc.
General Exchange Functions	» Interview process owners of key roles in the target general exchange functions e.g., call center, compliance management, training, data/records maintenance. » Review process control documentation for these functions. » Conduct process walkthroughs to identify and classify key controls for testing. » Select samples to test design and effectiveness of key controls and document any findings and recommendations.	» Internal control documentation – policies and procedures on general exchange functions » Customer Service Representative performance reports » CCA employee training records

KPMG reviewed documents and performed inquiries, observations, walkthroughs and interviews with CCA management and process owners who perform select key program functions.

KPMG identified controls through our walkthroughs with CCA process owners relating to applicable program requirements and identified gaps based on process objectives and associated risks. We tested identified controls and oversight activities within the audit scope and identified several findings indicating deficiencies in internal control activities.

Specific to 45 C.F.R. §155.1200(c), our scope of work was designed to assess overall compliance with 45 C.F.R. §155, CCA's processes and procedures designed to prevent improper eligibility determinations and enrollment transactions, and identification of errors that may have resulted in incorrect eligibility determinations.

Objectives, Scope, and Approach (continued)

Approach

The audit was conducted in the following phases: Audit Planning, Information Gathering and Analysis, Audit Execution, and Reporting. Each phase is described below.

Audit Planning: The first phase of this project involved embedding performance audit project management protocols to set tone, manage expectations and define communications protocols from the outset. During this phase, we developed, reviewed with stakeholders and implemented several key project management artifacts, as follows:

- Project Charter
- Communication Plan
- Document Request List

We held a formal Project Kickoff Meeting to introduce key stakeholders to the KPMG engagement team and confirm our mutual understanding of the audit scope and objectives. We also conducted regular status meetings with our principal CCA liaison and periodic in-progress observation session with the CCA Executive Director in the course of audit execution.

Information Gathering and Analysis: Following engagement kickoff, this phase involved further developing our understanding of CCA's activities, processes and controls during the audit period and developing our approach to audit execution. Specifically, we performed the following tasks:

- Reviewed existing documentation: We obtained background documentation from CCA process owners including, where applicable, policies and procedures, process flows, sample management reports and other background documentation. We reviewed this documentation to augment and refine our team's understanding of CCA's control environment and control activities.
- Conducted interviews, walkthroughs and high-level process reviews: We met with various CCA process owners, line management and staff to expand our understanding of the specific and general exchange functions identified in our audit scope. We sought to develop our understanding of the interactions, respective duties and responsibilities of key roles in targeted general function areas (e.g., call center operations) and key procedures relating to eligibility, enrollment and financial management.

Audit Execution: This phase consisted of developing our audit program and executing tests of CCA's controls and compliance with regulatory requirements within 45 C.F.R. §155. This involved the following activities:

- Reviewing and testing specific procedures to assess the processes around Financial Processing activities, including premium billing, member payment and refund processing, transaction reporting to health insurance carriers, management review and reconciliation procedures, and exchange sustainability protocols.
- Reviewing and testing specific procedures to assess the processes around high-risk IT Privacy and Security control areas following the Minimum Acceptable Risk Standards for Exchanges (MARS-E) control catalog.

Objectives, Scope, and Approach (continued)

- Reviewing and testing safeguards over member eligibility determinations, exemption requests and appeals, subject to limitations due to inability to access data from the initial HIX system.
- Reviewing and testing safeguards over enrollment actions such as enrolling individuals in QHP offerings and generating enrollment reporting forms.
- Reviewing and testing specific procedures relating to oversight and financial integrity responsibilities of general exchange functions, including call center operations and vendor management, governance activities, Navigator and assister programs, QHP/QDP certification, and SHOP program oversight.

Validation and Reporting: This phase consisted of validating the draft findings with CCA process owners, developing observations and recommended improvements, and discussing CCA's plans for corrective action. Our detailed findings are documented further below.

Procedures and Methodology

We reviewed the requirements of 45 C.F.R. §155 to identify performance audit objectives relevant to CCA's exchange functions. We performed this engagement in accordance with Government Auditing Standards and developed audit programs and testing procedures in accordance with GAS and KPMG audit methodologies.

- *Document review, interview and walkthrough procedures* – We reviewed CMS Final Rule 9957 and associated regulations under 45 C.F.R. §155 to identify compliance requirements subject to this performance audit. KPMG worked with CCA management to identify process owners for key activities and performed interviews and walkthroughs to document processes and control activities existing during the audit period. Based on this information, KPMG requested supporting documentation to help confirm our understanding of the process activities and controls identified and developed audit procedures to test the design and operating effectiveness of identified controls.
- *Sample testing approach* – In support of testing the design and effectiveness of selected controls, KPMG made sample selections of transactions and other control activities to perform test procedures. One of the factors that one may consider necessary when determining the extent of evidence necessary to persuade us that the control is effective is the risk of failure of the control. As the risk of failure of the control decreases, the evidence that we obtain also decreases. Conversely, as the risk of failure of the control increases, the evidence we obtain also increases such that we might choose to obtain more persuasive audit evidence or otherwise adjust testing procedures. This allows us to vary the evidence obtained for each individual control based on the risk of failure of the individual control.
- *Consideration of fraud, illegal acts, misconduct and abuse* – In planning the audit, we had a responsibility to gather and review information to identify and assess the risk of fraud occurring that is significant within the context of performance audit objectives. When fraud risk factors were identified that the engagement team believed were significant within the context of the performance audit objectives, we had the responsibility to design procedures to provide reasonable assurance of detecting if such fraud occurred or is likely to have occurred. Assessing the risk of fraud is an ongoing process throughout the performance audit and relates not only to planning the performance audit but

also to evaluating evidence obtained during the performance audit. We considered the risks of potential fraud, misconduct and abuse within each testing area and adjusted testing procedures and sample sizes accordingly based on potential risks. Examples of approach modifications we applied for higher risk testing areas included increasing sample size, adjusting timing of testing procedures to focus on higher risk periods, applying judgmental selection of samples, applying analytic procedures, and applying more precise tests.

Limitations

During the audit period, CCA transitioned between two HIX systems; the initial HIX system was in use from January 2014 – November 2014 and was taken out of production once the successor HIX system was launched in November 2014. CCA informed us that the initial HIX system was no longer a production system during the performance of our audit procedures and data from this system would not be available to support control testing. Additionally, CCA informed us that due to identified functional deficiencies with this initial system, many core system functions relating to eligibility and enrollment were deactivated and manual workaround procedures developed, which included enrollment of nearly all subsidized customers into temporary Medicaid programs for the 2013-14 open enrollment and 2014 closed enrollment periods. As such, these circumstances impacted select elements of our audit program for testing Eligibility controls (e.g., system interface functions, verification activities), Enrollment controls (e.g., customer account changes, QHP enrollment transactions), and Financial Processing controls (e.g., premium billing and receipt activities, customer refund activities).

Due to the IT governance arrangement of the successor HIX system, CCA relies on a Commonwealth agency to perform key services relating to IT Privacy and Security. CCA is not a party to the service agreement between this agency and a third party service provider relating to successor HIX system operations; as such, CCA was unable to provide access to certain data sources to support our testing of IT Privacy and Security controls (e.g., ongoing monitoring activities, incident response activities).

Results – Findings, Observations, and Recommendations

Results – Findings, Observations, and Recommendations

Introduction

In accordance with Government Auditing Standards, KPMG prepared this report communicating the results of the completed performance audit, including relevant observations and recommendations. The findings presented as part of this engagement are restricted to the use stipulated in our contract. We disclaim any intention or obligation to update or revise the observations whether as a result of new information, future events, or otherwise. Should additional documentation or other information become available that impacts the observations reached in our deliverable, we reserve the right to amend our observations and summary documents accordingly.

Summary of Findings

Our detail findings are noted below. Please note that each finding is split into five areas:

- Condition – Explains the issue found as part of the audit
- Criteria – This is an explanation of the requirements related to the issue and a determination of how criteria and processes should be executed
- Cause – This is the assessment of the source of the risk area
- Effect – Potential result if the condition continues
- Recommendations – A short discussion on what should be done to improve the identified condition

As a result of our audit procedures, we identified findings relating to specific controls and processes that were subject to review. These findings are detailed further below and organized by condition, criteria, cause, effect, and recommended corrective action.

CMS Rule 9957 generally requires State Exchanges to perform oversight and financial integrity activities over exchange operations, keep an accurate accounting of receipts and expenditures, and perform monitoring and reporting activities on Exchange-related activities. These requirements generally align with accepted internal control framework concepts such as those identified in the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s 2013 *Internal Controls – Integrated Framework*, which identifies fundamental internal control principles for the control environment, specific control activities, and monitoring.

Government Auditing Standards (i.e., the Government Accounting Office (GAO) Yellow Book) further define internal controls to include the processes and procedures for planning, organizing, directing, and controlling program operations and management's system for measuring, reporting, and monitoring program performance. KPMG identified controls through our walk-throughs with CCA process owners and identified gaps based on process objectives and associated risks. We tested identified controls and oversight activities within the audit scope and identified several findings indicating deficiencies in internal control activities. These deficiencies could increase CCA's risks of ineffective oversight and program integrity practices. For example, CCA was unable to provide certain documentation and data from its initial HIX system to support testing of specific controls over enrollment, eligibility, and financial processing activities. CCA did not exercise rigorous oversight of a key vendor performing customer service, financial processing and some IT development functions, and experienced a number of performance challenges as a result. CCA did not exercise effective oversight of IT Privacy and Security controls due to poorly defined governance responsibilities between CCA and other state agencies

responsible for administering key elements of the successor HIX system. These conditions may contributed to weaknesses in executing control activities.

Other findings indicated deficiencies in internal control activities which may have limited CCA's ability to perform effective oversight, review, and reconciliation practices and comply with regulatory requirements for records maintenance, accessibility, and reporting. For example, CCA did not effectively perform oversight, review and reconciliation activities relating to certain financial processing areas, including premium revenue and carrier payment reporting. CCA's practices for maintaining records of financial interests of board members, while geared toward complying with Commonwealth laws and regulations, do not meet all federal requirements.

Results – Findings, Observations, and Recommendations (continued)

Finding #2014-01 – Access to Data

Condition: KPMG noted two primary areas where access to data necessary to perform detailed testwork in core Exchange operational areas was limited.

- The initial HIX system was taken out of production by CCA in November 2014. Control tests involving the initial HIX system as well as validation of system reports generated from the initial HIX data sources could not be performed, as CCA could not provide any sample transaction data to support such tests.
- Due primarily to timing issues, certain transaction-level data from the successor HIX system pertaining to eligibility, enrollment, and certain areas of financial processing was not available for testing.

Criteria: As defined in 45 C.F.R. § 155.1210, the Exchange must maintain documents, records, and other evidence which is sufficient to accommodate periodic auditing of the Exchange.

Cause: CCA indicated that the initial HIX system remained in active production for approximately one week following the launch of the successor HIX systems, with both systems running in parallel during this time. The initial HIX system was taken out of production in November 2014 and was no longer a production system prior to commencing this performance audit. Additionally, CCA indicated that the initial HIX system data accessibility was limited due to ongoing litigation between CCA and its vendor.

Inability to access to successor HIX system transaction-level data was due to engagement timing, as well as restrictions governing access to Personally Identifiable Information / Protected Health Information (PII/PHI).

Effect: Inability to provide data sufficient for audit puts CCA at risk of noncompliance with federal health benefit exchange regulations.

Recommendation: Develop and adhere to a comprehensive policy to satisfy federal regulations regarding data availability for audit.

Finding #2014-02 – Vendor Oversight

Condition: CCA did not provide sufficient oversight of supporting vendors' satisfaction of their core contractual obligations and performance reporting responsibilities in the following areas:

- Periodic monitoring of contractually-required performance metrics;
- Development of key customer interaction activities such as customer satisfaction surveys, e-mail, and Web chat support;
- Review and assessment of performance penalties;
- Obtaining sufficient reporting detail to perform effective review of timely application of customer premium payments from suspense accounts;
- Timely identification and processing of customer refunds.

Criteria: As defined in 45 C.F.R. § 155.200, the Exchange must perform required functions related to oversight and financial integrity; as defined in 45 C.F.R. § 155.205, the Exchange must perform certain activities relating to consumer assistance through a call center.

Additionally, the CCA's agreement with its call center vendor requires:

- Timely reporting of contractually required performance metrics;
- Performance of customer outreach activities including periodic customer satisfaction surveys and support of e-mail and Web chat communication capabilities;
- Review and approval of refund information identified and recorded in the vendor's Financial Management System (FMS);
- Review and approval of contractor reports before invoicing.

Cause: CCA did not follow established procedures or fully enforce contractual vendor performance requirements, as evidenced by the conditions above. CCA relied on compilations of summary-level reporting data from the call center vendor for select contractual performance requirements and did not perform substantive reviews of vendor performance against established criteria.

Effect: CCA's existing oversight practices did not allow for adequate scrutiny of vendor practices and enforcement of accountability. Failure to periodically and diligently oversee vendor activities and performance reporting may increase the risk of inadequate contractual performance.

Recommendation: Consider strengthening current vendor oversight procedures by:

- Enhancing current monitoring practices to help ensure vendor satisfaction of core performance objectives.
- Formalizing the current ad-hoc refund adjudication processes between the vendor and CCA for processing customer premium payments in suspense and customer refunds in attempt to process such transactions more timely. Over the longer term, consider the potential viability of an automated solution to address this issue.
- Performing periodic reconciliation of vendor invoices and retaining adequate evidence to substantiate this activity.
- Reviewing contractual reporting requirements and current reports relating to financial processes and assessing if additional changes are needed to support proper financial management (e.g., premium account aging).

Finding #2014-03 – IT Governance

Condition: CCA did not perform effective oversight of external-party operations that are essential to the Authority's core functions in the following areas:

- CCA relies on another state agency to perform control activities over select IT privacy and security functions. This relationship and the associated responsibilities are not memorialized in a formal agreement outlining specific tasks which CCA is responsible for and which CCA relies on the other state agency to perform.
- Through this other state agency, CCA relies on a third-party service provider to perform key control activities in support of its successor HIX system. CCA is not a party to the other agency's contract with the third-party service provider, limiting its ability to exercise oversight of the service provider's activities.

Criteria: 45 C.F.R. §155.260 requires the Exchange to execute a contract or agreement with all non-Exchange entities which access, collect, use, or disclose PII; additionally, 45 C.F.R. §155.260 requires the Exchange to implement privacy and security standards including reasonable operational, administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure of personal information stored by the Exchange.

Cause: These conditions are caused by a lack of formally defined and documented responsibilities for key IT privacy and security controls between CCA, servicing state agencies, and third-party service providers.

Effect: This condition creates the risk that CCA is unable to adequately monitor privacy and security controls relating to its core HIX system and fulfill oversight requirements. Lack of a formal agreement specifically delineating express responsibilities for elements of the required IT privacy and security control suite may create gaps in critical control measures.

Recommendation: Formalize the nature of the relationship and obligations among CCA, other governmental agencies, and third-party vendors, as necessary, to help ensure well-defined roles, and clear oversight responsibilities.

Finding #2014-04 – Financial Processes

Condition: CCA did not perform effective management review of customer premium payments and premium payments to carriers, as evidenced by conditions such as the following:

- As a standard control measure, CCA initially sought to reconcile monthly 820 reports and carrier payment reports generated by the FMS system against member eligibility data. However, due to limitations with the initial HIX system, CCA was unable to obtain the required source data from this application to perform meaningful reconciliations of customer premium payments received and carrier premium payments made. As the designed reconciliation activity could not be performed, a set of manual compensating controls were necessary to address this control objective.
- Despite this system limitation, CCA did not develop and implement a robust control activity to compensate for this issue. While CCA was able to obtain and review a supporting series of exception-based insurance carrier reports, its deliberate consultations with relevant parties to address reconciling items identified were not well-evidenced.

Criteria: Criteria for enrollment of qualified individuals into QHPs are defined in 45 C.F.R. §155.400. As defined in 45 C.F.R. §155.200, the Exchange must perform required functions related to oversight and financial integrity. As defined in 45 C.F.R. §155.1200, the Exchange must accurately account for receipts and expenditures.

Cause: System functionality with the initial HIX system did not allow for proper execution of this control measure resulting in CCA staff using less effective oversight measures in an effort to provide assurance over the information reported.

Effect: CCA used data outputs from the same system in attempt to perform some measure of validation of the aggregate data reported. This condition increased the risk that CCA may not properly detect issues with the reliability and accuracy of data to support financial reporting activities, as no comparisons are made to source data in the successor HIX system nor to information received from carriers. Additionally,

this practice may have limited CCA's ability to identify errors or exceptions relating to enrollment and premium activity on a timely basis and apply corrective action steps.

Recommendation: Consider strengthening current vendor oversight procedures by:

- Reviewing reconciliation procedures to incorporate reconciliation of 820 reports and carrier payment reports to source data obtained from successor HIX system and carrier confirmation reports.
- Expanding existing exception-based review processes for carrier reporting to monitor reporting on a more systematic basis.

Finding #2014-05 – Governance

Condition: While CCA has observed the Commonwealth's laws and regulations for disclosure of conflicts of interest and financial interests for board members since its creation, CCA did not adhere to all federal regulations regarding board governance principles for state-based Exchanges. Instead, CCA relied on exception-based reporting from its governing board members to monitor disclosures of financial interests.

Criteria: Standards for Exchange Governance principles are defined in 45 C.F.R. §155.110(d): "Governance principles. (1) The Exchange must have in place and make publicly available a set of guiding governance principles that include ethics, conflict of interest standards, accountability and transparency standards, and disclosure of financial interest. (2) The Exchange must implement procedures for disclosure of financial interests by members of the Exchange board or governance structure."

Cause: CCA did not follow federal regulatory requirements, but rather relied on Massachusetts state laws, which only require financial interest disclosures from governing board members in specific circumstances.

Effect: This condition is inconsistent with applicable federal regulations and increases the risk to the Authority of ineffective governance and oversight.

Recommendation: Implement and maintain formal governance principles including ethics, conflicts of interest standards, accountability and transparency, and disclosure of financial interests.

Finding #2014-06 – Policies and Procedures (Internal Controls)

Condition: CCA did not maintain a complete set of internal control policies and procedures during the period of review. Specifically, the following were not observed during the audit:

- Robust and accurate documentation of current internal controls across all CCA operational areas;
- Regularly documented reviews and updates of policies and procedures.

In addition, a key oversight position was vacant during significant portions of the audit period.

Criteria: As defined in 45 C.F.R. §155.200, the Exchange must perform required functions related to oversight and financial integrity.

Cause: This condition was caused by inconsistent practices for maintaining key supporting control documents. While policies and procedures supporting multiple areas within CCA accurately reflected component control activities, certain policies and procedures were found to be outdated or not in use.

Results – Findings, Observations, and Recommendations (continued)

Additionally, CCA for several months during the audit period did not fill its vacant Chief Financial Officer position.

Effect: Failure to document and perform timely maintenance of policies and procedures comprising an organization’s internal controls reduces and limits the effectiveness of the organization's overall control environment.

Recommendation: Regularly review and analyze the adequacy of the elements comprising the authority's control framework, and make timely adjustments to strengthen key control activities.

Management's Response

2014 Programmatic Audit

Management Response

Submitted on May 28, 2015

Management's Response

Summary

The Health Connector's new management team recognizes the independent auditor's analysis of our programmatic procedures and controls for calendar year 2014. As noted in the report, the Commonwealth Health Insurance Connector Authority's (the Health Connector) 2014 operations were deeply challenged by the limitations of the initial Health Insurance Exchange (HIX) Information Technology system built by the Commonwealth's first system integrator, resulting in the use of workarounds and manual processes to ensure continued access to health insurance for the residents of the Commonwealth. Repairs to the HIX system, and elaboration of basic functionality, continue, but the Connector has been working to stabilize and improve operations and operational control, vendor oversight, and customer experience.

The findings of the report highlight a number of opportunities for enhanced controls that the Health Connector management team is committed to investigating in an effort to support its operations. The Health Connector management team intends to work with staff, partner agencies and vendors to implement many of the recommendations provided by the audit as we work to improve our operations, enhance our technology platform and continue to expand health insurance coverage throughout Massachusetts.

Finding #2014-01 – Access to Data

For Open Enrollment 2014, the Health Connector implemented a HIX Information Technology system built by the Commonwealth's first systems integrator which had significant technical limitations. The system's technical limitations resulted in a de minimis volume of fewer than 50 subsidized QHP eligibility determinations being conducted in the initial HIX; the remainder of subsidized applicants were, as noted in the report, enrolled in a CMS-approved temporary Medicaid program managed by MassHealth. A significantly larger number of unsubsidized QHP determinations and enrollments were conducted via the initial HIX.

The Health Connector acknowledges that eligibility and enrollment data from the initial HIX could not be provided in the abbreviated time frame established for the purposes of audit sample testing. At the time of the audit, the initial HIX system had been taken out of production and, consequently, no mechanism was available to provide data in an easily consumed and rapid manner. However, all data collected by the initial HIX has been retained in accordance with records retention requirements and could be made available for review.

The Health Connector ceased using the initial HIX system as of November 2014 and, as a result, does not anticipate any corrective actions are required to ensure future access to this particular data for programmatic audit purposes.

The Health Connector provided thorough support for the testing of eligibility and enrollment controls in the successor HIX system implemented by the Commonwealth's new systems integrator for Open Enrollment 2015. As noted in the report, limitations on the provision of transaction-level data were the result of the limited time available for the audit and Health Connector teams. The sample requests made by KPMG required customized SQL queries by the Health Connector's IT team and manual "look-up" and printing of each sample case by Health Connector Operations staff. Finally, the unique features of Massachusetts' exchange, including Medicaid integration and the ConnectorCare subsidy program, required additional background interviews and more iterations of reviews by the audit team, resulting in a longer sample review timeline.

Management's Response (continued)

The Health Connector anticipates that, in future audits, the provision of sample data will be made more efficient by early definition of reporting requirements.

Finding #2014-02 – Vendor Oversight

The Health Connector acknowledges that, during 2014, vendor oversight of the Health Connector's customer service and business operations vendor did not meet expectations. As a result of the significant limitations of the initial HIX system, substantial and unplanned, additional work activities were placed on the customer service and business operations vendor. As a result, their performance did not meet the expectations included in the contract, nor those of the Health Connector or our customers.

The Health Connector has undertaken a set of corrective measures related to the oversight of the customer service and business operations vendor. First, the Health Connector has placed the vendor under a formal corrective action plan as specified in the contract. Second, the Health Connector has launched an Operational Assessment to identify and address limitations in the organization's customer service and business operations activities. The Assessment Team, made up of senior members from all Health Connector departments, as well as agency partner and vendor organizations, examined all aspects of the Health Connector's customer experience and back-office practices to identify pain points, deficiencies, and opportunities for improvement. The initial phase of the Assessment has concluded and significant changes have been made to the vendor's organizational structure, staffing and business practices to support improved customer experience.

E-mail and web chat support, noted in the report as contracted activities that were not performed by customer service and business operations vendor, was work premised upon the availability of IT functionality built by the Commonwealth's first systems integrator. This functionality was de-scoped from the initial HIX system and, as such, the Health Connector does not consider this to be a failure by customer service and business operations vendor to provided required services. Going forward, the organization will seek to enhance the documentation of the "downstream" impacts of any IT scope changes and to provide additional clarity to vendors regarding their associated contractual responsibilities.

Finding #2014-03 – IT Governance

The Health Connector believes that the capabilities provided by the Massachusetts Office of Information Technology (MassIT) meet or exceed the requirements of state and federal regulations. Both the initial and successor HIX system's privacy and security controls, overseen by MassIT, were approved by both the Centers for Medicare & Medicaid Services (CMS) and the Internal Revenue Service (IRS). MassIT exercises rigorous controls over the two primary IT system vendors. The Health Connector provides effective oversight of its staff, as well as its partner vendors. The report does not identify any specific risks or gaps in the security or privacy controls implemented as part of the successor HIX system.

The Health Connector believes that the relationship between itself and MassIT provides sufficient visibility and collaboration to ensure that the system meets the necessary security and privacy requirements. In addition, MassIT plays an important role in supporting the "single front door" shared eligibility concept, a central principle of the Affordable Care Act, which has been implemented by the Health Connector and our partners at MassHealth.

Management's Response (continued)

We do, however, recognize that a more systematized agreement among the Health Connector, MassIT and the Massachusetts Executive Office of Health and Human Services (EOHHS) would further support our shared roles and responsibilities, including such matters as access controls. To this end, the Health Connector has this month concluded an interagency agreement with MassIT and EOHHS, which delineates responsibilities for, among matters, data privacy and security. The Health Connector will continue to work with our Commonwealth partners and vendors to develop more formalized protocols and understandings regarding governance of the shared eligibility system.

Finding #2014-04 – Financial Processes

The Health Connector concurs with the report's note that significant technical limitations in the initial HIX system resulted in the data collected by this system being determined as unsuitable or unavailable for financial reconciliation purposes. Health Connector Finance staff were unable to identify a replacement data source and, as a result, were required to rely solely on the customer service and business operations vendor's Financial Management System (FMS) as the source of truth for financial transactions. The Health Connector acknowledges that the use of a single source is not optimal practice. As a result of the implementation of the successor HIX system, the Health Connector is now able to use the successor HIX as a second source for financial reconciliation purposes.

The Health Connector, with the implementation of the successor HIX system and automated 834 and 820 transactions to carriers, has improved its carrier financial reconciliation process. The Health Connector provides a monthly 834 file, monthly 820 file and monthly carrier payment report to carriers to support their financial reconciliation activities. Carriers then provide exception-based feedback to the Health Connector, in accordance with industry practices, for review and correction. Health Connector staff meets with the customer service and business operations vendor on a weekly basis to resolve and review any discrepancies reported from carriers, after which updates are communicated to carriers.

Finding #2014-05 – Governance

The Health Connector's Board of Directors are governed by the state's conflict of interests law, contained at Massachusetts General Laws (MGL) Chapter 268A. These legal requirements, which govern board members, are a comprehensive code of ethics, and address ethics, conflicts, accountability, transparency, and the disclosure of financial or other interests that constitute a conflict with public roles and responsibilities. These requirements are provided in written form to board members upon appointment and annually thereafter. Board members have all completed training on their ethics responsibilities and requirements. Board members have in the past provided disclosures of financial interests where required by state law. These requirements, which operate by state law, are consistent with federal guidance regarding board governance. The report does not identify any evidence of unreported conflicts of interest or lapses in financial disclosure requirements. It further does not suggest that the Board has not been governed by legal ethics requirements under state law.

However, the Health Connector acknowledges the opportunity to further clarify the Board's high ethical standards by working with the Board to develop a written statement applicable to the Board that memorializes these requirements.

Management's Response (continued)

Finding #2014-06 – Policies and Procedures (Internal Controls)

As noted in the report, the unique challenges presented by the limitations of the initial HIX system required the Health Connector to implement a series of workarounds to ensure coverage of the residents of the Commonwealth of Massachusetts. To that end, some documented standard operating procedures and policies were not viable or were not updated to reflect temporary workaround activities.

While the Health Connector did not have a Chief Financial Officer in place during the audit period, the organization's financial activities were effectively managed by the Director of Finance, with oversight provided by the Executive Director who served previously as the organization's CFO. In addition, during the audit period, the Health Connector was actively recruiting for a new Chief Financial Officer.

The Health Connector does not agree that the identified gaps constitute a material finding and were, in large measure, the result of the anomalous and extraordinary system limitations present in 2014. However, in an effort to ensure ongoing improvements in organizational practices, the Health Connector will formalize the regular review of policies and procedures.

Appendix A – List of Interviewed Personnel

Appendix A – List of Interviewed Personnel

Name	Title
Louis Gutierrez	CCA Executive Director
Ed DeAngelo	CCA General Counsel
Vicki Coates	CCA Chief Operating Officer
Jason Hetherington	CCA Chief Information Officer
David Kerrigan	CCA Director of Business Development
Jen Bullock	CCA Director of Customer Service & Operations
Dom DiVito	CCA Director of Accounting
Kari Miller	CCA Manager of Finance
Sarah Bushold	CCA Senior Manager of External Affairs & Plan Management
Michael Norton	CCA Senior Manager of External Affairs & Carrier Relations
Lauren Ripley	CCA Assistant General Counsel
Merritt McGowan	CCA Assistant General Counsel
Andrew Egan	CCA Assistant General Counsel
Shirl Mulford	CCA Director of Human Resources
Nancy Stehfast	CCA Appeals Unit Manager
Rebekah Diamond	CCA Manager of External Affairs
Heather Cloran	CCA Manager of Student Health Insurance Programs
Niki Conte	CCA Associate Director for Public Outreach & Education
Paul Landesman	CCA Manager of Outreach & Education
Stacy Halloran	CCA Senior Accountant & Benefits Coordinator
Sam Osoro	CCA Senior Financial Analyst
Brian Schuetz	CCA Director of Business & Technology Integration
Elba Mendez	CCA Implementation Manager
Joanne Biag	CCA Senior Manager of Operations
Valerie Berger	CCA Program Manager
JoAnna Waterfall	CCA Operations Manager
Tatsiana Murauyeva	CCA Manager of Operations
Nelson Teixeira	CCA Manager of Customer Service
Manny Gonzalez	CCA Operations Associate
Jason Hetherington	CCA Chief Information Officer
April May	CCA IT Process Manager
Simon Bellan	CCA Enterprise Architect
David Lemoine	CCA Senior Manager, IT Strategy & Partnerships

Appendix A – 20 Data Elements (continued)

Name	Title
Sage Shaw	CCA IT Implementation Manager
Kevin Burns	Commonwealth agency service provider Chief Security Officer
Scott Margolis	Commonwealth agency service provider HIX Security & Privacy Compliance Manager
Kevin Prefontaine	Commonwealth agency service provider Security & Privacy Compliance Manager
Cathy Karst	Third Party IT Vendor Representative
Charlene Cunningham	Third Party IT Vendor Representative
Thomas Cole	Third Party IT Vendor Representative
Rodrigo Ruiz	Third Party IT Vendor Representative
Daniel Henderson	Third Party IT Vendor Representative
Geoffrey Potts	Third Party Call Center Vendor Representative
Sean Warner	Third Party Call Center Vendor Representative
Annette DiFelice	Third Party Call Center Vendor Representative
Wes McCullough	Third Party Call Center Vendor Representative
Deana Zimmerman	Third Party Call Center Vendor Representative
Robyn Bluestein	Third Party Call Center Vendor Representative
Karla Castillo	Third Party Call Center Vendor Representative

Appendix B – Glossary of Terms

Appendix B – Glossary of Terms

ACA	Patient Protection and Affordable Care Act
APTC	Advance Premium Tax Credit
CCA	Commonwealth Health Insurance Connector Authority
CFR	Code of Federal Regulations
CMR	Code of Massachusetts Regulations
CMS	Centers for Medicare and Medicaid Services
CSR	Cost Sharing Reduction
FMS	Financial Management System
FPL	Federal Poverty Level
GAS	Government Auditing Standards
HIPAA	Health Insurance Portability and Accountability Act
HIX	Health Information Exchange
HHS	U.S. Department of Health and Human Services
MassIT	Massachusetts Office of Information Technology
OIG	Office of the Inspector General, U.S. Department of Health and Human Services
PHI	Protected Health Information
PII	Personally Identifiable Information
QDP	Qualified Dental Plan
QHP	Qualified Health Plan
SBM	State-Based Marketplace
SHOP	Small Business Health Options Program

Appendix C –

Corrective Action Plan

2014 Programmatic Audit

Corrective Action Plans

Submitted on May 28, 2015

Appendix C – Corrective Action Plan

Audit Report Corrective Action Plan		
Issue Title: Finding #2014-01 – Access to Data		
Audit Report Recommendation: Develop and adhere to a comprehensive policy to satisfy federal regulations regarding data availability for audit.		
Description of Remediation: Enhance the provision of sample data by the timely execution of a BAA and early definition of reporting requirements.		
Milestone	**Target Date**	**Completion Date**
1. In future programmatic audits, require a clear definition of data requirements in a time frame that will permit data gathering and testing.	At initiation of Programmatic Audit contract	
2. Conduct detailed requirements definition sessions to develop reporting requests for eligibility and enrollment test sampling	During initial phase of Programmatic Audit	
Plan for Monitoring and Validation: n/a		
Responsible Entity or Individual: Programmatic Audit Liaison		

Appendix C – Corrective Action Plan (continued)

<table>
<tr><th colspan="3">Audit Report Corrective Action Plan</th></tr>
<tr><td colspan="3">Issue Title: Finding #2014-02 – Vendor Oversight</td></tr>
<tr><td colspan="3">Audit Report Recommendation: Consider strengthening current vendor oversight procedures by:
Enhancing current monitoring practices to help ensure vendor satisfaction of core performance objectives.
Formalizing the current ad-hoc refund adjudication processes between the vendor and CCA for processing customer premium payments in suspense and customer refunds in attempt to process such transactions more timely. Over the longer term, consider the potential viability of an automated solution to address this issue.
Performing periodic reconciliation of vendor invoices and retaining adequate evidence to substantiate this activity.
Reviewing contractual reporting requirements and current reports relating to financial processes and assessing if additional changes are needed to support proper financial management, e.g., premium account aging.</td></tr>
<tr><td colspan="3">Description of Remediation: The Health Connector will conduct a broad assessment of its operational procedures, with a focus on improving vendor reporting/oversight and customer experience.</td></tr>
<tr><th>Milestone</th><th>Target Date</th><th>Completion Date</th></tr>
<tr><td>1. Implement enhanced Service Level Agreement (SLA) monthly reporting from customer service and business operations vendor</td><td>January 2015</td><td>January 2015</td></tr>
<tr><td>2. Implement enhanced Issue Tracking reporting for customer service and business operations vendor</td><td>January 2015</td><td>January 2015</td></tr>
<tr><td>3. Operations Assessment: Identify all pain points, root causes and system limitations</td><td>April 2015</td><td>April 2015</td></tr>
<tr><td>4. Operations Assessment: Develop a plan to make significant and demonstrable progress on the aged inventory</td><td>May 2015</td><td>May 2015</td></tr>
<tr><td>5. Operations Assessment: Develop a set solutions to prevent the re-creation of service issues and inventory</td><td>May 2015</td><td>May 2015</td></tr>
<tr><td>6. Operations Assessment: Develop a set of metrics to monitor ongoing operational performance</td><td>May 2015</td><td>May 2015</td></tr>
<tr><td>7. Implement monthly meetings with CCA Operations, CCA Finance and customer service and business operations vendor staff to review performance, SLAs, review contractual penalties, and identify “go-forward” opportunities</td><td>June 2015</td><td></td></tr>
<tr><td colspan="3">Plan for Monitoring and Validation:
Conduct weekly Operations Assessment status reviews to monitor process to assessment goals
Provide periodic updates to CCA Board of Directors and Office of the Governor</td></tr>
<tr><td colspan="3">Responsible Entity or Individual: Chief Operating Officer, Director of Member Services</td></tr>
</table>

Appendix C – Corrective Action Plan (continued)

Audit Report Corrective Action Plan		
Issue Title: Finding #2014-03 – IT Governance		
Audit Report Recommendation: Formalize the nature of the relationship and obligations among CCA, other governmental agencies and third party vendors, as necessary, to help ensure well-defined roles, clear oversight responsibilities.		
Description of Remediation: Work with Commonwealth partners and vendors to develop formalized agreements to define roles and responsibilities.		
Milestone	**Target Date**	**Completion Date**
1. Execute interagency agreement regarding data privacy and security responsibilities among Health Connector, MassIT and EOHHS	May 2015	May 2015
2. Convene a multi-agency working group (CCA, EOHHS, MassIT) to develop general framework for agreement	June/July 2015	
3. Convene topic-specific multi-agency working groups to define key details for agreement (IT Privacy and Security, Finance, Operational Coordination)	July 2015	
4. Draft and seek comments/review of multi-agency agreement	Q3-Q4 2015	
5. Execute multi-agency agreement	Q4 2015	
Plan for Monitoring and Validation: Monthly review of agreement status/progress at HIX Project Executive Steering Committee		
Responsible Entity or Individual: Executive Director, General Counsel, Chief Information Officer		

Appendix C – Corrective Action Plan (continued)

<table>
<tr><th colspan="3">Audit Report Corrective Action Plan</th></tr>
<tr><td colspan="3">Issue Title: Finding #2014-04 – Financial Processes</td></tr>
<tr><td colspan="3">Audit Report Recommendation: Consider strengthening current vendor oversight procedures by:
Reviewing reconciliation procedures to incorporate reconciliation of 820 reports and Carrier Payment Reports to source data obtained from successor HIX system and carrier confirmation reports.
Expanding existing exception-based review processes for carrier reporting to monitor reporting on a more systematic basis.</td></tr>
<tr><td colspan="3">Description of Remediation: Building on the capabilities of the successor HIX system and automated 834 and 820 transactions to carriers, CCA will work to improve its carrier financial reconciliation process by diversifying input source data and developing automated reconciliation capabilities.</td></tr>
<tr><th>Milestone</th><th>Target Date</th><th>Completion Date</th></tr>
<tr><td>1. Implement automated 834 outbound and inbound XML transactions with issuers</td><td>October – December 2014</td><td>December 2014</td></tr>
<tr><td>2. Implement automated 820 outbound XML transactions to issuers</td><td>January 2015</td><td>January 2015</td></tr>
<tr><td>3. Implement transfer of an 820 XML report that matches the wired amount that carriers would receive from the State and from members’ monthly premiums.</td><td>March 2015</td><td>March 2015</td></tr>
<tr><td>4. Implement a process for the creation and transmission to CCA of a member-level report from successor HIX system, a valid secondary source with billing rates and enrollment status information</td><td>August 2015</td><td></td></tr>
<tr><td>5. Create a statistical program to validate that the 820 XML report from the customer service and business operations vendor confirms the current enrollment status and the value of payments are valid. If that is not the case, CCA will manually investigate any discrepancies with the vendor’s billing manager. CCA will not pay any subsidy amounts that are in discrepancy with this process.</td><td>September 2015</td><td></td></tr>
<tr><td>6. Implement revised customer refund policy and procedures</td><td>Q4 2015</td><td></td></tr>
<tr><td>7. CCA will continue reconciliation of the 820 XML report and the Carrier Payment Report, which is a report that the customer service and business operations vendor produces for CCA to send to carriers.</td><td>Ongoing</td><td>Ongoing</td></tr>
<tr><td colspan="3">Plan for Monitoring and Validation: Perform monthly reconciliation process with all available data sources, which requires management review and approval, to ensure accurate payments are made to carriers.</td></tr>
<tr><td colspan="3">Responsible Entity or Individual: Director of Finance, Director of Accounting, Senior Financial Analyst</td></tr>
</table>

Appendix C – Corrective Action Plan (continued)

Audit Report Corrective Action Plan		
Issue Title: Finding #2014-05 – Governance		
Audit Report Recommendation: Implement and maintain formal governance principles including ethics, conflicts of interest standards, accountability and transparency, and disclosure of financial interests.		
Description of Remediation: The Health Connector will work to develop an addendum to the Board of Director rules to further clarify the Board's conflict of interest requirements		
Milestone	**Target Date**	**Completion Date**
1. Draft addendum to Board rules	July 2015	
2. Conduct reviews and request feedback from appropriate external entities	August 2015	
3. Seek Board approval/adoption of addendum	September 2015	
Plan for Monitoring and Validation: n/a		
Responsible Entity or Individual: General Counsel		

Audit Report Corrective Action Plan		
Issue Title: Finding #2014-06 – Policies and Procedures (Internal Controls)		
Audit Report Recommendation: Regularly review and analyze the adequacy of the elements comprising the authority's control framework, and make timely adjustments to strengthen key control activities.		
Description of Remediation: The Health Connector will formalize the regular review of policies and procedures.		
Milestone	**Target Date**	**Completion Date**
1. Implement annual review of customer-facing policies and procedures	April 2015 & annually prior to open enrollment	April 2015
2. Implement annual review of internal and financial policies and procedures	September 2015	
Plan for Monitoring and Validation: n/a		
Responsible Entity or Individual: Deputy Executive Director, Strategy & External Affairs, Chief Operating Officer, General Counsel		