KPMG
cutting through complexity

Commonwealth Health Insurance Connector Authority

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

March 24, 2016

FINAL REPORT

For the Period January 1–June 30, 2015

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

Contents

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

March 24, 2016

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 2015-02, related to the Commonwealth Health Insurance Connector Authority's (CCA) compliance with Centers for Medicare and Medicaid Services (CMS) Rule 9957 (45 C.F.R. §155) requirements. We conducted our test work during the period December 9, 2015 through March 24, 2016 and our results, reported herein, are for the period January 1–June 30, 2015.

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 recommendations based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings 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, and recommendations as they relate to the performance audit.

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 risk of ineffective oversight and program integrity practices.

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

This report is intended solely for the information and use of the CCA 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

In this Executive Summary, we provide the Commonwealth Health Insurance Connector Authority (CCA) with the background, objective, scope, approach, and summary of results and findings related to this performance audit. The remainder of this document details the audit methodology as well as the findings and recommendations that resulted from our testwork.

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 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 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 portions of its operations to private vendors (e.g., customer service and call center operations, select financial processing activities, some IT development and maintenance, and SHOP operations) and relies on other public agencies and their private vendors to provide other key services relating to core IT systems.

Objective

The objective of this audit was to assess CCA's compliance with 45 C.F.R. § 155 regulations for the period January 1–June 30, 2015.

KPMG LLP (KPMG) was responsible for performing the programmatic audit in accordance with Government Auditing Standards (GAS) and preparing a written report communicating the results of the audit, including relevant findings and recommendations. These results may include deficiencies in internal controls that are significant within the context of the objective 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 may have been identified as a result of this engagement.

Executive Summary (continued)

Scope

Program areas subject to audit included processes and controls over:

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

Approach

The audit was conducted in the following phases: Audit Planning, Information Gathering and Analysis, Audit Execution, and Validation 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.

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 testwork.

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 developing draft findings and recommended improvements, validating the draft findings with CCA process owners, and discussing CCA's plans for corrective action.

Summary of Results and Findings

As a result of our audit procedures, KPMG identified the following findings relating to specific controls and processes. These are summarized on the following two pages. Those findings that appear to have been remediated have been designated as such.

In addition, these findings are explained in greater detail and organized by condition, criteria, cause, effect, and recommendation in the Findings and Recommendations section of this report. CCA's response to each of these findings is found in the Management's Response section of the report.

Executive Summary (continued)

Finding #2015-01 – Oversight of Call Center Background Checks, Training Requirements, and Member Suspense Account Management

CCA did not provide sufficient oversight of a supporting vendor in the following two areas:

- Proactive monitoring of Call Center employee background check completion and satisfaction of training certification/recertification requirements **(Remediated).**
- Review of vendor management regarding member premium payments in suspense including tolerances for transaction aging and population volume.

Finding #2015-02 – IT Governance – Intergovernmental Agreement

For part of the time period under audit, CCA did not have written agreements regarding the oversight of the security function in the HIX system:

- CCA is part of a consortium of Commonwealth agencies, which perform control activities over select IT privacy and security functions. This relationship, and the associated responsibilities, were not memorialized in a formal agreement, outlining specific tasks which CCA is responsible for and those which CCA relies on the other Commonwealth agencies to perform for four months of the six-month audit period **(Remediated).**
- Through this consortium, CCA relies on a third-party service provider to perform key control activities in support of the successor HIX system. CCA is not a party to the contract with the third-party service provider, limiting CCA's ability to exercise oversight of the service provider's activities **(Remediated).**

Finding #2015-03 – Corporate Governance – Reliance on Commonwealth Regulations to Satisfy Formal Governance Policy/Procedure Requirements

While CCA has adhered to Commonwealth laws and regulations since its creation, including state ethics and conflicts of interest laws and requirements for board member disclosures of conflicts and financial interests, CCA did not adhere to federal regulations requiring adoption of formal, publicly available governance policies by state-based Exchanges. CCA relied on certain procedures under Commonwealth laws and regulations such as exception-based reporting of board members' conflicts and financial interests and annual distribution of state ethics laws as opposed to having a specific code of conduct policy in place to address the federal requirements **(Remediated).**

Finding #2015-04 – IT Security and Privacy Controls – Access Administration, Business Continuity, and Data Loss Prevention

KPMG testing identified exceptions to Exchange IT privacy and security controls in the areas of access management, business continuity planning, and data loss prevention.

- Access appears to have been granted to users that may not require access. 94 users who do not appear to have logged into the HIX system had active HIX IDs. 73 users who had not logged into the HIX system in over 180 days still maintained active HIX IDs.
- During testing, two users were found to possess two active IDs to the HIX system. Two vendor users that left the HIX-IES project, subsequently returned, but did not have their original HIX system IDs

terminated prior to being granted new IDs. This resulted in both users having two active IDs to the HIX system. CCA did subsequently remove the initial IDs for both users.

- Access to the CCA Appeals database (Database), which houses PII/PHI, does not appear to have been adequately controlled. The Database is located on a shared drive where all users with domain access have been granted "read" and "execute" permission. While the data is encrypted, and administrative access is restricted to four users, all users with domain access can copy and transfer the encrypted data **(Remediated).**
- MassIT uses Voltage e-mail encryption service and Transport Layer Security (TLS) to mitigate the risk of data loss prevention. However, there is no technical, preventive control to ensure sensitive information is not transmitted externally via e-mail should the user neglect or choose to ignore the use of Voltage.

Finding #2015-05 Verification of Eligibility Determinations

As a result of our sample tests of CCA's processes for manual verifications of eligibility applications, we identified the following exceptions:

- Instances where applicants were notified of a requirement to verify certain categories of attested information, including residency and income, but did not submit required documentation within the required 90-day verification period **(Partially Remediated).**
- Instances where applicants submitted required documentation for residency, income, and incarceration status, but were not verified within the required 90-day verification period **(Partially Remediated).**
- Instances where applicants who had been automatically verified as not incarcerated were erroneously sent notices requiring them to manually verify their non-incarceration status.

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 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 annual programmatic audit to CMS; make public a summary of the results of the external audit; and develop and inform CMS of a corrective action plan.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 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 11-member Board, which includes four ex-officio members: the Secretary of Health and Human Services, the Secretary of Administration and Finance, the Commissioner of Insurance, and the Executive Director of the Group Insurance Commission. The governor appoints an actuary, a health economist, a representative of small business, and an underwriter. The Attorney General appoints an employee health benefits specialist, a representative of health consumers, and a representative of organized labor. The Health Connector Board composition and responsibilities are defined by Commonwealth statute. Within the audit period, key changes include transition of the Board Chair role to the Secretary of Health and Human Services (HHS), previously held by the Secretary of Administration and Finance, and elevation of Medicaid agency representation from the Director of MassHealth to the Secretary of EOHHS. 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.

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 January 1, 2015. CCA contracts certain operations to private vendors (customer service, call center, and SHOP 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.

Objective, Scope, and Approach

Objective, Scope, and Approach

Objective

KPMG was engaged to perform a programmatic audit in accordance with both 45 C.F.R. §155.1200(c) and Government Auditing Standards (GAS) to assess the Commonwealth Health Insurance Connector Authority's compliance with 45 C.F.R. §155 regulations for the six months ended June 30, 2015.

KPMG was responsible for preparing a written report communicating the results of the audit, including relevant findings and recommendations. These results should 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 GAS, 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 six months ended June 30, 2015 and our procedures were limited to the following areas:

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, and 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.	» 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. » Select samples to test design and effectiveness of key controls and document any findings and recommendations.	» Internal control documentation—such as policies and procedures for new members, terminations, status changes, etc. » Reconciliations with QHP issuers and CMS
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.

Objectives, Scope, and Approach (continued)

Audit Area	Representative Tasks	Sample Documentation
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, observed processes, conducted walkthroughs, and held interviews with CCA management and key process owners who perform select 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. KPMG conducted Tests of Design to consider whether the control, individually or in combination with other controls, is capable of effectively preventing or detecting and correcting noncompliance as well as Tests of Operating Effectiveness to consider whether the control was implemented and operated in a manner appropriate to accomplish the control objective. 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.

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 effectively conduct the audit, manage stakeholder expectations, and execute communications protocols from the outset.

A formal Project Kickoff Meeting was held to introduce key CCA stakeholders to the KPMG engagement team and confirm our mutual understanding of the audit scope and objectives. During the course of the audit, regular status meetings were also conducted with the CCA Chief Operating Officer and the principal CCA liaison, and a project "mid-point" in-progress observation session with the CCA Executive Director was also conducted.

Objectives, Scope, and Approach (continued)

Information Gathering and Analysis: Following Audit Planning, this phase involved further developing our understanding of CCA's activities, processes and controls for the audit period and developing our audit approach. 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 relevant 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 and corresponding key procedures.

Audit Execution: This phase consisted of finalizing 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 control catalog
- Reviewing and testing safeguards over member eligibility determinations, and appeals
- 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 findings and recommendations for improvement, and obtaining CCA's plans for corrective action. Our detailed findings are documented further below.

Objectives, Scope, and Approach (continued)

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 GAS 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.

Results – Findings and Recommendations

Results – Findings and Recommendations

Introduction

In accordance with GAS, KPMG prepared this report communicating the results of the completed performance audit, including relevant findings 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 findings whether as a result of new information, future events, or otherwise. Should additional documentation or other information become available that impacts the findings reached in our deliverable, we reserve the right to amend our findings and summary documents accordingly.

Summary of Findings

Our detailed 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. GAS (i.e., the Government Accounting Office 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.

Results – Findings and Recommendations (continued)

Finding #2015-01–Oversight of Call Center Background Checks, Training Requirements, and Member Suspense Account Management

Condition: CCA did not provide sufficient oversight of a supporting vendor in the following two areas:

- Proactive monitoring of Call Center employee background check completion and satisfaction of training certification/recertification requirements
- Review of vendor management regarding member premium payments in suspense including tolerances for transaction aging and population volume

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.

Cause: CCA did not have sufficient procedures to meaningfully ensure vendor satisfaction of Call Center Customer Service Representative (CSR) training requirements, instead relying upon vendor self-reporting by exception and unspecified tolerance parameters for overseeing timely management of member suspense account balances**.**

Effect: Failure to periodically oversee vendor activities may lead to shortcomings in internal control.

Recommendation: Consider strengthening current oversight procedures by:

- Performing regular periodic reviews of a sample of new Call Center CSR employees to verify background checks have been appropriately completed and initial training requirements have been met **(Note: Condition has been remediated)**.
- Formalizing the acceptable tolerances for suspense transaction volume and aging for processing customer premium payments in suspense to help ensure timely transaction processing by the servicing vendor. Document and educate CCA finance department personnel such that all departmental members are capable of providing meaningful oversight of this area.

Finding #2015-02–IT Governance – Intergovernmental Agreement

Condition: For part of the time period under audit, CCA did not have written agreements regarding the oversight of the security function in the HIX system:

- CCA is part of a consortium of Commonwealth Agencies, which perform control activities over select IT privacy and security functions. This relationship, and the associated responsibilities, were not memorialized in a formal agreement, outlining specific tasks which CCA is responsible for and those which CCA relies on the other Commonwealth Agencies to perform for four months of the six-month audit period.
- Through this consortium, CCA relies on a third-party service provider to perform key control activities in support of the successor HIX system. CCA is not a party to the contract with the third-party service provider, limiting CCA's 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: CCA entered into an intergovernmental agreement with the Massachusetts Office of Information Technology (MassIT), the Executive Office of Health and Human Services, and the Office of Medicaid on May 6, 2015. CCA also entered into an intergovernmental agreement with MassIT effective November 13, 2015 that governs the monitoring of privacy and security controls for the HIX system. **(Note: Condition has been remediated).**

Finding #2015-03–Corporate Governance – Reliance on Commonwealth Regulations to Satisfy Formal Governance Policy/Procedure Requirements

Condition: While CCA has adhered to Commonwealth laws and regulations since its creation, including state ethics and conflicts of interest laws and requirements for board member disclosures of conflicts and financial interests, CCA did not adhere to federal regulations requiring adoption of formal, publicly available governance policies by state-based Exchanges. CCA relied on certain procedures under Commonwealth laws and regulations such as exception-based reporting of board members' conflicts and financial interests and annual distribution of state ethics laws as opposed to having a specific code of conduct policy in place to address the federal requirements.

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, instead relying on Massachusetts 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. **(Note: Condition has been remediated with implementation of Code of Ethics as of October 2015.)**

Finding #2015-04–IT Security and Privacy Controls – Access Administration, Business Continuity, and Data Loss Prevention

Condition: KPMG testing identified exceptions to Exchange IT privacy and security controls in the areas of access management, business continuity planning, and data loss prevention.

- **Access Management.** Access appears to have been granted to users that may not require access. 94 users who do not appear to have logged into the HIX system had active HIX IDs. 73 users who had not logged into the HIX system in over 180 days still maintained active HIX IDs.
- **Access Management.** During testing, two users were found to possess two active IDs to the HIX system. Two vendor users that left the HIX-IES project, subsequently returned, but did not have their original HIX system IDs terminated prior to being granted new IDs. This resulted in both users having two active IDs to the HIX system. CCA did subsequently remove the initial IDs for both users.
- **Access Management.** Access to the CCA Appeals database (Database), which houses PII/PHI, does not appear to have been adequately controlled. The Database is located on a shared drive (R:\Legal\Appeals\Databases) where all users with domain access have been granted 'read' and 'execute' permission. While the data is encrypted, and administrative access is restricted to four users, all users with domain access can copy and transfer the encrypted data.
- **Data Loss Prevention.** MassIT uses Voltage e-mail encryption service and Transport Layer Security (TLS) to mitigate the risk of data loss prevention. However, there is no technical, preventive control to ensure sensitive information is not transmitted externally via e-mail should the user neglect or choose to ignore the use of Voltage.

Criteria: 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: CCA does not have sufficient procedures in place to oversee elements of the required IT Privacy and Security control suite including access management, business continuity planning and testing, and data loss prevention.

Effect: Vulnerabilities in controls may be exploited by internal and external adversaries to gain unauthorized access to PII and PHI. Data and system breaches can result in operational downtime for CCA, reputational loss, and financial loss due to fines and corrective measures.

Recommendation: Take additional steps to address these issues by updating governing policies/plans as necessary, to help ensure clear roles, oversight, and accountability of:

- Access Management
- Data Loss Prevention.

Additional recommendations are as follows:

- **Access Management.** Implement an automatic disablement of an HIX ID that has not been used for 180 days. Alternately, CCA could strengthen the compensating control for performing monthly attestations of users with over 180 days of inactivity. These reports should require that management respond to the attestation request to actively approve the users on the list. Users not approved by

management as part of the attestation reporting should be removed from the HIX system. The monthly reports and responses from management should be saved for auditing purposes.

- **Access Management**. Periodically review and approve who should have access to the CCA Appeals database and the associated password. This review could happen at the same time that the database password is reset and distributed to those with a clear business or security need. The procedure should include renewing the password when an individual changes roles within CCA and no longer requires access, leaves the organization, or on a periodic basis, whichever happens first. Additionally, the shared drive permissions should be reduced to grant access to only the four specific users with the authorized approval to use the Appeals Database. (**Note: Condition has been remediated as of March 2016.)**
- **Data Loss Prevention.** Implement a system to prevent violations in e-mail communication policies, e.g., a Data Leak Prevention tool, to secure data in the case employees forget to use the "Secure" e-mail encryption solution.

Finding #2015-05–Verification of Eligibility Determinations

Condition: As a result of our sample tests of CCA's processes for manual verifications of eligibility applications, we identified the following exceptions:

- Instances where applicants were notified of a requirement to verify certain categories of attested information, including residency and income, but did not submit required documentation within the required 90-day verification period.
- Instances where applicants submitted required documentation for residency, income and incarceration status, but were not verified within the required 90-day verification period.
- Instances where applicants who had been automatically verified as not incarcerated were erroneously sent notices requiring them to manually verify their nonincarceration status.

Criteria: 45 CFR §155.315 requires the Exchange to make reasonable efforts to identify and address the causes of inconsistencies identified through verification of application data against electronic data sources (e.g., residency, income, citizenship status, lawful presence of noncitizens, incarceration status, American Indian/Alaska Native status). Specifically, these efforts include notifying the applicant of the inconsistency and allowing 90 days to provide satisfactory documentation to resolve the inconsistency. If the Exchange remains unable to verify the inconsistency after 90 days, it must determine eligibility based on available data sources and notify the appellant it was unable to verify the attestation.

Cause: These 90-day verifications exceptions appear to be attributable to gaps in HIX system functionality. Prior to February 2015, CCA did not appear to have full system functionality for its customer service personnel to verify documents submitted by applicants and maintained in a separate document work flow system, which resulted in delays in verifying applicants' supporting documentation on a timely basis. CCA did receive limited system functionality to support this activity in February 2015, and received full functionality in May 2015. Additionally, CCA did not appear to activate existing functionality within the HIX system to close the 90-day verification period in situations where applicants failed to provide documentation. The erroneous request to verify non-incarceration status was generated by a system error for incarceration status verifications.

Results – Findings and Recommendations (continued)

Effect: Applicants may receive incorrect eligibility determinations, based on inconsistent or inaccurate source data, incorrect incarceration status notifications, or may not receive accurate eligibility determinations within the 90-day verification period.

Recommendation: Test and implement system functionality to allow for timely verification of applicant-provided documentation of self-attested information and identification of applications, which have exceeded the 90-day period. **(Note: CCA has implemented the verification functionality within the HIX system as of May 2015 and is currently testing functionality for expiring the 90-day verification period as of March 2016. Regarding incorrect incarceration status notifications, CCA uses a workaround to identify and verify, on a daily basis, any affected cases).**

Management's Response and Corrective Action Plan

January 1, 2015 – June 30, 2015 Programmatic Audit

Management Response and Corrective Action Plans

March 28, 2016

Management's Response and Corrective Action Plan

Summary

The Health Connector recognizes the independent auditor's analysis of our programmatic procedures and controls for the period January 1 - June 30, 2015. We have reviewed the report and take seriously all findings and recommended remediation.

The Health Connector management team will work with staff; partner agencies and vendors to implement many of the audit recommendations as we work to improve operations enhance our technology platform and continue to expand health insurance coverage throughout Massachusetts.

Finding #2015-01 – Oversight of Call Center Background Checks, Training Requirements and Member Suspense Account Management

We acknowledge a more robust method of managing member premium payments in suspense, including tolerances for transaction ageing and population volume is prudent. Documentation will be created that explains how to successfully monitor activity in suspense accounts and Finance and Accounting staff will be trained on the process and demonstrate competency with the activity. The timeline for completion is April 2016.

Finding #2015-04 – IT Security and Privacy Controls – Access Administration, Business Continuity and Data Loss Prevention

While full automation of disablement of HIX ID is not an available solution at this time, policies and procedures for manual disablement will be reviewed and strengthened to ensure this compensating control is adequate. Working with systems integration, business operations vendor the Executive Office of Health and Human Service and other partners, the policies and procedures will be modified to ensure no account remains active beyond 180 days of user inactivity.

We will evaluate potential options for Data Leak Prevention, taking into account industry standards and practices.

Finding #2015-05 – Verification of Eligibility Determinations

While the Health Connector currently processes verifications submitted by members, the Health Connector is conducting testing in order to resolve inconsistencies for individuals who have not submitted manual verification. Based on the success of testing, the Health Connector will begin resolving inconsistencies in April 2016 for individuals who did not submit manual verification.

There is an ongoing communication plan to alert enrolled members who have not submitted required documentation that they must comply or risk having their coverage change or end. The communication plan includes direct member outreach by letter, phone and email to the impacted population. Training has been provided to Customer Service Representatives and document processing staff in order to provide updates on the member impact of failure to send eligibility verification documents.

Management's Response and Corrective Action Plan

Audit Report Corrective Action Plan		
Issue Title: Finding #2015-01 – Oversight of Call Center Background Checks, Training Requirements and Member Suspense Account Management		
Audit Report Recommendation: • Perform regular periodic reviews of a sample of new call center customer service representatives to verify background checks have been appropriately completed and initial training requirements have been met • Formalize the acceptable tolerances for suspense transaction volume and aging for processing customer premium payments in suspense to help ensure timely transaction processing by the servicing vendor • Document and educate Health Connector Finance and Accounting personnel such that appropriate department members are capable of providing meaningful oversight of this area		
Description of Remediation: • The Health Connector will implement policies and procedures to ensure all new call center hires have undergone background checks and training by obtaining from the call center vendor documentation that background checks and training have been completed • Documentation will be created that explains how to successfully monitor activity in suspense accounts • Finance and Accounting staff will be trained on the process and must demonstrate competency with the activity		
Milestone	**Target Date**	**Completion Date**
1. Conduct regular periodic reviews of new Cell Center CSR employees to verify background checks and completion of training.		March 2016
2. Document process to monitor payments in suspense.	April 2016	
3. Train finance department staff to monitor payments in suspense.	April 2016	
Plan for Monitoring and Validation: Background Checks and completion of training requirements will be completed with each class of new hires. Appropriate Finance and Accounting staff will be trained on how to effectively monitor premium payments in suspense.		
Responsible Entity or Individual: Chief Operating Officer and Director of Accounting		

Audit Report Corrective Action Plan
Issue Title: Finding #2015-04 – IT Security and Privacy Controls – Access Administration, Business Continuity and Data Loss Prevention
Audit Report Recommendation: Take additional steps to address these issues by updating governing policies/plans as necessary, to help ensure clear roles, oversight, and accountability of: • Access Management • Data Loss Prevention Additional recommendations are as follows: • **Access Management.** Implement an automatic disablement of a HIX ID that has not been used for 180 days. Alternately, CCA could strengthen the compensating control for performing monthly attestations of users with over 180 days of inactivity. These reports should require that management respond to the attestation request to actively approve the users on the list. . Users not approved by management as part of the attestation reporting should be removed from the HIX system. The monthly reports and responses from management should be saved for auditing purposes. • **Access Management**. Periodically review and approve who should have access to the CCA Appeals database and the associated password. This review could happen at the same time that the database password is reset and distributed to those with a clear business or security need. The procedure should include renewing the password when an individual changes roles within CCA and no longer requires access, leaves the organization, or on a periodic basis, whichever happens first. Additionally, the shared drive permissions should be reduced to grant access to only the 4 specific users with the authorized approval to use the Appeals Database. Note: Condition has been remediated as of March 2016. **Data Loss Prevention.** Implement a system to prevent violations in e-mail communication policies (*e.g.,* a Data Leak Prevention tool) to secure data in the case employees forget to use the "Secure" e-mail encryption solution.

Description of Remediation

Access Management: While full automation of disablement of HIX ID is not an available solution at this time, policies and procedures for manual disablement will be reviewed and strengthened to ensure this compensating control is adequate. Working with systems integration, business operations vendor the Executive Office of Health and Human Service and other partners the policies and procedures will be modified to ensure no account remains active beyond 180 days of user inactivity.

Data Loss Prevention: Evaluate potential options for Data Leak Prevention, taking into account industry standards and practices and available solutions.

Milestone	Target Date	Completion Date
1. Updated domain security for the CCA Appeals database to ensure only authorized users had access		March 2016
2. Update Access Management policies and procedures to ensure disabling of HIX accounts prior to 180 days of inactivity	April 2016	
3. Conduct analysis of Data Leak Prevention tools and make a recommendation to CCA Leadership regarding implementation of tool	May 2016	
4. Implement recommended solution for Data Leak Prevention, if any.	June 2016	

Plan for Monitoring and Validation: Review, on a quarterly basis, the monthly activities for HIX ID disablement. Validation procedures for Data Leak Prevention will vary based on implemented solution.

Responsible Entity or Individual: Chief Information Officer

Audit Report Corrective Action Plan

Issue Title: Finding #2015-05 – Verification of Eligibility Determinations

Audit Report Recommendation: Test and implement system functionality to allow for timely verification of applicant-provided documentation of self-attested information and identification of applications which have exceeded the 90 day period.

Description of Remediation: While the Health Connector currently processes verifications manually submitted by members, the Health Connector is conducting testing in order to resolve inconsistencies for individuals who have not submitted verification. Based on the success of testing, the Health Connector will begin resolving inconsistencies in April 2016 for individuals who did not submit manual verification. There is an ongoing communication plan to alert enrolled members who have not submitted required documentation that they must comply or risk having their coverage change or end. The communication plan includes direct member outreach by letter, phone and email to the impacted population. Training has been provided to customer service representatives and document processing staff in order to provide updates on the member impact of failure to send eligibility verification documents.

Milestone	Target Date	Completion Date
1. Implement the verification functionality within the HIX system		May 2015
2. Remediate the system error regarding incorrect incarceration status notifications in a future system update	June 2016	
3. Begin to implement functionality for expiring the 90 day verification period	April 2016	

Plan for Monitoring and Validation: End-to-end testing is being conducted and overseen by a cross-functional team at the Health Connector and includes participants from all impacted project entities and subject matter experts. In addition to testing, the Health Connector has been closely monitoring the population with remaining inconsistencies and will track eligibility and enrollment changes that occur when inconsistencies are resolved as a result of the system redetermination triggered by the expiration of the 90 days.

Responsible Entity or Individual: Chief Operations Officer and Chief Information Officer

Appendix A – List of Interviewed Personnel

Appendix A – List of Interviewed Personnel

Name	Title
Alex Muggah	Director of Reporting
Andrew Egan	Assistant General Counsel
Andy Graham	Product Implementation Manager
Ashley Hague	Deputy Executive Director, Strategy and External Affairs
Brian Schuetz	Director, Program and Product Strategy
David Mack	QA Manager
Dom DiVito	Director of Accounting
Ed DeAngelo	Assistant General Counsel
Elba Mendez	Implementation Manager
Elliot Gorman	System Architect
Jason Hetherington	Chief Information Officer
Jen Bullock	Director of Member Services
JoAnna Waterfall	Operations Manager
Kari Miller	Director of Finance
Kevin McDevitt	IT Implementation
Laura Solorzano	Quality and Training Manager with Dell
Lauren Ripley	Assistant General Counsel
Louis Gutierrez	Executive Director
Maria Joy	External Affairs Associate
Marissa Woltmann	Associate Director, Policy and Implementation Specialist
Merritt McGowan	Assistant General Counsel
Michael Piantanida	Director of IT Implementation
Nancy Stehfast	Appeals Unit Manager
Nelson Teixeira	Associate Director of Member Services
Nia Salcedo	Member Service Associate
Niki Conte	Associate Director of Public Outreach and Education
Nupur Gupta	Financial Analyst
Patricia Jennings	Associate Director of Business Development
Sam Osoro	Financial Analyst
Samuel Affram	Senior QA Analyst
Stacy Halloran	Senior Accountant
Tamara Pitts	Contract Manager
Tatsiana Murauyeva	Senior Manager of Operations

Appendix A – List of Interviewed Personnel (continued)

Name	Title
Terri Shine	Director of Human Resources
Valerie Berger	Senior Manager, Member Policy
Vicki Coates	Deputy Executive Director, Chief Operating Officer
William Karger	Manager of Sales and Client Services
Geoff Potts	Customer Delivery Executive
Basudeb Bhaumik	Senior Leader
Manek Awasty	Call Center Senior Leader
Sean Warner	Call Center Manager
Jon Williams	Call Center Manager
Ashley Manning	Training Manager
Rajesh Narayanan	Back Office Senior Leader

Appendix B – Glossary of Terms

Appendix B – Glossary of Terms

ACA	Patient Protection and Affordable Care Act
APTC	Advance Premium Tax Credit
BCP	Business Continuity Plan
CCA	Commonwealth Health Insurance Connector Authority
CFR	Code of Federal Regulations
CMS	Centers for Medicare and Medicaid Services
CSR	Cost Sharing Reduction
GAS	Government Auditing Standards
HIX	Health Information Exchange
HHS	U.S. Department of Health and Human Services
MassIT	Massachusetts Office of Information Technology
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