KPMG

# Commonwealth Health Insurance Connector Authority

**Performance Audit of Centers for Medicare and Medicaid Services Rule 9957 Requirements**

FINAL REPORT
For the period July 1, 2015–June 30, 2016

July 14, 2017

kpmg.com

# Contents

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

Telephone +1 617 988 5706
Fax +1 617 687 2589
Internet www.us.kpmg.com

July 14, 2017

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 (the 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 testwork during the period March 7, 2017 through July 14, 2017, and our results, reported herein, are for the period July 1, 2015–June 30, 2016.

We conducted this 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 and 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 the Audit 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 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 that 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 section, we provide a summary of the detailed report to follow on the Commonwealth Health Insurance Connector Authority's (CCA) background, objective, scope, approach, and summary of results and findings related to this 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 (SBMs) to engage an independent qualifying auditing entity that follows generally accepted government auditing standards to perform an annual independent external audit. The SBM must ensure that the 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 effective 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), and administers 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 (IT), and 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 July 1, 2015–June 30, 2016.

KPMG LLP (KPMG) was responsible for performing the 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.

# Scope

Program areas subject to audit included processes and controls over:

- IT Privacy and Security
- Eligibility
- Enrollment
- Financial Processing
- Oversight and Program Integrity Standards
- Qualified Health Plan Certification
- General Exchange functions, including:
  - Call center
  - HR and training
  - Data and records management
  - 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 select 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 three pages. Those findings that appear to have been remediated or are findings that are repeated from the June 1, 2016 report 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.

## Finding #2016-01 – Timely contract completion

CCA did not obtain timely contract signatures for multiple entities supporting Connector operations, namely, Certified Application Counselors (CAC) organizations; Navigator organizations; Broker Enrollment Assisters, and the call center.

## Finding #2016-02 – Intergovernmental monitoring

CCA did not adequately monitor that all Minimum Acceptable Risk Standards for Exchanges (MARS-E) control functions were operating effectively at the Exchange's key vendors and intergovernmental partners in the following MARS-E areas:

— Access controls

— Audit and accountability

— Contingency planning

— Security assessment and authorization

— Identification and authentication

— System and communications protection

## Finding #2016-03 – Inactive Account Monitoring

The in-scope applications do not automatically disable inactive CCA accounts. Periodic reviews over inactive accounts under CCA's purview are not adequately performed, as certain inactive accounts were not disabled timely.

Additionally, multifactor authentication was not implemented during the period in scope and password parameters employed did not meet MARS-E requirements.

## Finding #2016-04 – MARS-E Compliance

While certain user activity is audited and logged at the various systems, systems are not configured to audit all events as required by MARS-E controls including all use of administrator privileges, security policy modifications, and user account management activities. Also, while audit logs may be consulted when required to investigate events, there are no formal periodic reviews conducted to help identify potential inappropriate or unusual activity.

## Finding #2016-05 – Continuity Planning

The CCA's Continuity Planning measures do not:

— Contain procedures to address potential failures for systems owned and operated by other key stakeholders to help ensure appropriate coordination for the continued operations of as well as movement of data through the Exchange

— Define measures for user access to restored systems from their Disaster Recovery sites.

— Address how the recovery of the information systems is performed.

## Finding #2016-06 – Annual Attestation Report

The Exchange does not address all systems with a role in the processing or retention of sensitive data within its System Security Plan (SSP). For those systems that were included within the Exchange's Annual Attestation Report (AAR) over compliance with the SSP, multiple failed controls were identified regarding adherence to the following MARS-E requirements:

— Audit and accountability

— Identification and authentication

— System and information integrity

## Finding #2016-07 – Verification of Eligibility Determination

CCA uses manual verifications to resolve inconsistencies between application and electronic data. KPMG's review of this process identified the following:

— Instances where applicants were notified of their requirement to provide support for attested information (e.g., lawful presence, residency, income), but failed to submit the required documentation timely

— Instances where CCA either did not follow up with these applicants to redetermine eligibility or followed up with the applicants to redetermine eligibility after the 90-day verification period had elapsed.

## Finding #2016-08 – Document Retention

Our review of CCA's processes for eligibility determination and member enrollments identified four instances in which the call center vendor could not locate the supporting documentation provided in response to a Request for Information (RFI).

# Background

# Background

The 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 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 an SBM to engage an independent qualifying auditing entity that follows generally accepted government auditing standards to perform an annual independent external programmatic audit. The SBM must ensure that the 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 Audit to CMS, make public a summary of the results of the external audit, and develop and inform CMS of a corrective action plan.

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 (HHS), 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 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 Executive Office of Health and Human Services (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 IT). CCA employed approximately 67 fulltime-equivalent personnel as of June 30, 2016. CCA contracts certain operations to private vendors (customer service, call center, and SHOP operations; select financial processing activities; and 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 an Audit in accordance with both 45 C.F.R. §155.1200(c) and GAS to assess the CCA's compliance with 45 C.F.R. §155 regulations for the fiscal year ended June 30, 2016.

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 fiscal year ended June 30, 2016 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.<br>— Conduct process walk-throughs to identify and classify key controls for testing, including:<br>– Personally identifiable information (PII) and the confidentiality, disclosure, maintenance, and use of information<br>– Incident management/reporting procedures<br>– Data loss and security breach incidents.<br>— Select samples to test design 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<br>— Reports—incident reporting, user access, etc. |

| Audit area | Representative tasks | Sample documentation |
|---|---|---|
| **Eligibility** | — Interview process owners and review process control documentation.<br>— Conduct process walk-throughs to identify and classify key controls for testing including verification of basic applicant data, MAGI eligibility, account update procedures, exemption requests, and reporting to federal and state agencies.<br>— Select samples to test design 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.<br>— Management reports—applications and eligibility determinations activity<br>— Member applications—paper, electronic |
| **Enrollment** | — Interview process owners and review process control documentation.<br>— Conduct process walk-throughs to identify safeguards over enrollment actions such as:<br>– Enrolling individuals in QHP offerings<br>– Generating and correctly populating Forms 834<br>– Reporting.<br>— 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.<br>— Reconciliations with QHP issuers and CMS |
| **Financial Processing** | — Interview financial process owners and review process control documentation.<br>— Conduct process walk-throughs to review and understand the calculations and reporting of QHP premiums and payments, carrier payment reconciliation activity, suspense payments, and related reporting.<br>— Select samples to test design and effectiveness of key controls and document any findings and recommendations. | — Internal financial policies and procedures<br>— Financial reports—such as billing reports, FMS enrollment reports, carrier payment reconciliations, etc. |

| 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, HR and training, and data/records maintenance.<br>— Review process control documentation for these functions.<br>— Conduct process walk-throughs to identify and classify key controls for testing.<br>— 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<br>— Customer Service Representative performance reports<br>— CCA employee training records |

KPMG reviewed documents, performed inquiries, observed processes, conducted walk-throughs, reviewed applicable third-party reports, and held interviews with CCA management and key process owners who perform select program functions.

KPMG identified controls through walk-throughs 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 where relevant 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), the 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.

Additionally, CCA directed that the Appeals area (Subpart F) not be tested in the course of our procedures. This is therefore noted as a scope limitation for the Audit.

# 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.

## Audit Planning

The first phase of this project involved embedding 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.

## 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 MARS-E control catalog

— Reviewing and testing safeguards over member eligibility determinations

— 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 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 below in the Results section.

# Procedures and methodology

We reviewed the requirements of 45 C.F.R. §155 to identify 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 walk-through procedures – We reviewed CMS Final Rule 9957 and associated regulations under 45 C.F.R. §155 to identify compliance requirements subject to this Audit. KPMG worked with CCA management to identify process owners for key activities and performed interviews and walk-throughs 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 select controls.

— Sample testing approach – In support of testing the design and effectiveness of select 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 the Audit objectives. When fraud risk factors were identified that the engagement team believed were significant within the context of the 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 Audit and relates not only to planning the Audit but also to evaluating evidence obtained during the 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

In accordance with GAS, KPMG prepared this report communicating the results of the completed 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 – Explains the requirements related to the issue and a determination of how criteria and processes should be executed

— Cause – 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-based 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 Accountability 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.

## Finding #2016-01 – Timely Contract Completion

**Condition:** CCA did not obtain timely contract counter-signatures for multiple supporting Connector operations, namely:

— Counter-signatures for five navigator organization contracts were not obtained prior to the effective date of the contract. Signature of CCA's executive director was obtained on August 21, 2015 for all five contracts, while the effective date of each contract was August 1, 2015.

— Seven of ten broker enrollment assister agreements and amendments were not counter-signed by CCA.

— Call center support change orders were not counter-signed before work commenced.

**Criteria:** All navigator and CAC organization contracts are to be reviewed and approved to help ensure critical place services and functions of the CACs as outlined in 45 C.F.R. §155.225 and 45 C.F.R. §155.210. Furthermore, 45 C.F.R. §155.200 requires an Exchange to perform required navigator functions related to oversight and financial integrity, and per 45 C.F.R. §155.205, the Exchange must perform certain activities relating to consumer assistance through a call center.

**Cause:** CCA does not have sufficient procedures in place to ensure timely reviews and approvals of contracts with external service providers such as navigator organizations, CACs, brokers, and the call center.

**Effect:** Services performed without a binding contract may expose CCA to legal and reputational risk.

**Recommendation:** Improve existing policies and controls to help ensure timely review and approval of all Exchange contracts before contract start dates.

## Finding #2016-02 – Intergovernmental Monitoring

**Condition:** CCA did not adequately monitor that control functions performed by the Exchange's key vendors and inter-governmental partners were adequate in areas such as:

— Access controls

— Audit and accountability

— Contingency planning

— Security assessment and authorization

— Identification and authentication

— System and communications protection.

**Criteria:** 45 C.F.R. §155.260 requires the Exchange to execute a contract or agreement with all non-Exchange entities that 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 confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure of personal information stored by the Exchange.

**Cause:** Insufficient procedures to oversee the effectiveness of MARS-E control pertaining to key vendors and intergovernmental partners

**Effect:** Lack of effective controls in these areas may increase the likelihood of a breach of confidentiality, integrity, and availability.

**Recommendation:** Review and enhance existing agreements with intergovernmental partners and service agreements with key vendors to help ensure MARS-E controls are adhered to as required and control weaknesses are addressed timely. Further, CCA should ensure that sufficient monitoring procedures are in place to help ensure that various key vendors and governmental partners adhere to contract requirements.

## Finding #2016-03 – Inactive Account Monitoring

**Condition:** The in-scope applications do not automatically disable inactive CCA accounts. Periodic reviews over inactive accounts under CCA's purview are not adequately performed, as certain inactive accounts were not disabled timely.

Additionally, multifactor authentication was not implemented during the period in scope and password parameters employed did not meet MARS-E requirements.

**Criteria:** 45 C.F.R. §155.260 requires the Exchange to execute a contract or agreement with all non-Exchange entities that 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 confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure of personal information stored by the Exchange.

**Cause:** Sufficient settings for automatic disablement of inactive CCA accounts as well as multifactor authentication are not currently in place.

**Effect:** Unused accounts expand the surface area of attack and may increase the risk of unauthorized and undetected access to the systems. Further, the risk of unauthorized access to privileged and non-privileged accounts may increase due to the lack of the enforcement of strong passwords and multifactor authentication.

**Recommendation:** Implement settings that automatically disable inactive CCA accounts on a periodic basis. CCA should revisit their inactive account review process, and, if necessary revise such that all accounts under their purview that have not been active for a significant period of time are disabled timely.

While CCA has controls in place for authentication, including the use of "whitelisting" and passwords, CCA should further strengthen controls by implementing two-factor authentication and establishing password parameters that adhere to MARS-E requirements.

## Finding #2016-04 – MARS-E Compliance

**Condition:** While certain user activity is audited and logged at the various systems, systems are not configured to audit all events as required by MARS-E controls including all use of administrator privileges, security policy modifications, and user account management activities. Also, while audit logs may be consulted when required to investigate events, there are no formal reviews conducted to help identify potential inappropriate or unusual activity.

**Criteria:** 45 C.F.R. §155.260 requires the Exchange to implement privacy and security standards to ensure the confidentiality, integrity, and availability of the information and to prevent unauthorized or inappropriate access, use, or disclosure of personal information stored by the Exchange.

**Cause:** CCA does not implement audit logging technologies for in-scope systems and does not have a manual or automated process for review.

**Effect:** Unusual or inappropriate activity may not be logged and may remain undetected, which could lead to the undetected breach of information confidentiality and integrity.

**Recommendation:** Take measures to configure systems, firewalls, and routers to generate audit records for specific events, as defined by MARS-E or implement a security incident and event monitoring utility/tool.

## Finding #2016-05 – Continuity Planning

**Condition:** The CCA's Continuity Planning measures do not:

— Contain procedures to address potential failures for systems owned and operated by other key stakeholders to help ensure appropriate coordination for the continued operations of as well as movement of data through the Exchange

— Define measures for user access to restored systems from their disaster recovery sites

— Address how the recovery of the information systems is performed.

**Criteria:** 45 C.F.R. §155.260 requires the Exchange to execute a contract or agreement with all non-Exchange entities that 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 confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure of personal information stored by the Exchange.

**Cause:** Insufficient procedures to oversee elements of MARS-E controls pertaining to intergovernmental service agreements and vendor contracts

**Effect:** Inadequate contingency planning may prevent CCA from maintaining an appropriate level of service over the Exchange and its supporting processes in the case of an emergency.

**Recommendation:** Work with key vendors and intergovernmental parties to:

— Develop and document a comprehensive and integrated contingency plan including all vendors and governmental partners with a role in helping to ensure the continued operations of the Exchange in the event of a disaster at any one of the organization entities involved

— Conduct periodic tests to validate the operating effectiveness of the contingency plan, including safeguards to preserve the privacy, integrity, availability, completeness, and accuracy of data.

## Finding #2016-06 – Annual Attestation Report

**Condition:** The Exchange does not address all systems with a role in the processing or retention of sensitive data within its SSP. For those systems that were included within the Exchange's AAR over compliance with the SSP, multiple failed controls were identified regarding adherence to the following MARS-E requirements:

— Audit and accountability

— Identification and authentication

— System and information integrity

**Criteria:** 45 C.F.R. §155.260 requires the Exchange to execute a contract or agreement with all non-Exchange entities that 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 confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure of personal information stored by the Exchange.

**Cause:** There are insufficient controls in place to oversee elements of MARS-E requirements

**Effect:** Lack of effective controls in these areas may result in an increased likelihood of a breach of confidentiality, integrity, and availability.

**Recommendation:** Address all systems with a role in the processing or retention of sensitive data within its SSP. Outline and address control gaps in CCA's plan of actions and milestones to CMS by establishing a project plan, prioritizing gap remediation by level of risk, and including governance and funding implications as well as a maintenance.

## Finding #2016-07 – Verification of Eligibility Determination

**Condition:** CCA uses manual verifications to resolve inconsistencies between application and electronic data. KPMG's review of this process identified the following:

— Instances where applicants were notified of their requirement to provide support for attested information (e.g., lawful presence, residency, income), but failed to submit the required documentation timely

— Instances where CCA either did not follow up with these applicants to redetermine eligibility or followed up with the applicants to redetermine eligibility after the 90-day verification period had elapsed.

**Criteria:** 45 C.F.R. §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 non-citizens, 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 the available data sources and notify the applicant it was unable to verify the attestation.

**Cause:** The manual verification process employed by CCA is insufficient to capture and resolve the inconsistencies between application and electronic data within the 90-day verification period.

**Effect:** Applicants may receive inappropriate coverage and subsidies pending verification of their eligibility.

**Recommendation:** Review and update the system functionality currently in place for expiring time clocks on outstanding requests, so eligibility redeterminations are performed in a compliant, timely manner. Further, improve the manual oversight process such that inconsistencies are remedied more timely.

## Finding #2016-08 – Document Retention

**Condition:** Our review of CCA's processes for eligibility determination and member enrollments identified four instances in which the call center vendor could not locate the supporting documentation provided in response to a Request for Information (RFI).

**Criteria:** CFR §155.1210 specifies requirements related to the maintenance of records for the Exchange. The State Exchange must maintain and must ensure its contractors, subcontractors, and agents maintain for 10 years, documents and records (whether paper, electronic, or other media) and other evidence of accounting procedures and practices, which are sufficient to do the following: (1) Accommodate periodic

auditing of the State Exchange's financial records; and (2) Enable HHS or its designee(s) to inspect facilities, or otherwise evaluate the State Exchange's compliance with Federal standards. Various type of records are specified, including data and records relating to the State Exchange's eligibility verifications and determinations, enrollment, transactions, appeals, and plan variation certifications. A State Exchange must make all records and must ensure its contractors, subcontractors, and agents must make the records available to HHS, the OIG, the Comptroller General, or their designees, upon request.

**Cause:** Vendor oversight practices appear to be insufficient towards ensuring timely accessibility of member documentation

**Effect:** Documentation that is not maintained or stored in a consistent manner may limit member data accessibility and present challenges for monitoring and quality assurance.

**Recommendation:** CCA should implement QA procedures to provide appropriate vendor oversight of eligibility and enrollment documentation maintenance.

# Management's response and corrective action plan


# July 1, 2015 – June 30, 2016 Programmatic Audit

## Management Response and Corrective Action Plans

**July 14, 2017**

**Management's Responses and Corrective Action Plan**

**Summary**

The Health Connector recognizes the independent auditor's analysis of our programmatic procedures and controls for the period July 1, 2015 – June 30, 2016. 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 #2016-01 – Timely contract counter-signature**

**Management Response:** The CCA acknowledges that there were some agreements where counter signatures from CCA were late (after the agreement start date) or missing. All agreements were reviewed during the drafting process and agreed to by all parties to said agreement prior to finalizing and signing by the vendor, contractor, assisters, navigators or any other organization that the CCA may be working with in relation to the Healthcare Exchange. In all these cases, the non-CCA party provided timely signature of the agreements.

In regards to the counter-signatures for the Certified Application Counselors (CAC), these agreements are non-financial agreements. MassHealth, the state's Medicaid agency, oversees the certification and training for these entities. The agreement is sent after having been vetted by MassHealth and the organization signs the agreement and dates it. Their signature date is used as the effective date so that specific employees within these organizations can obtain access to the Learning Management System (LMS) for certification. With that said, the CCA in conjunction with MassHealth will work to ensure that the CCA counter signature is completed in a more timely fashion.

Similarly, the Broker Enrollment Assister (BEA) agreements is a non-financial agreement. Once the BEA has signed the agreement, it is then granted access to training in it must pass in order to become a certified BEA. The CCA will ensure that any agreement, terms and condition and/or contract will include all necessary signatures. With the rollout of our new Group Market Exchange, we are reviewing our prior contracting process with brokers to see how we can improve it moving forward, part of which will be separating out BEAs from certified brokers.

The CCA acknowledges that Call Center support change orders were not signed prior to work commencing. Prior to work commencing, the CCA and the call center vendor had reached agreement on scope and pricing for the change order, but had not completed finalizing the written change order. We currently address this by having monthly meetings with our vendor to discuss and assess whether a change order would be needed in advance and, should one be required, the work would not commence until after both parties agreed to the terms and signed the respective agreement.

**Finding #2016-02 – Inter-governmental Monitoring**

**Management Response:** The CCA will review its contracts with its partners to see where enhancements can be made to ensure that applicable MARS-E controls are adhered to by the vendors. The CCA will continue to work with its vendors in the various Security Meetings that we have ensuring that we achieve our objectives listed in the POAM to remedy any potential issues.

**Finding #2016-03 – Inactive Account Monitoring**

**Management Response:** The CCA acknowledges that multi-factor authentication was not implemented during this period. However, there was in place a compensating control, where organizations have been vetted and whitelisting has been granted. Furthermore, the CCA is currently in the process of implementing multi-factor authentication with an expected implementation date of Q4 2018.

Automated disabling of inactive account IDs (ShareFile, HIX IDs, Active Directory) continues to be an unviable solution. Our current compensating control was in effect prior to the audit period and was updated in April 2016 to clearly define the 90-day termination policy for inactive accounts. Starting June 2016, 90-day inactive account reports were generated for the prior month. During this time, there was continued refinement of the process from when the policy was updated to ensure accurate and timely deactivation of inactive accounts. Any inactive accounts overseen by the CCA are submitted for termination after 90-days of inactivity. The CCA acknowledges that the accounts identified as being over the 90-day period occurred during the initial implementation and refinement period of implementing the new workflow and ensuring the correct logic and format was being used in its development. The CCA will continue to monitor and work with internal resources to automate the loading and production of 90-day term reports on a more consistent basis.

**Finding #2016-04 – MARS-E Compliance**

**Management Response:** The CCA acknowledges that a SIEM is not utilized at the organizational level and that certain applications and systems do track and log activities for a period of time prior to writing over legacy logs. However, prior to the CCA implementing a SIEM, which may be unnecessary and overly burdensome, MARS-E recommends that a security risk assessment be conducted to assess what information is potentially at risk should such an intrusion occur. Furthermore the CCA, is in the process of conducting a Privacy Risk Assessment in compliance with MARS-E 2.0 and part of this activity is to assess our systems and data inventory to assess what data is most vulnerable or at risk. The assessment is set to complete around August 2017 with further resources being required after August 2017 to address any potential issues and strengthen existing processes and procedures.

**Finding #2016-05 – Continuity Planning**

**Management Response:** The CCA acknowledges that there is no one integrated COOP that references the various COOPS that are in effect for the Health Insurance Exchange (HIX). As such, the CCA will work with the HIX Project Leads to have an integral vendor develop and create a robust COOP for the HIX. We have begun the process of working with our other financial processing and call center vendor to update their COOP as well with our first meeting held in or around July 2017. Finally, the CCA COOP will be reviewed and updated to incorporate references to the various vendor COOPs.

**Finding #2016-06 – Annual Attestation Report (AAR)**

**Management Response:** The 2014 SSP submitted to CMS reviewed and included various systems and some more recent systems were not included in this document as they were not in existence or being used at that time. However, when the CCA reviews and assesses its IT infrastructure for any CMS required attestation the entire IT environment is considered, not just the portion referenced in 2014. As our IT environment evolved with the implementation and utilization of new systems, controls and/or applications, assessing our current infrastructure on a two-year old document would have been neither reflective of the CCA at the time of completion nor accurate as to our current infrastructure. The CCA acknowledges that the 2016 AAR does not reference the specific systems; however, there is no need to do so nor is it required. Additionally, in our review of the AAR, we take into account all systems currently online as they relate to our infrastructure and any relationships we have with vendors to ensure that our AAR is reflective as of that point in time. MassIT received an extension to submit our SSP in 2017, so that we can align with the implementation for MARS-E 2.0, which is why there was not one within the audit period. The CCA will work with its vendors/partners in continuing to remediate items within its POAM.

**Finding #2016-07 – Verification of Eligibility Determination**

**Management Response:** The CCA acknowledges that the manual inconsistency process may take longer than expected. However, as required by 45 C.F.R. §155.315(f), the CCA works to determine each member who is determined eligible and subsequently has a Request for Information (RFI) at the time of their determination, and has the opportunity to provide proof in response to the RFI. The CCA began work with its vendor during fiscal year 2015 and continues to work with them to ensure that time clocks are running timely and that any other issues discovered are raised and investigated for any potential remediation.

**Finding #2016-08 – Document Retention**

**Management Response:** Members who were found eligible for QHP plans needed to provide proof of specific information. In some cases, members who did not provide this proof were time clocked out, or the system expired them. These members, as allowed by law, were granted provisional coverage for 90-days so that they can submit any necessary documentation. In some cases, if a member did not provide proof they would be 'downgraded' (meaning they would have to pay more in premiums as a failure to provide the necessary information) or terminated. The CCA will investigate the cause of instances where documentation was not correctly recorded.

| Audit Report Corrective Action Plan | | |
|---|---|---|
| **Issue Title: Finding #2016-01 – Timely contract counter-signature** | | |
| **Audit Report Recommendation:**<br>Recommendation: Improve existing policies and controls to help ensure timely review and approval of all Exchange contracts before contract start dates. | | |
| **Description of Remediation:**<br>• The Health Connector will review its current procedures in obtaining signatures for both BEAs and CACs and discuss internally how to ensure any necessary counter signatures are signed timely. | | |
| **Milestone** | **Target Date** | **Completion Date** |
| 1. Meeting to discuss the contract requirements and procedures for BEAs | October 2017 | |
| 2. Review and draft new document for BEAs only<br>3. Any Brokers that want to be BEAs re-sign newly defined document and begin training on LMS | December 2017 | |
| 4. Discuss and document contracting process for CAC contracts | November 2017 | |
| 5. Discussion with vendor regarding call center work orders and ensuring that contracts are in place and signatures obtained prior to starting work | July 2017 | |
| **Plan for Monitoring and Validation:** Monthly meetings with call center vendor | | |
| **Responsible Entity or Individual:** Compliance Manager, Legal, Contract Manager | | |

| Audit Report Corrective Action Plan | | |
|---|---|---|
| **Issue Title: Finding #2016-02 – Inter-governmental Monitoring** | | |
| **Audit Report Recommendation:**<br>• Review and enhance existing agreements with inter-governmental partners and service agreements key vendors to help ensure MARS-E controls are adhered to as required and control weaknesses are addressed timely.<br>• Further, CCA should ensure that sufficient monitoring procedures are in place to help ensure that various key vendors and governmental partners adhere to contract requirements. | | |
| **Description of Remediation:**<br>• CCA will review its current agreement with its partners and will discuss with legal the amending of these agreements as necessary<br>• CCA has drafted new language for its operations and maintenance agreement with MassIT pertaining to the IT services that it receives from that agency | | |
| **Milestone** | **Target Date** | **Completion Date** |
| 1. Ensure that FY 2018 agreement with MassIT addresses audit recommendations | December 2017 | |
| 2. Ensure that new EOHHS/Connector ISA pertaining to governance of the HIX/IES system addresses audit recommendations | January 2018 | |
| 3. Amend current operations agreement with NTT to ensure compliance with MARS-E V2. | March 2018 | |
| **Plan for Monitoring and Validation:** | | |
| **Responsible Entity or Individual:** Chief Information Officer, Legal, Compliance Manager | | |

| Audit Report Corrective Action Plan |
|---|
| **Issue Title: Finding #2016-03 –Inactive Account Monitoring** |
| **Audit Report Recommendation:**<br>• Implement settings which automatically disable inactive CCA accounts on a periodic basis. |

- CCA should revisit their inactive account review process, and, if necessary revise such that all accounts under their purview that have not been active for a significant period of time are disabled timely.
- While CCA has controls in place for authentication, including the use of "whitelisting" and passwords, CCA should further, strengthen controls by implementing two-factor authentication and establishing password parameters that adhere to MARS-E requirements.

**Description of Remediation:**

- The CCA will work with internal resources to identify the best way to ensure that reports are uploaded and run on a more consistent basis each month to ensure that those accounts it is responsible for are terminated in accordance with internal policies and federal regulations.
- The CCA will work with its stakeholders to further improve password strength.
- The CCA will work with its stakeholders on the implementation of multi-factor authentication

| Milestone | Target Date | Completion Date |
|---|---|---|
| 1. Review current process and procedures, and define new specifications | October 2017 | |
| 2. Generate logic and test functionality | February 2018 | |
| 3. Document new process and procedure | June 2018 | |
| 4. CCA will discuss with MassIT and the security team regarding password strength and work to implement a solution | December 2018 | |
| 5. Implementation of multi-factor authentication | Q4 2018 | |

**Plan for Monitoring and Validation:** IT Process Manager will continue to oversee the disabling of inactive accounts and monitor the termination of these accounts.

**Responsible Entity or Individual:** IT Process Manager, Enterprise Architect, Compliance Manager, Vendors integral to the HIX as necessary.

**Audit Report Corrective Action Plan**

**Issue Title: Finding #2016-04 – MARS-E Compliance**

**Audit Report Recommendation:**

- Take measures to configure systems, firewalls, and routers, to generate audit records for specific events, as defined by MARS-E or implement a Security Incident and Event Monitoring utility / tool.

**Description of Remediation:**

- The CCA through the conduction of a Privacy Risk Assessment will work to identify what information it maintains is at risk should an intrusion or breach occur.

| Milestone | Target Date | Completion Date |
|---|---|---|
| 1. Completion of Privacy Risk Assessment in accordance with MARS-E 2.0 | October 2017 | |
| 2. Review of Privacy Risk Assessment results to determine any gaps | February 2018 | |
| 3. Create a Data Inventory of all data maintained and/or stored within the CCA systems and document | August 2018 | |
| 4. Identify which information is at risk and assess the need of a SIEM and/or other auditing mechanism | October 2018 | |
| 5. Implementation of a SIEM or other auditing tool as necessary for CCA only | December 2018 | |

**Plan for Monitoring and Validation:**

**Responsible Entity or Individual:** Chief Information Officer, Compliance Manager, Legal

**Audit Report Corrective Action Plan**

**Issue Title: Finding #2016-05 – Continuity Planning**

**Audit Report Recommendation:**

Work with key vendors and inter-governmental parties to:

- Develop and document a comprehensive and integrated Contingency Plan including all vendors and governmental partners with a role in helping to ensure the continued operations of the Exchange in the event of a disaster at any one of the organization entities involved;
- Conduct periodic tests to validate the operating effectiveness of the Contingency Plan, including safeguards to preserve the privacy, integrity, availability, completeness and accuracy of data.

**Description of Remediation:**

- CCA and its key vendors will review current COOPs they are responsible for and update them.
- CCA will ensure its internal COOP is updated with the necessary information to direct readers to the appropriate COOP.

| Milestone | Target Date | Completion Date |
|---|---|---|
| 1. Review and update NTT COOP with NTT team and internal resources | January 2018 | |
| 2. Notify HIX Project Leads regarding the findings regarding the updating of the Optum/hCentive COOP for the HIX | August 2017 | |
| 3. Obtain initial draft of the Optum/hCentive COOP for the HIX | December 2018 | |
| 4. Review and update of CCA COOP to reflect the newly defined COOPs from both NTT and Optum/hCentive for their respective systems | TBD | |

**Plan for Monitoring and Validation:** Updates provided during team meetings with key resources

**Responsible Entity or Individual:** Vendors integral to the HIX, Deputy Executive Director & Chief Operating Officer, Chief Information Officer, Compliance Manager

**Audit Report Corrective Action Plan**

**Issue Title: Finding #2016-06 – Annual Attestation Report**

**Audit Report Recommendation:**

- Address all systems with a role in the processing or retention of sensitive data within its System Security Plan (SSP).
- Outline and address control gaps in CCA's Plan of Actions and Milestones (POAM) to CMS by establishing a project plan, prioritizing gap remediation by level of risk, and including governance and funding implications as well as a maintenance.

**Description of Remediation:**

- Work with lead MassIT to complete and submit our new SSP in accordance with deadlines discussed and approved by CMS
- Work to remediate POAM in accordance with MassIT on a scheduled agreed to with CMS.

| Milestone | Target Date | Completion Date |
|---|---|---|
| 1. Finalize and submit our SSP and all necessary documents | September 2017 | |
| 2. Continue to remediate items identified in the POAM | Ongoing | Quarterly based on risk rating (High = 30 days, Medium = 3 months, Low = 6 months) |

**Plan for Monitoring and Validation:** Security Meetings between the various entities and IT teams from MassIT, CCA, MH, Optum/hCentive and NTT.

**Responsible Entity or Individual:** MassIT, Chief Information Officer, Compliance Manage

| Audit Report Corrective Action Plan | | |
|---|---|---|
| **Issue Title: Finding #2016-07 – Verification of Eligibility Determination** | | |
| **Audit Report Recommendation:**<br>• Review and update the system functionality currently in place for expiring time clocks on outstanding requests, so eligibility re-determinations are performed in a compliant a timely manner.<br>• Further, improve the manual oversight process such that inconsistencies are remedied more timely. | | |
| **Description of Remediation:**<br>• CCA in conjunction with its external HIX vendors will review and conduct a root cause analysis regarding the discrepancies within the system and work to identify how best to resolve these | | |
| **Milestone** | **Target Date** | **Completion Date** |
| 1. Increase timeliness of expirations | September 2017 | |
| 2. Review business specifications and remediate issues over the next release cycles (releases 12-13) to ensure that system is working as designed and selecting all RFIs based on expiration rules | March 2018 | |
| **Plan for Monitoring and Validation:** Continued project meetings to obtain project updates, review and discuss any discrepancies and issues that may have occurred. | | |
| **Responsible Entity or Individual:** Director of Member Implementation, Compliance Manager | | |

| Audit Report Corrective Action Plan | | |
|---|---|---|
| **Issue Title: Finding #2016-08 – Document Retention** | | |
| **Audit Report Recommendation:**<br>• CCA should work with its vendors/partners to ensure appropriate oversight of eligibility and enrollment documentation maintenance. | | |
| **Description of Remediation:**<br>• The CCA in conjunction with its vendor partners, will review and conduct a root cause analysis regarding the discrepancies and work to identify how best to resolve these | | |
| **Milestone** | **Target Date** | **Completion Date** |
| 1. Have vendors conduct a root cause analysis | Q4 2018 | |
| 2. Continue to work with vendors and partners to identify and resolve issues | Ongoing | |
| **Plan for Monitoring and Validation:** Project meetings to obtain project updates, review and discuss any discrepancies and issues that may have occurred. | | |
| **Responsible Entity or Individual:** Director of Member Implementation, Compliance Manager | | |

# Appendix A – List of interviewed personnel

# Appendix A – List of interviewed personnel

| |
|---|
| Assistant General Counsel |
| Manager of IT Process |
| Director, Program and Product Strategy |
| Compliance Manager |
| Director of Accounting |
| General Counsel |
| Chief Actuary |
| Implementation Manager |
| System Architect |
| Chief Information Officer |
| Chief Financial Officer |
| Senior Manager Quality and Training |
| Assistant General Counsel |
| Executive Director |
| Product Manager Health and Dental Programs |
| Assistant General Counsel |
| Director of Customer Experience |
| Associate Director of Public Outreach and Education |
| MA-HIX Security and Privacy Compliance Manager (MassIT) |
| Senior Accountant |
| Senior Outreach Coordinator and Policy Analyst |
| Director of Reporting |
| Senior Manager of Operations |
| Director of Human Resources |
| Director of Member Implementation |
| Deputy Executive Director, Chief Operating Officer |

# Appendix B – Glossary of terms

# Appendix B – Glossary of Terms

| | |
|---|---|
| **ACA** | Patient Protection and Affordable Care Act |
| **CAC** | Certified Application Counselors |
| **CCA** | Commonwealth Health Insurance Connector Authority |
| **C.F.R.** | Code of Federal Regulations |
| **CMS** | Centers for Medicare and Medicaid Services |
| **GAS** | Government Auditing Standards |
| **HHS** | U.S. Department of Health and Human Services |
| **MassIT** | Massachusetts Office of Information Technology |
| **PII** | Personally Identifiable Information |
| **QDP** | Qualified Dental Plan |
| **QHP** | Qualified Health Plan |
| **SBM** | State based Marketplace |
| **SHOP** | Small Business Health Options Program |
| **SSP** | System Security Plan |

**kpmg.com/socialmedia**