Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued July 15, 2022

Office of Medicaid (MassHealth)—Review of Continuity of Operations Plan

For the period January 1, 2020 through June 30, 2021

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

July 15, 2022

Ms. Marylou Sudders, Secretary
Executive Office of Health and Human Services
1 Ashburton Place, 11th Floor
Boston, MA 02108

Dear Ms. Sudders:

I am pleased to provide this performance audit of MassHealth's continuity of operations plan and contingency planning for its Medicaid Management Information System. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, January 1, 2020 through June 30, 2021. My audit staff discussed the contents of this report with MassHealth management, whose comments are reflected in this report.

I would also like to express my appreciation for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

OVERVIEW OF AUDITED ENTITY 3

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY 5

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE 7

1. **MassHealth did not annually update its continuity of operations plan or conduct staff training or exercises related to the plan.** 7
2. **MassHealth did not annually update or test its disaster recovery plan.** 8

LIST OF ABBREVIATIONS

COOP	continuity of operations plan
DRP	disaster recovery plan
EOHHS	Executive Office of Health and Human Services
EOTSS	Executive Office of Technology Services and Security
IT	information technology
MMIS	Medicaid Management Information System
OSA	Office of the State Auditor

EXECUTIVE SUMMARY

The Office of the State Auditor (OSA) receives an annual appropriation for the operation of a Medicaid Audit Unit to help prevent and identify fraud, waste, and abuse in the Commonwealth's Medicaid program. This program, known as MassHealth, is administered under Chapter 118E of the Massachusetts General Laws by the Executive Office of Health and Human Services (EOHHS), through the Division of Medical Assistance. Medicaid is a joint federal-state program created by Congress in 1965 as Title XIX of the Social Security Act. At the federal level, the Centers for Medicare & Medicaid Services, within the United States Department of Health and Human Services, administer the Medicare program and work with state governments to administer state Medicaid programs.

OSA has conducted a performance audit of MassHealth's continuity of operations plan (COOP) and disaster recovery plan (DRP) for its Medicaid Management Information System (MMIS) for the period January 1, 2020 through June 30, 2021. The purpose of this audit was to determine whether MassHealth complied with Executive Order 490 and Sections 6.1 and 6.2 of the Executive Office of Technology Services and Security's Business Continuity and Disaster Recovery Standard IS.005.

The audit was conducted as part of OSA's ongoing independent statutory oversight of the state's Medicaid program. As with any government program, public confidence is essential to this program's success and continued support.

Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1 **Page 7**	MassHealth did not annually update its COOP or conduct staff training or exercises related to the plan.
Recommendations **Page 8**	1. MassHealth should establish monitoring controls to ensure that it properly adheres to the policies and procedures it has established for updating and testing its COOP. 2. MassHealth should work with EOHHS to annually update its COOP and conduct staff training and exercises.

Finding 2 **Page 8**	MassHealth did not annually update or test its DRP.
Recommendations **Page 9**	1. MassHealth should establish written policies and procedures for assigning, managing, and monitoring its DRP. 2. MassHealth should identify an offsite disaster recovery location to use for MMIS. Once the site has been selected, MassHealth should test the updated DRP and incorporate the results into it.

OVERVIEW OF AUDITED ENTITY

Under Chapter 118E of the Massachusetts General Laws, the Executive Office of Health and Human Services (EOHHS), through the Division of Medical Assistance, administers the state's Medicaid program, known as MassHealth. MassHealth provides access to healthcare for approximately 1.8 million low- and moderate-income children, families, seniors, and people with disabilities annually. In fiscal year 2021, MassHealth paid healthcare providers more than $18.1 billion, of which approximately 45% was funded by the Commonwealth. Medicaid expenditures represented approximately 40% of the Commonwealth's total fiscal year 2021 budget.

EOHHS is responsible for working with MassHealth to establish its continuity of operations planning, business continuity planning, and disaster recovery planning controls over MassHealth's Medicaid Management Information System (MMIS). Since 1978, state agencies have been required by executive orders to perform and document their planning efforts for the continuity of operations during emergencies. Most recently, Executive Order 490, issued in September 2007, states,

> *To achieve a maximum state of readiness, these plans should be incorporated into the daily operations of every secretariat and agency in the executive department, and should be reviewed on a regular basis and, with respect to agencies supplying services critical in times of emergency, exercised regularly. . . . In addition, each critical secretariat and agency shall submit an annual report to the Executive Office of Public Safety and Security.*

MMIS

MMIS is the claim processing and data warehouse system MassHealth uses. MMIS contains various types of information, such as healthcare information about services provided to MassHealth members and billing submission data, and is used for processing data, verifying eligibility, and running reports that identify medical treatment.

Continuity of Operations Plan and Disaster Recovery Plan

According to the Massachusetts Emergency Management Agency's "State Agency COOP Program Template,"

> *The . . . Continuity of Operations Plan (COOP) provides a framework to ensure continued operation of mission essential functions for up to 30 days when an internal or external emergency impacts [an] Agency's facilities, systems, personnel, and/or operations.*

The continuity of operations plan should address important elements that are fundamental to business continuity planning, such as a list of essential business functions, a designation of MassHealth's mission-critical systems, MassHealth's emergency notification procedures, personnel contact information, and a detailed list of responsibilities for continuity of operations.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios.

Executive Office of Technology Services and Security

The Executive Office of Technology Services and Security's (EOTSS's) predecessor agency was MassIT, which had a supervisory role over information technology (IT) at Commonwealth executive branch agencies. On August 1, 2017, the Governor formed EOTSS with the goal of consolidating more IT functions in executive branch agencies into a central agency. This was called the One Network initiative.

EOTSS, and EOHHS's IT Department, manage MMIS. Although EOTSS has had an increasing role with agencies' IT Departments, EOHHS is still responsible for establishing controls to ensure proper safeguarding of the information it collects and retains in MMIS.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of MassHealth's continuity of operations plan (COOP) for its Medicaid Management Information System (MMIS) for the period January 1, 2020 through June 30, 2021.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Below is a list of our audit objectives, indicating each question we intended our audit to answer, the conclusion we reached regarding each objective, and where each objective is discussed in the audit findings.

Objective	Conclusion
1. Does MassHealth have a COOP that has been updated and exercised, and on which employees have been trained, in accordance with Executive Order 490?	**No; see Finding 1**
2. Does MassHealth adhere to disaster recovery standards in accordance with Sections 6.1 and 6.2 of the Executive Office of Technology Services and Security's Business Continuity and Disaster Recovery Standard IS.005?	**No; see Finding 2**

To achieve our audit objectives, we gained an understanding of the internal control environment related to the objectives by conducting inquiries with MassHealth.

In addition, we performed the following procedures to obtain sufficient, appropriate audit evidence to address the objectives.

To determine whether the MassHealth COOP met the requirements of Executive Order 490, we reviewed the COOP, dated July 2016, to determine whether it was updated annually. We interviewed MassHealth officials who were responsible for oversight of the COOP, asking whether the plan had been run through for practice and whether employees had been trained in relation to the plan. Additionally, we reviewed the list of employees in the COOP plan and confirmed that the employees were still active in the

Commonwealth's "Global Email List" to determine whether the COOP was up to date with current key decision-makers.

To determine whether a formal disaster recovery plan (DRP) was in place to restore essential operations and enable MassHealth to continue its daily operations in a timely manner if automated systems were unavailable for an extended period, we interviewed knowledgeable MassHealth management personnel about their "New MMIS Disaster Recovery / Business Continuity Plan." We reviewed this plan, which was dated September 2008. We also reviewed the names of the key decision-making employees listed in the plan to determine whether they were still active EOHHS employees, in order to ensure that the plan was up to date with current key decision-makers.

We reviewed the results of the MA-21 software system[1] disaster recovery exercise conducted in March 2021 to determine what would be the impact of a disruption of services if an emergency arose.

1. This system determines whether a MassHealth applicant meets all MassHealth's eligibility requirements, and if so, it determines the most comprehensive healthcare coverage type for which the applicant is eligible. MA-21 is separate and distinct from MMIS.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. MassHealth did not annually update its continuity of operations plan or conduct staff training or exercises related to the plan.

During our audit period, MassHealth did not annually update its continuity of operations plan (COOP) for its mission-critical information technology (IT) system, the Medicaid Management Information System (MMIS). The last COOP MassHealth prepared was dated July 1, 2016. Further, MassHealth did not conduct any annual staff training or exercises to test the effectiveness of its COOP during a simulated emergency situation.

As a result, MassHealth's COOP may not be sufficient to ensure that MassHealth can continue to provide all its services during an emergency situation.

Authoritative Guidance

Executive Order 490 states,

> *Section 4. [A] secretariat or agency shall regularly, and in no event less than once per calendar year, conduct trainings and exercises to put into practice its submitted . . . Continuity of Operations plans.*
>
> *Section 5. These trainings and exercises shall be designed to simulate emergency situations which may arise, and shall be designed to test the effectiveness of the various components of the . . . Continuity of Operations plans. . . .*
>
> *Section 6. Each . . . secretariat within the executive department shall incorporate findings from these trainings and exercises into its . . . Continuity of Operations plans, and based on these findings, shall regularly, and in no event less than once per calendar year, update these plans. . . . Likewise, each . . . agency within the executive department shall incorporate findings from these trainings and exercises into its Continuity of Operations plan, and based on these findings, shall regularly, and in no event less than once per calendar year, update its Continuity of Operations Plan.*

Reasons for Issue

MassHealth officials stated that the agency had decided to delay updating its COOP until the 2019 coronavirus pandemic had substantially abated so that it could incorporate the lessons it learned from its pandemic response into an updated version of the COOP. Although MassHealth did have policies and procedures regarding the annual updating and testing of the COOP, it had not established monitoring controls to ensure that it properly adhered to them.

Recommendations

1. MassHealth should establish monitoring controls to ensure that it properly adheres to the policies and procedures it has established for updating and testing its COOP.
2. MassHealth should work with the Executive Office of Health and Human Services (EOHHS) to annually update its COOP and conduct staff training and exercises.

Auditee's Response

As noted during the course of the audit, MassHealth was in the process of updating its COOP in early 2020 but suspended its efforts and redirected staff efforts in response to the [2019 coronavirus] pandemic. At a time that required immediate reprioritization, MassHealth focused its efforts on successfully maintaining critical operations during this global pandemic.

MassHealth agrees with the [Office of the State Auditor's] recommendations listed above and has resumed its work to update the MassHealth COOP. MassHealth is also establishing monitoring controls to ensure adherence to COOP-related procedures.

Auditor's Reply

Based on its response, MassHealth is taking measures to address our concerns on this matter.

2. MassHealth did not annually update or test its disaster recovery plan.

MassHealth had not updated its disaster recovery plan (DRP) since June 18, 2009 and did not test the DRP annually. Further, although the Executive Office of Technology Services and Security (EOTSS) provides offsite storage of MMIS in the form of electronic backup copies and magnetic media copies, MassHealth does not have an offsite location to restore MMIS in the event of an unforeseen interruption in its business operations.

As a result, MassHealth is vulnerable to a disruption of services that could negatively affect its members if its IT capabilities are inoperable for an extended period. The "MA21 Disaster Recovery Exercise March 2021 Postmortem Report," dated May 11, 2021, from EOTSS to EOHHS states,

Not having the Medicaid Management Information System (MMIS) severely impacts the ability of MassHealth as an organization to perform their function in providing members with . . . access to benefits.

Authoritative Guidance

EOTSS's Business Continuity and Disaster Recovery Management Standard IS.005, effective October 15, 2018, states,

6.2.1 Commonwealth Executive Offices . . . must develop and maintain processes for disaster recovery plans at both onsite primary Commonwealth locations and at alternate offsite locations. . . .

6.2.2 Commonwealth Executive Offices . . . must ensure that [DRPs] shall be tested annually.

Reasons for Issue

MassHealth does not have any policies and procedures regarding the updating and testing of its DRP.

Recommendations

1. MassHealth should establish written policies and procedures for assigning, managing, and monitoring its DRP.
2. MassHealth should identify an offsite disaster recovery location to use for MMIS. Once the site has been selected, MassHealth should test the updated DRP and incorporate the results into it.

Auditee's Response

MassHealth will finalize and publish the policies and procedures for the MMIS Disaster Recovery Plan (DRP) by the end of calendar year 2022. This will include steps to monitor and review the plan on an annual basis.

MassHealth is preparing to migrate to Amazon Web Services (AWS) for MMIS disaster recovery. Due to the complexity of the technology implementation, significant cyber security reviews, and the involvement of multiple agencies, this migration will take time but expects completion by Summer 2024. This migration will be done in close coordination with the Executive Office of Technology Services and Security (EOTSS), which is in the process of closing its Chelsea and Springfield data centers and migrating to AWS as part of its Cloud First strategy. When the migration is complete, MMIS will take advantage of DRP services available within AWS. The MMIS DRP will then be updated, tested, and integrated into the regular DRP monitoring schedule.

Auditor's Reply

Based on its response, MassHealth is taking measures to address our concerns on this matter.