OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued December 23, 2024

Commonwealth Health Insurance Connector Authority

For the period July 1, 2021 through June 30, 2023

State House Room 230 ■ Boston, MA 02133 ■ auditor@massauditor.gov ■ www.mass.gov/auditor

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

December 23, 2024

Audrey Morse Gasteier, Executive Director
Commonwealth Health Insurance Connector Authority
100 City Hall Plaza, 6th Floor
Boston, MA 02108

Dear Ms. Gasteier:

I am pleased to provide to you the results of the enclosed performance audit of the Commonwealth Health Insurance Connector Authority. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2021 through June 30, 2023. As you know, my audit team discussed the contents of this report with agency managers. This report reflects those comments.

I appreciate you and all your efforts at the Commonwealth Health Insurance Connector Authority. The cooperation and assistance provided to my staff during the audit went a long way toward a smooth process. Thank you for encouraging and making available your team. I am available to discuss this audit if you or your team has any questions.

Best regards,

Diana DiZoglio
Auditor of the Commonwealth

cc: Kate Walsh, Secretary of the Executive Office of Health and Human Services
Andrew Egan, General Counsel of the Commonwealth Health Insurance Connector Authority
Brittany Algar, Senior Compliance Manager of the Commonwealth Health Insurance Connector Authority

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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 the Commonwealth Health Connector Insurance Authority (Connector) for the period July 1, 2021 through June 30, 2023.

The purpose of our audit was to determine whether the Connector did the following:

- conducted eligibility requirement tests to ensure that all applicants who received benefits met the criteria established by Sections 12.05 and 12.06 of Title 956 of the Code of Massachusetts Regulations;
- had policies and procedures in place to process complaints and documented actions taken to resolve complaints received; and
- provided annual cybersecurity awareness training to its employees in accordance with Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security's Information Security Risk Management Standard IS.010

Below is a summary of our finding, the effect of that finding, and our recommendations, with links to each page listed.

Finding 1 **Page 11**	The Connector does not maintain a log of possible fraud complaints received.
Effect	Without documentation of fraud complaints received, the Connector cannot monitor the number of complaints, as well as actions taken to address specific complaints.
Recommendations **Page 12**	1. The Connector should develop and implement written policies and procedures surrounding the receipt and resolution of complaints. 2. All fraud complaints received should be logged into the Connector's privacy and security incidents log, along with documentation to support the actions taken to resolve them.

OVERVIEW OF AUDITED ENTITY

The Commonwealth Health Insurance Connector Authority (Connector) was established pursuant to Chapter 176Q of the Massachusetts General Laws, as added by Section 101 of Chapter 58 of the Acts of 2006, to provide affordable health insurance to the citizens of Massachusetts. People who do not meet the required income eligibility levels to participate in the Commonwealth's Medicaid program (also known as MassHealth) are referred to the Connector, which was established to help them obtain affordable health insurance.

The Connector is an independent public entity not subject to the supervision and control of any other executive office, department, commission, board, bureau, agency, or political subdivision of the Commonwealth, except as specifically provided in general or special law.

According to its website, the Connector's mission is to "advance access to high-quality health care by serving as a transparent and transformative marketplace for Massachusetts residents and small businesses to come together and easily find, compare, and enroll in affordable health insurance."

The Connector is governed by an 11-member board that includes the chair, who is the Secretary of the Executive Office of Health and Human Services; the Secretary of the Executive Office for Administration and Finance; the Commissioner of Insurance; the Executive Director of the Group Insurance Commission; four members appointed by the Governor; and three members appointed by the Attorney General.

The Connector's central office is located at 100 City Hall Plaza in Boston and has walk-in locations in Boston, Springfield, and Worcester. As of June 30, 2023, the Connector had 79 employees.

The Connector is not funded by any line items (or appropriations) in the Commonwealth's annual budget. It receives funding from the following two sources:

- the Commonwealth Care Trust Fund, which was established in accordance with Section 2OOO of Chapter 29 of the General Laws, which states, "Amounts credited to the fund shall be expended without further appropriation for programs administered by the commonwealth health insurance connector authority pursuant to chapter 176Q [of the General Laws] that are designed to increase health coverage for residents of the Commonwealth," and
- Section 12(a) of Chapter 176Q of the General Laws, which states, "The connector may apply a surcharge to all health benefit plans or stand-alone vision or stand-alone dental plans which shall be used only to pay for administrative and operational expenses of the connector."

Connector Enrollment

Individuals and families applying for health insurance through the Connector can do so via the Health Connector online portal, on a paper application in person, over the telephone, or with an assister.[1] The applicant's household information—which includes the applicant's name, Social Security number, date of birth, household income, place of residence, family size, projected yearly income(s) of working household members, proof of Massachusetts residency, and whether any household members currently have health insurance—is entered into the Connector's database and used to make an eligibility determination.

The Connector verifies an applicant's reported income with the US Internal Revenue Service and the Massachusetts Department of Revenue. The Connector verifies an applicant's residency using an online research tool called LexisNexis. Other information, such as immigration status and access to other health coverage like Medicare, is verified using the Federal Data Services Hub (which involves the US Social Security Administration, the US Department of Homeland Security, and Medicare/Medicaid). If discrepancies exist between an applicant's attestation and the Connector data, the Connector sends the applicant a request for additional documentation to support their application.

The Connector follows regulations as found in Section 155 of Title 45 of the Code of Federal Regulations to determine whether an applicant is eligible to participate in the program and to verify information provided by applicants.

The table below shows a distinct count of all enrolled Connector participants across the state during the audit period.

County	Number of Distinct Enrollees During the Audit Period
Middlesex	58,867
Essex	36,950
Suffolk	34,700
Worcester	32,508
Norfolk	24,976
Bristol	23,521
Plymouth	20,804
Hampden	15,427

1. An assister is a certified enrollment expert who can help applicants understand their coverage options, answer questions they may have, and help them find the most affordable coverage that meets their needs.

County	Number of Distinct Enrollees During the Audit Period
Barnstable	12,518
Hampshire	5,181
Berkshire	5,134
Franklin	3,824
Dukes	1,647
Nantucket	1,252
Out of State	2,199
Other*	107,747
Total	387,255

* Other represents people who did not provide a ZIP code.

Connector's Complaint/Issue Process

Anyone can request assistance from the Connector by telephone, email, or mail or in person. A request comes in one of the following two ways:

- A request is routed through Accenture, a third party that handles initial customer relations for the Connector related to member-facing billing, enrollment, eligibility, and more.
- A request is made by a member who makes an allegation related to fraud, privacy breach, discrimination, or language rights issues, using four dedicated email inboxes and phone lines.

If an issue that Accenture received requires escalation, it is forwarded to the Connector Ombuds Team,[2] which conducts additional research and issue resolution. The total number of issues referred to Connector Ombuds Team during the audit period was 2,309.

Any issue that Accenture or the Connector Ombuds Team believes is related to fraud, privacy breach, discrimination, or language rights issues is forwarded to the compliance manager and/or the privacy officer. Complaints that rise to the level of an actual case related to fraud, privacy breach, discrimination, or language rights violations will be tracked in the Ombuds or the Connector's privacy and security incident logs until completion. The privacy and security log contains a description of the complaint, the

2. The Connector Ombuds Team is composed of Connector staff members and is responsible for the end-to-end resolution of complaints received from various escalation channels.

name of the individual making the complaint, the severity of the complaint (critical, moderate, or minor),[3] the number of people affected, and steps taken to manage and respond to the complaint. The compliance manager then sends remediation steps to the privacy officer for review and approval. In conjunction with the compliance manager, the privacy officer ensures that the applicable laws, regulations, and Connector policies and procedures are followed to remediate the complaints in an appropriate manner.

The Connector legal team stated that no issues received during the audit period rose to the level of an actual case related to fraud, privacy breach, discrimination, or language rights violation.

Cybersecurity Awareness Training

The Executive Office of Technology Services and Security (EOTSS) has established policies and procedures that apply to all Commonwealth agencies within the executive branch. These policies and procedures require executive branch agencies to implement internal procedures that ensure that their employees comply with the requirements in EOTSS's aforementioned policies and procedures. EOTSS recommends, but does not require, non-executive branch agencies to follow its policies and procedures. Section 6.2 of EOTSS's Information Security Risk Management Standard IS.010 states,

> *The objective of the Commonwealth information security training is to educate users on their responsibility to help protect the confidentiality, availability and integrity of the Commonwealth's information assets. Commonwealth Offices and Agencies must ensure that all personnel are trained on all relevant rules and regulations for cybersecurity.*

To ensure that employees in all Commonwealth agencies within the executive branch are clear on their responsibilities, EOTSS's policies and procedures require that all newly hired employees[4] must complete an initial cybersecurity awareness training course within 30 days of their orientation, and that all existing employees[5] complete an annual refresher cybersecurity awareness course. However, Connector policy requires that all newly hired employees complete cybersecurity awareness training before being given access to the data. The Connector's Human Resources Department issues a System Access Request to the

3. According to the Connector's "Policy and Procedures for Responding to and Reporting Security or Disclosure Related Incidents," the Connector categorizes complaints into three distinct severity levels: critical, moderate, and minor. Critical complaints are defined as those involving the misuse of personally identifiable information and violations of the Health Insurance Portability and Accountability Act. Moderate complaints encompass civil legal actions, which may include regulatory penalties or other civil disputes that could adversely affect the reputation of the Connector. Minor complaints refer to violations of policy that do not result in security breaches.
4. For the purposes of this audit report, we use the term newly hired employees to refer to employees who were hired during the audit period, unless stated otherwise.
5. For the purposes of this audit report, we use the term existing employees to refer to employees who were hired before the start of the audit period, unless stated otherwise.

authority's Information Technology Department to inform it when a newly hired employee has completed the training.

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 certain activities of the Commonwealth Health Insurance Connector Authority (Connector) for the period July 1, 2021 through June 30, 2023.

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, if applicable, where each objective is discussed in the audit findings.

Objective	Conclusion
1. Did the Connector conduct eligibility requirement tests to ensure that all applicants receiving benefits met the criteria established by Sections 12.05 and 12.06 of Title 956 of the Code of Massachusetts Regulations?	**Yes**
2. Did the Connector have policies and procedures to process complaints, and did it document the actions taken to resolve the complaints it received?	**No; see Finding 1**
3. Did the Connector provide cybersecurity awareness training to its employees in accordance with Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Management Standard IS.010?	**Yes**

To accomplish our audit objectives, we gained an understanding of the aspects of the Connector's internal control environment relevant to our objectives by reviewing applicable policies and procedures and by interviewing staff members and management. In addition, to obtain sufficient, appropriate evidence to address our audit objectives, we performed the procedures described below.

Connector Enrollment

To determine whether the Connector conducted eligibility requirement testing to ensure that all enrollees receiving benefits met the criteria established by Sections 12.05 and 12.06 of Title 956 of the Code of

Massachusetts Regulations, we took a number of actions. Using a 95% confidence level,[6] a 0% expected error rate,[7] and a 5% tolerable error rate,[8] we selected a random, statistical[9] sample of 60 people who were enrolled during the audit period out of a total population of 601,854.[10] For our sample, we examined each application to determine the following:

- whether the Connector verified (1) each enrollee's income as a percentage of the federal poverty level and (2) that the income matched the information with both the Massachusetts Department of Revenue and the US Internal Revenue Service;
- whether the Connector verified that each enrollee was not eligible for Medicare or Medicaid;
- whether the Connector verified that each enrollee was a Massachusetts resident by ensuring that the corresponding address matched with LexisNexis or the US Postal Service;
- whether the Connector verified that each enrollee's Social Security number matched US Social Security Administration records; and
- whether the Connector verified (1) that each enrollee met the criteria based on their immigration status and (2) whether the enrollee was incarcerated by obtaining information from the US Department of Homeland Security.

Based on the test results, we determined that the Connector conducts eligibility requirement tests to ensure that applicants receiving benefits meet the criteria established by Sections 12.05 and 12.06 of Title 956 of the Code of Massachusetts Regulations. No exceptions were noted in our sample selected for testing. Because we utilized statistical analysis, there is a 95% likelihood that the results of this sample accurately represent the experience of the entire population.

6. Confidence level is a mathematically based measure of the auditor's assurance that the sample results (statistic) are representative of the population (parameter), expressed as a percentage. A 95% confidence level means that 95 out of 100 times, the statistics accurately represent the larger population.
7. Expected error rate is the number of errors that are expected in the population, expressed as a percentage. It is based on the auditor's knowledge of factors such as prior audit results, the understanding of controls gained in planning, or a probe sample. In this case, we are assuming there are no errors in the data provided to us by the auditee.
8. The tolerable error rate (which is expressed as a percentage) is the maximum error in the population that is acceptable while still using the sample to conclude that the results from the sample have achieved the objective.
9. Auditors use statistical sampling to select items for audit testing when a population is large (usually over 1,000) and contains similar items. Auditors generally use a statistics software program to choose a random sample when statistical sampling is used. The results of testing using statistical sampling, unlike those from judgmental sampling, can usually be used to make conclusions or projections about entire populations.
10. As stated above, there were 387,255 distinct enrollees during our audit period. Some of these distinct enrollees enrolled in more than one year of coverage during the two-year audit period, resulting in a population of 601,854 enrollments.

Connector's Complaint/Issue Process

To determine whether the Connector had policies and procedures in place to process complaints and documented the actions taken to resolve these complaints, we inquired with management regarding the process used and created a flowchart to document our understanding of the process.

The Connector management informed us that they do not track all complaints but only those that rise to the level of privacy and security incidents. As a result, we concluded that the Connector does not have a complaint log that would serve as documentation of complaints received. See Finding 1.

Cybersecurity Awareness Training

To determine whether the Connector provided initial and annual cybersecurity awareness training to its employees, as required by Sections 6.2.3 and 6.2.4 of the EOTSS's Information Security Risk Management Standard IS.010, we took the following actions. We obtained a list of Connector employees who were employed by the Connector as of June 30, 2023. This list included 79 active, 37 terminated, and 33 newly hired employees. We took the following actions using this list:

- We selected a random, nonstatistical sample of 20 active and terminated employees from the list to ensure that each took their annual cybersecurity awareness training as required by Section 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010.
- For each employee newly hired during the audit period, we selected a random, nonstatistical sample of 10 to ensure that each employee signed their certification within 30 days, as required by Section 6.2.3 of EOTSS's Information Security Risk Management Standard IS.010.

Based on the test results, we determined that the Connector provides cybersecurity awareness training to its employees in accordance with Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010. No exceptions were noted.

Data Reliability Assessment

The Connector's Enrollees

To determine the reliability of the list of the 601,854 enrollees that we obtained from the Connector's system[11] that were approved to enroll for health insurance during the audit period, we interviewed officials who were knowledgeable about the data. We reviewed System and Organization Control

11. The Connector utilized the Massachusetts Health Insurance Exchange and Integrated Eligibility system to process eligibility.

reports[12] that covered the audit period and ensured that an independent auditor had performed certain information system control tests. We also tested the enrollee data for any worksheet errors (e.g., hidden objects such as rows, headers, and other content). To confirm the accuracy of the enrollee data in the Massachusetts Health Insurance Exchange and Integrated Eligibility System, we selected a random sample of 20 in the list of enrollees from the data and compared the information in the data (i.e., member identification number, reference identification number, and gender) to source documents to ensure that the information was accurate.

Cybersecurity Awareness Training

To determine the reliability of the lists provided by the Connector of employees who were, during the audit period, active, newly hired, and/or terminated, we checked the spreadsheet for duplicate records, identified any employees whom the Connector hired during the audit period, and confirmed whether employment start dates and/or termination dates were within the audit period. We also reconciled the entire population of active Connector employee records in the list to payroll summary data that we extracted from the Office of the Comptroller of the Commonwealth's CTHRU database[13] and the cybersecurity awareness training systems that the Connector used during the audit period. We took a sample of 10 newly hired employees out of the 33 and determined whether the Connector's Human Resources Department issued a System Access Request to the authority's Information Technology Department, granting each newly hired employee access to the system after completion of the cybersecurity awareness training.

Based on the results of the data reliability assessment procedures described above, we determined that the information we obtained was sufficiently reliable for the purposes of our audit.

12. A System and Organization Control report is a report on controls, issued by an independent contractor, about a service organization's systems relevant to security, availability, processing integrity, confidentiality, or privacy.
13. According to the Office of the Comptroller of the Commonwealth's website, "CTHRU is an innovative open records platform . . . that offers transparency into the finances and payroll of the Commonwealth of Massachusetts. CTHRU provides users with an intuitive experience for exploring how and where public money is utilized."

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Commonwealth Health Connector Insurance Authority does not maintain a log of possible fraud complaints received.

The Commonwealth Health Connector Insurance Authority (Connector) could not provide a log of alleged fraud complaints that were received through telephone, email, mail, or in-person means during the audit period.

Without documentation of fraud complaints received, the Connector cannot monitor the number of complaints, as well as actions taken to address specific complaints.

Authoritative Guidance

According to Section 10.01 of the Office of the Comptroller of the Commonwealth's *Internal Control Guide: [Office of the Comptroller of the Commonwealth] Statewide Risk Management* document, agencies are required to develop "policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives."

In addition, according to Section 12.01 of the Office of the Comptroller of the Commonwealth's *Internal Control Guide: [Office of the Comptroller of the Commonwealth] Statewide Risk Management* document, managers and other personnel members in key roles should document internal control, all transactions, and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either a paper or an electronic form.

Also, the following information is found in the "Quick Guide: Schedule Number 06–18" from the *Massachusetts Statewide Records Retention Schedule*, as revised in July 2022:

> *B04–04: Licensure Complaints, Investigations, and Hearing Records*
>
> *See sub-schedules for specific retention periods.*
>
> *Documents complaints received and/or investigated relating to unregulated activities. Complaint types include regulatory non-compliance, fraud and program abuse, administrative process, and citizen requests for services. Includes intake documentation, complaint forms, interview notes, hearing transcriptions, investigation reports, appeals, [and] hearing proceedings.*

Reasons for Issue

According to an email to us from the Connector's compliance manager, "There were no complaints that rose to the level of a privacy and security incident. Also, we only track complaints that rise to the level of Privacy and Security incidents in the [privacy and security] Incident log." We could not verify the accuracy of this statement, because there was no log of complaints for us to review to determine the severity of complaints, the accuracy of their categorization, or how well the authority evaluated and adjudicated them.

Recommendations

1. The Connector should develop and implement written policies and procedures surrounding the receipt and resolution of complaints.

2. All fraud complaints received should be logged into the Connector's privacy and security incidents log, along with documentation to support the actions taken to resolve them.

Auditee's Response

In response to [the Office of the State Auditor's] draft audit report on the Health Connector covering the period July 1, 2021, through June 30, 2023, the Health Connector acknowledges that the Auditor is recommending that the Health Connector "develop and implement written policies and procedures surrounding the receipt and resolution of complaints," and that "fraud complaints received should be logged into the Connector's privacy and security incidents log."

The term "complaint" is non-specific and vague, but the Health Connector understands it to refer to the various areas of compliance oversight with which it is tasked, namely complaints of Fraud, Waste, and Abuse; violations of its Privacy Policy; violations of its Nondiscrimination Policy; and violations of its Language Access Policy.

The Health Connector does not agree that all of these kinds of complaints should be tracked in its privacy and security incidents log, since that log is reserved only for documenting privacy or security incidents.

Further, the Health Connector notes that it makes available to members of the public several channels to report violations of the above-mentioned policies, including complaint forms, email addresses, and phone lines dedicated to each type. The Health Connector takes seriously its obligations investigate any complaint that alleges a violation of these policies, and notes that to date it has received none.

That said, the Health Connector understands that the Auditor recommends logging all communications received through these dedicated complaint channels, including those that are misdirected, inappropriate, spam, or otherwise fail to allege a violation of a Health Connector policy. The Health Connector therefore will create policies and procedures to document each

communication received through a dedicated complaint channel and log them in an appropriate location, consistent with the Auditor's recommendations.

Auditor's Reply

The key issue that led to our audit finding was that the Connector did not log all complaints received, nor did it document the resolution of complaints. Without a documented log of complaints, the auditee is not in compliance with the Office of the Comptroller of the Commonwealth's guidance or the Massachusetts Statewide Records Retention Schedule, listed above in the "Authoritative Guidance" section. This prevents Connector management from receiving relevant information to assist in the management and improvement of the operations of the authority and prevents auditors from receiving documentation to support audits that review the performance of the Connector. Based on its overall response, the Connector is taking measures to address our concerns regarding this matter.