COVERED CALIFORNIA

MEMORANDUM

June 19, 2025

TO: Allison Pease, Director
Office of Legal Affairs

FROM: Kirk Marston, Chief Audit Executive
Program Integrity Division, Office of Audit Services

RE: Office of Legal Affairs – Final Audit Report –
State Privacy Requirements Audit (Assignment # 2425.02)

In accordance with the Fiscal Year 2024-25 Internal Audit Plan that was approved by Covered California's Audit Committee in August 2024, the Office of Audit Services conducted an audit to assess the Privacy Office's compliance with state privacy requirements for the period of July 1, 2023, through June 30, 2024. Our report of this audit is attached.

We appreciate the cooperation and assistance of the Office of Legal Affairs management and staff during our audit. If you have any questions regarding this report, please contact me at 916-954-3498 or kirk.marston@covered.ca.gov.

Cc: Executive Office
Jessica Altman, Executive Director
Brandon Ross, General Counsel, Program Compliance & Accountability

Office of Legal Affairs
Natalie Smith, Deputy Director
Margaret Porto, Privacy Officer

Program Integrity Division
Thien Lam, Director
Kevin Cathy, Branch Chief, Office of Audit Services
Alicia Watts, Section Chief, Office of Audit Services
Kurt Faubion, Audit Manager, Office of Audit Services
Ramen Singh, Lead Internal Auditor, Office of Audit Services
Gurpreet Dhillon, Assisting Internal Auditor, Office of Audit Services

REVIEW OF STATE PRIVACY REQUIREMENTS

COVERED CALIFORNIA
OFFICE OF LEGAL AFFAIRS

FINAL AUDIT REPORT

ISSUED ON:
JUNE 19, 2025

PREPARED BY:
COVERED CALIFORNIA
PROGRAM INTEGRITY DIVISION
OFFICE OF AUDIT SERVICES

AUDIT TEAM:
KIRK MARSTON, CHIEF AUDIT EXECUTIVE
KEVIN CATHY, BRANCH CHIEF
ALICIA WATTS, SECTION CHIEF
KURT FAUBION, AUDIT MANAGER
RAMEN SINGH, INTERNAL AUDITOR
GURPREET DHILLON, INTERNAL AUDITOR

Table of Contents

Executive Summary

Objective and Scope

The Office of Audit Services conducted an audit to assess the Privacy Office's compliance with state privacy requirements protecting consumer personally identifiable information for the period of July 1, 2023, through June 30, 2024.

Positive Observations

The following are areas we noted with reasonable assurance where the Privacy Office established effective controls to ensure Covered California complies with state privacy requirements:

- The Privacy Office effectively tracks privacy incidents and ensures consumers are notified timely, which reflects Covered California's commitment to protecting consumer information.

- The Privacy Office established a robust set of policies, which helps ensure Covered California employees comply with state privacy requirements.

- The Privacy Office designed Covered California's privacy and information security training to include state privacy requirement topics, which helps ensure employees are knowledgeable of and comply with the requirements.

Reportable Condition(s)

We noted some matters below that we consider to be reportable under the *Global Internal Audit Standards:*

- **The Privacy Office did not provide adequate oversight of contractors who access personally identifiable information**

- **The Privacy Office did not track and monitor Workforce training activities to ensure compliance with training requirements**

Follow-up

The Office of Audit Services will follow up with management on their progress of corrective action plans and will report updates accordingly to the Audit Committee. A follow-up audit may be performed to determine the completion and adequacy of the corrective action plans.

Background, Objective, Scope, and Methodology

Background

The Office of Legal Affairs ensures Covered California's compliance with laws and mitigates risk. It provides guidance on statutes and regulations pertaining to Covered California and collaborates with state and federal regulatory agencies. Additionally, it supports Covered California's efforts to develop a comprehensive data strategy that will better define how the organization will collect, manage, and access data to provide robust security and privacy protections, manage risk, and facilitate effective decision making.

Under California law, Covered California is required to comply with the Information Practices Act. The Privacy Office, within the Office of Legal Affairs, is responsible for the development and implementation of privacy policies and procedures in accordance with federal and state laws. The Privacy Office works with the Information Security Office to protect the confidentiality of consumers' personally identifiable information (PII) through the enforcement of federal and state privacy-related legal requirements.

To ensure compliance with state privacy requirements, the Privacy Office is responsible for employee privacy training, privacy incident reporting, and proposed remedial measures. It also oversees privacy-related contracts with non-exchange entities, the permissible use of PII, consumer privacy inquiries, and privacy-related communications between Covered California and federal oversight agencies.

Objective

The objective of this audit was to assess the Privacy Office's compliance with state privacy requirements protecting consumers' PII.

Scope

The scope of this audit covered the Privacy Office's policies, procedures, and records for the period of July 1, 2023, through June 30, 2024.

Methodology

Our evaluation included gaining an understanding of the Privacy Office's policies and procedures as they relate to the state privacy requirements. Additionally, audit procedures were performed to determine whether Privacy Office management and staff are effectively and efficiently ensuring Covered California adheres to state privacy requirements.

Results

Positive Observations

The following are areas we noted with reasonable assurance where the Privacy Office established effective controls to ensure Covered California complies with state privacy requirements:

- The Privacy Office effectively tracks privacy incidents and ensures consumers are notified timely, which reflects Covered California's commitment to protecting consumer information.

- The Privacy Office established a robust set of policies, which helps ensure Covered California employees comply with state privacy requirements.

- The Privacy Office designed Covered California's privacy and information security training to include state privacy requirement topics, which helps ensure employees are knowledgeable of and comply with the requirements.

Findings & Recommendations

Finding #1 – The Privacy Office did not provide adequate oversight of contractors who access personally identifiable information

Finding Rating:	Priority	High	Medium	Low

Condition
We reviewed the Privacy Office's oversight of contractors who access PII and found that the Privacy Office did not:

- Maintain a log of agreements and contracts with contractors that involved the disclosure or use of PII.
- Ensure that PII was returned or destroyed in accordance with the provisions once agreements and contracts were terminated.
- Ensure that contractors completed the required privacy and information security training.

Criteria
Civil Code, Information Practices Act of 1977, section 1798.19 states, "Each agency when it provides by contract for the operation or maintenance of records containing personal information to accomplish an agency function, shall cause, consistent with its authority, the requirements of this chapter to be applied to those records."

Privacy Standards Guide, section 14.4 - Contract Review and Oversight states, in part, "Covered California shall maintain a log of all agreements or contracts which involve the disclosure or use of PII, and the Privacy Officer shall periodically review the log to ensure PII is either returned or destroyed."

Privacy Standards Guide, section 11 - Privacy Training states, in part, "The Privacy and Information Security Officer shall likewise develop the content for and oversee the implementation of Exchange/CC privacy and security awareness training for Non-Exchange Entities which are provided access to consumer PII."

Cause
The Privacy Office asserted that the policies within the Privacy Standards Guide for adequate oversight of contractors were not operationalized due to resource limitations.

Effect
By not providing adequate oversight of contractors who access PII, there is a risk that contractors are not in compliance with Covered California's Privacy Standards Guide. This could result in possible data breaches, unauthorized access to personal information, reputational damage, and legal and regulatory issues.

Recommendation
The Privacy Office should establish and implement procedures aligned with the Privacy Standards Guide to ensure proper contractor oversight.

Finding #2 – The Privacy Office did not track and monitor Workforce training activities to ensure compliance with training requirements

Finding Rating:	Priority	High	Medium	Low

Condition
The Privacy Office did not track and monitor privacy and information security awareness training compliance, as required by Covered California's Privacy Standards Guide. We reviewed the training records of 42 Covered California employees and identified that:

- 34 employees did not complete the training by the required due date.
- One new employee did not complete the training within the required three-day window from their hire date.

Criteria
Civil Code, Information Practices Act of 1977, section 1798.20 states, in part, "Each agency shall establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information and instruct each such person with respect to such rules and the requirements of this chapter, including any other rules and procedures adopted pursuant to this chapter and the remedies and penalties for noncompliance."

Privacy Standards Guide, section 11.6 - Privacy Training states, in part, "The Privacy Officer and Information Security Officer or their designee shall develop and oversee content development for Workforce privacy and information security awareness training and shall track and monitor Workforce training activities to ensure compliance with training requirements and to assess the general effectiveness of the training content."

Cause
While the Privacy Office shares responsibility with Covered California University and supervisors/managers to ensure employees complete the required training, there was a lack of resources within the Privacy Office to effectively fulfill this task.

Effect
By not monitoring completion of the required training, employees may not be aware of privacy rules, regulations, and the acceptable use policies. This can lead to misuse of data, PII exposure, data breaches, operational disruptions, legal and financial penalties, and reputational damage.

Recommendation
The Privacy Office should establish and implement procedures aligned with the Privacy Standards Guide to ensure employees complete the required privacy and information security awareness training.

Conclusion

During our audit, the Privacy Office has been working towards further improving Covered California's compliance with state privacy requirements. However, as shown in the two findings we identified, opportunities exist to lower the risk of unauthorized access or possible misuse of PII, reputational damage, and legal and regulatory issues from occurring. In general, one finding is rated as high risk and one finding is rated as medium risk due to potential negative impacts to Covered California's reputation, consumer trust, and protection of consumer PII.

Management Response

Presented below is the Privacy Office's management response to the findings which include their corrective action plans.

Finding 1:	The Privacy Office did not provide adequate oversight of contractors who access personally identifiable information
Recommendation 1:	The Privacy Office should establish and implement procedures aligned with the Privacy Standards Guide to ensure proper contractor oversight.
Privacy Office Management Response/ Corrective Action:	The Privacy Office anticipates completion of any changes to the Privacy Standards Guide by the end of December 2025 and full implementation of aligning procedures by the end of June 2026.
Targeted Completion Date:	June 30, 2026

Finding 2:	The Privacy Office did not track and monitor Workforce training activities to ensure compliance with training requirements
Recommendation 2:	The Privacy Office should establish and implement procedures aligned with the Privacy Standards Guide to ensure employees complete the required privacy and information security awareness training.
Privacy Office Management Response/ Corrective Action:	The Privacy Office anticipates substantial compliance with the training requirements by the end of December 2025 and full implementation of new training compliance processes by the end of June 2026.
Targeted Completion Date:	June 30, 2026

Evaluation of Response

The corrective action plans provided by the Privacy Office, if implemented as intended, should be sufficient to correct the reportable conditions noted. The Office of Audit Services will conduct quarterly follow-ups to provide reasonable assurance that the corrective action plans have been implemented and are operating as designed. Additionally, a follow-up audit may be performed to determine the completion and adequacy of the correction action plans.

We thank the Privacy Office for their help and cooperation during this audit.

APPENDIX A

Finding Ratings

Finding	Priority	High	Medium	Low
1. The Privacy Office did not provide adequate oversight of contractors who access personally identifiable information		**X**		
2. The Privacy Office did not track and monitor Workforce training activities to ensure compliance with training requirements			**X**	

Rating Definitions

Priority	Immediate and on-going threat to the achievement of division or Covered California strategic goals and objectives. In particular: - Significant adverse impact on reputation - Non-compliance with statutory requirements - Potential or known financial losses - Substantially raising the likelihood that risks will occur Management must implement corrective actions as soon as possible and monitor the effectiveness.
High	High probability of adverse effects to the division or Covered California as a whole. Management must put in place corrective actions within a reasonable timeframe and monitor the effectiveness of the corrective actions. - High potential for adverse impact on reputation - Increase in the possibility of financial losses - Increase in the likelihood that risks may occur
Medium	Medium probability of adverse effects to the division or Covered California as a whole. Management must put in place corrective actions within a reasonable timeframe and monitor the effectiveness of the corrective actions. - Medium potential for adverse impact on reputation - Potential increase in the likelihood that risks may occur
Low	Low probability of adverse effects to the division or Covered California as a whole, but that represent an opportunity for improving the efficiency of existing processes. Correcting this will improve the efficiency and/or effectiveness of the internal control system and further reduce the likelihood that risks may occur.