Introduced: 7/31/2026
Version: 1

Current Status: Agenda Ready
Matter Type: Preliminary Analysis Report

a. Receive a preliminary report to Board Referral Number 2026.13 (Askew) to strengthen County contract standards for data privacy, data sharing, and protection against unauthorized secondary use of County information for departments that procure or manage technology, software, data, or information services.
b. Direct County departments to continue efforts to strengthen County contract standards, data privacy, security, and Artificial Intelligence governance practices:
1. Update the County Standard Agreement, including the Agreement for Professional Services, to incorporate appropriate data privacy, security, and AI-related requirements.
2. Work with County Counsel to evaluate and develop minimum data privacy and security requirements for non-standard agreements, as appropriate.
3. Reestablish a consistent centralized review process for technology-related contracts to support evaluation of data privacy, security, AI, and other technology-related risks.
4. Develop a countywide data privacy and AI governance framework, including consideration of a countywide data privacy policy and continued promotion of the County Generative AI Policy across County departments.
5. Continue collaboration among PWFP, ITD, and County Counsel to complete the Countywide Records Retention, Storage, and Disposition Policy.
c. Provide further direction within the Board's discretion consistent with the scope of the Board Referral.

RECOMMENDATION:

a. Receive a preliminary report to Board Referral Number 2026.13 (Askew) to strengthen County contract standards for data privacy, data sharing, and protection against unauthorized secondary use of County information for departments that procure or manage technology, software, data, or information services.
b. Direct County departments to continue efforts to strengthen County contract standards, data privacy, security, and Artificial Intelligence governance practices:
1. Update the County Standard Agreement, including the Agreement for Professional Services, to incorporate appropriate data privacy, security, and AI-related requirements.
2. Work with County Counsel to evaluate and develop minimum data privacy and security requirements for non-standard agreements, as appropriate.
3. Reestablish a consistent centralized review process for technology-related contracts to support evaluation of data privacy, security, AI, and other technology-related risks.

4. Develop a countywide data privacy and AI governance framework, including consideration of a countywide data privacy policy and continued promotion of the County Generative AI Policy across County departments.
5. Continue collaboration among PWFP, ITD, and County Counsel to complete the Countywide Records Retention, Storage, and Disposition Policy.
c. Provide further direction within the Board's discretion consistent with the scope of the Board Referral.

SUMMARY:
The Board Referral directs the County to strengthen County contract standards, data privacy governance, and protections against unauthorized secondary use of County information. To address the Referral, the County will enhance contract requirements, establish consistent technology contract review practices, develop countywide data privacy and artificial intelligence (AI) governance standards, promote responsible use of AI technologies, and complete the Countywide Records Retention, Storage, and Disposition Policy in collaboration with County departments.

DISCUSSION:
Background

The County of Monterey (County) relies on technology vendors, cloud services, data platforms, AI tools, and other third-party contractors to support County operations and public services. These partnerships require stronger contract standards, data privacy protections, security controls, and AI governance practices to ensure County information is properly accessed, used, shared, retained, and protected.

As technology evolves, County agreements and governance frameworks must address risks related to AI, automated decision-making, cloud services, and data use, including vendor responsibilities, subcontractor access, AI use, retention, breach notification, and protection against unauthorized disclosure or secondary use of County and resident information.

Referral Scope

The Referral requested a review of current County contract safeguards, including data privacy and security provisions, AI-related procurement requirements, and protections against unauthorized secondary use of County data, to identify gaps and opportunities to enhance County contract standards.

The Referral also requested recommendations for updates to County contract templates, procurement policies, and administrative procedures to ensure procurement practices keep pace with evolving technologies and emerging privacy risks, while considering fiscal, legal, operational, and technology impacts.

Additionally, the Referral requested the development of countywide standards to protect County-held data, including resident data, personally identifiable information (PII), and other sensitive information.

This includes incorporating best practices from peer jurisdictions, establishing data privacy and governance standards, strengthening vendor oversight, audit rights, and transparency related to subcontractors, AI tools, and data sharing, and defining data retention and disposal requirements.

Approach

In response to the Referral, the Information Technology Department (ITD) worked collaboratively with the County Administrative Office's (CAO) Contracts and Purchasing division, County Counsel, Public Works, Facilities and Parks (PWFP), and other participating County departments, representing a total of 20 County departments and offices. The collaborative review included evaluating applicable laws and regulations affecting County data privacy, information protection, public records obligations, and emerging AI governance considerations; reviewing current County contract templates and policies; collecting existing contract templates and use cases to assess current practices, identify gaps, and develop opportunities for enhancement; and reviewing peer jurisdiction practices to develop recommended data privacy, security, and AI governance practices for the County.

Legal and Regulatory Requirements

The review identified key laws and regulatory requirements relevant to County data privacy, information protection, public records obligations, and emerging AI governance considerations. Major requirements include the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), which establish privacy rights, transparency obligations, data protection requirements, and considerations related to automated decision-making technologies that are increasingly relevant to the responsible procurement and governance of AI systems.

Additional requirements include the California Public Records Act, Children's Internet Protection Act (CIPA), California Civil Code data broker registration requirements, Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Internal Revenue Service (IRS) data protection requirements for the Department of Child Support Services (DCSS), and applicable provisions of the Welfare and Institutions Code.

Together, these laws and regulations provide the foundation for County data privacy, security, and governance practices. They highlight the need for consistent countywide standards, vendor oversight, responsible data use practices, and governance frameworks that address evolving technologies, including AI, while ensuring compliance with applicable legal and regulatory requirements.

Current Contract Safeguards and Identified Opportunities

The review included County Standard Agreements, including Agreements for Professional Services, associated exhibits, County non-standard agreement process, and contract use cases provided by participating County departments.

The review found that current "Records and Confidentiality" clauses in the County Standard Agreement include general provisions, with opportunities to strengthen data privacy and security requirements. Standard agreements and associated exhibits could be enhanced to include consistent

requirements for data privacy, security, and the responsible procurement and use of AI technologies. County non-standard agreements could benefit from consistent minimum data privacy and security requirements.

Departments currently use confidentiality, data privacy, and security exhibits tailored to their specific agreement needs. When requested, ITD provides contract review support to help ensure appropriate data privacy, security, and technology considerations are addressed. However, a centralized technology contract review process is not consistently followed to evaluate data privacy, security, AI, and other technology-related risks across County agreements.

Peer Jurisdiction Data Privacy and Governance Review

The review team examined data privacy, security, and AI governance practices from seven peer jurisdictions, including the counties of Alameda, Los Angeles, Sacramento, San Bernardino, San Diego, Santa Clara, and Orange. The review identified varying governance models, with countywide privacy programs led by IT, Risk Management, Ethics and Compliance, or executive leadership. Several jurisdictions have established dedicated privacy offices, published privacy and Generative AI (GenAI) policies, or developed AI governance frameworks. The review also found that some jurisdictions maintain department-level responsibility for data management and compliance while providing centralized guidance, oversight, and governance for emerging technologies.

Current County Data Privacy and Governance Practices

The County's current practice is that departments manage their own data governance and business-specific data requirements. ITD provides the technology solutions, security controls, and technical guidance necessary to support departments in meeting their data governance and regulatory obligations. Upon department request, the Chief Information Officer's (CIO) Office provides data privacy, AI, and technology reviews, while the Chief Security Officer (CSO) provides cybersecurity reviews, security governance, and oversight.

Recommended Improvements

The review team recommends strengthening County contract standards and establishing a more consistent countywide data privacy governance framework. Recommended improvements include:

1. Update the County Standard Agreement, including the Agreement for Professional Services, to incorporate appropriate data privacy, security, and AI-related requirements.
2. Work with County Counsel to evaluate and develop minimum data privacy and security requirements for non-standard agreements, as appropriate.
3. Reestablish a consistent centralized review process for technology-related contracts to support evaluation of data privacy, security, AI, and other technology-related risks.
4. Develop a countywide data privacy and AI governance framework, including consideration of a countywide data privacy policy and continued promotion of the County Generative AI Policy across County departments.
5. Continue collaboration among PWFP, ITD, and County Counsel to complete the Countywide Records Retention, Storage, and Disposition Policy.

Fiscal, Legal, Operational, and Technology Impacts and Benefits

Implementation of the recommendations is expected to have limited fiscal impacts, primarily associated with staff time for policy development, contract updates, and implementation. Legal impacts include collaboration with County Counsel to update contract language and ensure compliance with applicable laws and regulations. Operational impacts include standardizing contract review processes, establishing countywide data privacy and AI governance practices, and coordinating implementation across County departments. Technology impacts include incorporating data privacy, security, and AI risk assessments into existing procurement and contract review processes.

These recommendations will strengthen protection of County and resident information, improve consistency across County contracts, reduce privacy and technology risks, enhance vendor accountability, support responsible AI governance, and establish consistent countywide data privacy and governance standards.

OTHER AGENCY INVOLVEMENT/COMMITTEE ACTIONS:
The Information Technology Department has coordinated with County Counsel, the County Administrative Office, Contracts and Purchasing, and Public Works, Facilities and Parks Departments to develop the report.

FINANCING:
Implementation of the recommendations is expected to have limited fiscal impacts, primarily associated with staff time for policy development, contract updates, and implementation.

BOARD OF SUPERVISORS STRATEGIC PLAN GOALS:
This strategy supports well-being and quality of life by protecting residents' personal and sensitive information and strengthening public trust in County services. It supports a diverse and thriving economy by promoting clear, consistent, and transparent vendor expectations that allow responsible innovation while protecting County data. It also supports safe and resilient communities by reducing privacy, cybersecurity, and vendor-related risks, and preserving County control over information collected through County programs and services.

X Well-Being and Quality of Life
__ Sustainable Infrastructure for the Present and Future
X Safe and Resilient Communities
X Diverse and Thriving Economy
__ Dynamic Organization and Employer of Choice

Prepared by: Alex Zheng, Deputy Chief Information Office, 759-6991

Approved by: Eric A. Chatham, Chief Information Officer, 759-6920

Attachments:
1. 2026.13 (Askew) Protection Against Unauthorized Secondary Use of County

Information

2. Referral #2026.13_Presentation