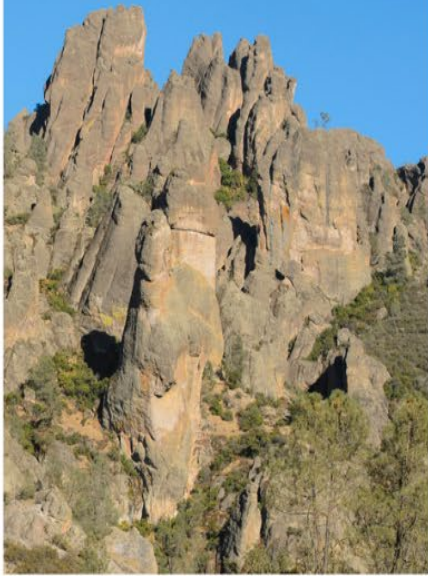




Preliminary Response Referral #2026.13

Strengthening Data Privacy and Contract Standards to Protect County-held Data

August 11, 2026
CAO's Office, County Counsel and ITD

Preliminary Response Referral #2026.13

Purpose

- **Maintain clear countywide standards, oversight, and safeguards to ensure technological innovation aligns with the County's commitment to:**
 - Protect privacy
 - Respect civil liberties
 - Promote transparency
 - Maintain public trust
 - Steward public information responsibly

Preliminary Response Referral #2026.13

Requested Deliverables

- **Deliverable #1. Review current County contract safeguards**
 - Review data privacy and security provisions
 - Review artificial intelligence (AI) related procurement requirements
 - Assess whether existing contracts adequately protect against unauthorized secondary use of County data
 - Identify any gaps or opportunities for enhancement

Preliminary Response Referral #2026.13

Requested Deliverables

- **Deliverable #2. Recommend updates to County contract templates, procurement policies, and administrative procedures**
 - Develop necessary updates to County contract templates, procurement policies, and administrative procedures
 - Identify any fiscal, legal, operational, or technology impacts associated with implementation
 - Ensure procurement practices keep pace with evolving technologies & emerging privacy risks

Preliminary Response Referral #2026.13

Requested Deliverables

- **Deliverable #3. Recommend countywide standards to protect County-held data including resident data, PII and sensitive data**
 - Incorporate best practices from peer jurisdictions
 - Establish data privacy & data governance standards
 - Require vendor oversight, audit rights, and transparency for subcontractors, AI tools, & data sharing
 - Establish data retention & disposal requirements

Preliminary Response Referral #2026.13

Deliverable #1. Review Current County Contract Safeguards

- Collaborated with County departments to collect existing contract templates and use cases
- Reviewed current County contract templates and policies
- Identified relevant laws and regulations affecting County data privacy (see Appendix I)

Preliminary Response Referral #2026.13

Deliverable #1. Review Current County Contract Safeguards

Initial Observations

- County Standard Agreement including Agreement for Professional Services
 - Current “Records and Confidentiality” clauses include general provisions, with opportunities to strengthen data privacy, and security requirements
 - Agreement could be enhanced to include consistent requirements for the procurement and responsible use of AI technologies
- County non-standard agreement
 - Agreement can benefit from consistent minimum data privacy and security requirements

Preliminary Response Referral #2026.13

Deliverable #1. Review Current County Contract Safeguards

Initial Observations

- Departments 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 and security considerations are addressed
- Centralized technology contract review process by ITD is not followed consistently to evaluate data privacy, security, AI, and other technology risks

Preliminary Response Referral #2026.13

Deliverable #2. Recommend Updates to Contract Templates, Policies and Procedures

- Update the County Standard Agreement, including the Agreement for Professional Services
 - Create a standard exhibit for data privacy, security, and protection requirements
 - Create a standard exhibit for artificial intelligence (AI) system requirements
- Explore establishing minimum requirements for non-standard contracts in collaboration with County Counsel
- Implement centralized review process by ITD, for technology-related contracts to evaluate privacy, security, AI, and other technology risks

Preliminary Response Referral #2026.13

Deliverable #3. Recommend Standards to Protect County-held Data

- Reviewed best practices on data privacy and security practice from seven peer jurisdictions (Appendix II)
 - Alameda County
 - LA County
 - Sacramento County
 - San Bernardino County
 - San Diego County
 - Santa Clara County
 - Orange County

Preliminary Response Referral #2026.13

Deliverable #3. Recommend Standards to Protect County-held Data

- **Monterey County current practice**
 - Departments manage their own data governance and business-specific data requirements
- **ITD**
 - Implements technology solutions and security controls that enable departments to meet their data governance and regulatory requirements
 - When requested, CIO office provides data privacy, AI and technology review
 - Chief Security Officer (CSO) provides cybersecurity review, security governance, and oversight

Preliminary Response Referral #2026.13

Deliverable #3. Recommend Standards to Protect County-held Data

- Establish a countywide data privacy and governance framework
 - Develop a countywide data privacy policy
 - Establish AI governance as part of the framework, including:
 - Responsible procurement and use of AI technologies
 - AI risk assessment and security review
 - Promote consistent adoption of the County Generative AI (GenAI) Policy across County departments
- Complete Countywide Records Retention, Storage, and Disposition Policy development by PWFP, ITD and County Counsel

Preliminary Response Referral #2026.13

Next Steps

- Update County Standard Agreement, including the Agreement for Professional Services with privacy, security, and AI exhibits
- Work with County Counsel, explore developing minimum data privacy and security requirements for non-standard contracts
- Reestablish consistent centralized review process for technology-related contracts
- Develop countywide data privacy policy
- Complete Countywide Records Retention, Storage, and Disposition Policy development by PWFP, ITD and County Counsel

Questions?



Preliminary Response Referral #2026.13

Appendix I. Legal and Regulatory Requirements Affecting Data Privacy

- California Consumer Privacy Act (CCPA)
- California general subpoena related laws and procedures
- California Privacy Rights Act (CPRA)
- California Public Records Act
- Children's Internet Protection Act (CIPA)
- Civil code regarding data brokerage registration (Civil Code 1798.99.80)
- Criminal Justice Information Services (CJIS)
- Health Insurance Portability and Accountability Act (HIPAA)
- IRS codes for DCSS
- Welfare Institutions code

Preliminary Response Referral #2026.13

Appendix II. Peer Jurisdictions Data Privacy and Security Practice

- **Alameda County**
 - Countywide Privacy Compliance Office under Risk Management
 - County publishes GenAI policy and Privacy Statement
- **Los Angeles County**
 - Countywide privacy program led by IT
 - AI policy and governance framework led by IT
- **Orange County**
 - Countywide privacy program led by IT
- **San Diego County**
 - Departments retain responsibility for data management and regulatory compliance
 - AI governance framework led by IT

Preliminary Response Referral #2026.13

Appendix II. Peer Jurisdictions Data Privacy and Security Practice

- **Sacramento County**
 - Office of Compliance & HIPAA under IT
 - Departments responsible for data classification/retention & AI policy
- **San Bernardino County**
 - Countywide privacy and compliance program led by the Office of Ethics and Compliance
- **Santa Clara County**
 - County Privacy Office led by CEO
 - AI governance framework in development

Preliminary Response Referral #2026.13

Appendix III. Proposed Data Governance Roles and Responsibilities

Function	Primary Responsibility	Owner
Data Governance	Establishes the overarching framework, policies, roles, and accountability for managing County data.	· Executive Sponsor: County Administrative Office (CAO) · Program Lead: ITD · Privacy & Security Lead: Chief Security Officer (CSO) · Governance Body: Cross-department Data Governance team
Data Privacy	Ensures data is collected, used, shared, and retained appropriately and in compliance with privacy requirements.	Departments by working with IT Security
Data Security	Protects data through technical and administrative controls, including access management and monitoring.	Departments by working with IT Security
Data Owners & Stewards	Defines data accountability, quality expectations, and appropriate business use.	Departments

Preliminary Response Referral #2026.13

Appendix III. Proposed Data Governance Roles and Responsibilities

Function	Primary Responsibility	Owner
Data Retention and Disposal	Governs data retention, archival, and disposition requirements.	Retention schedule in progress by PWFP, County Counsel and ITD Departments
Contracts & Purchasing	Ensures vendors meet County data privacy, security, and usage requirements through contracts.	Contracts & Purchasing Departments
Legal	Provides guidance on regulatory, contractual, and legal obligations. Ensures compliance with laws, regulations and County policies	County Counsel
Information Technology	Security and technology oversight. Implements technology solutions and controls to support governance requirements.	ITD