

HIGH STAKES OF THE CALIFORNIA PUBLIC RECORDS ACT PROTECTING YOUR AGENCY AND HANDLING DIFFICULT REQUESTS

Introduction and Background

The California Public Records Act (“CPRA”), codified at Government Code §7920.000 *et seq.*, was enacted in 1968. The CPRA is one of two “Sunshine Laws” in California aimed at promoting government transparency and accountability. In 2021, after decades of piecemeal amendments, which rendered the statute increasingly complex, the Legislature recodified the CPRA.¹ The recodification did not substantively alter the CPRA but rather reorganized a series of statutes that had become fragmented and difficult to navigate. The recodification resulted in an easier to use and understand statute.² The CPRA applies broadly to all state and local agencies³ in California and broadly defines public records to include any writing⁴ related to the public’s business, regardless of physical form or characteristics. The CPRA further guarantees broad access rights to the public, while also providing exemptions to protect certain sensitive information and a mechanism to ensure compliance through judicial remedies.

Overarching Goals:

- Ensure government transparency and accountability through access to public records.
- Promote civic participation and government oversight.
- Balance public access rights with individual privacy concerns.

This *High Stakes of the California Public Records Act* training introduces the CPRA and examines its legal framework, common pitfalls, and compliance challenges, while offering strategies for public agencies to strengthen compliance, reduce risk, manage complex or burdensome requests, handle difficult requesters, and maintain public trust.

Legal Framework

Ratified in 1968, the CPRA grants the public broad access rights to information generated by public agencies. Founded on the principle that government activities must be conducted openly and transparently, the CPRA empowers the public to understand how public officials make decisions and hold them accountable for their actions. Over time, there have been changes to the CPRA, but the underlying intent has remained consistent. Passed in 2004, Proposition 59 amended Article I of the California Constitution, further strengthening the CPRA. With its passage, the public’s right to access records was enshrined in Article I of the California Constitution:

¹ Gov. Code, §7920.005 “CPRA Recodification Act of 2021”

² Gov. Code, §§7920.100-7920.120

³ Gov. Code, §7920.540

⁴ Gov. Code, §7920.545

“The people have the right of access to information concerning the conduct of the people’s business, and, therefore, the meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny.”⁵

In 2023, the CPRA was recodified to improve usability and clarity.

Purpose

The CPRA’s sole function is to provide for the disclosure of identifiable public records. It is not a records retention, destruction, privacy, or usage statute. The CPRA does not dictate what information agencies may collect or how long they must maintain it; instead, it governs what must be disclosed once records exist.

In *Los Angeles Police Dept. v. Superior Court* (1977), the court stated the CPRA “*does not undertake to prescribe what type of information a public agency may gather, nor to designate the type of records such an agency may keep, nor to provide a method of correcting such records. Its sole function is to provide for disclosure.*”⁶

Scope

The CPRA applies to all state and local agencies in California, including departments, boards, commissions, and city councils.⁷

A “public record” is defined broadly within the CPRA.

- **Public Record:** A “public record” is “*any writing containing information relating to the conduct of the public’s business prepared, owned, used, or retained by any state or local agency, regardless of physical form or characteristics.*”⁸
- **Writing:** A “writing” is defined as “*any handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.*”⁹

An agency may possess a record through “actual” possession (a record that is in an agency file, on an agency computer, or in the agency’s computer system) or “constructive” possession (the agency has the right to control the record either directly or through another person).¹⁰

⁵ Cal. Const., art I, §3, sub (b)

⁶ *Los Angeles Police Dept. v. Superior Court* (1977) 65 Cal.App.3d 661,668

⁷ Gov. Code, §§ 7920.510, 7920.525, 7920.540

⁸ Gov. Code, §7920.530

⁹ Gov. Code, §7920.545, *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608,618-619

¹⁰ *Board of Pilot Comrs. for the Bays of San Francisco, San Pablo and Suisun v. Superior Court* (2013) 218 Cal.App.4th 577,598; *Consolidated Irrigation Dist. v. Superior Court* (2012) 205 Cal.App.4th 697,710

Access Rights

Under the CPRA, every “person” (individuals, corporations, partnerships, LLCs, or associations)¹¹ has the right to inspect public records during a local agency’s office hours (subject to certain exemptions¹²), and the right to promptly receive copies of public records¹³.

- Person: A “person” is defined as any natural person, corporation, partnership, limited liability company, firm, or association. A “person” is not required to disclose their identity to access public records.¹⁴

The CPRA does not require a requester to disclose their purpose for making the request. If a requester shares their purpose for requesting a record, the CPRA does not allow limitations on access to a public record based on their stated purpose, if the record is otherwise subject to disclosure.¹⁵

Exemptions

Both the CPRA and the California Constitution require that public writings be open to public scrutiny. While disclosure is the general rule, the CPRA provides a list of specific statutory exemptions that allow agencies to withhold certain categories of records or information. In constructing the exemptions, the Legislature recognized that public access to information must sometimes yield to competing public interests, chief among them being the right to privacy. The following are some of the most common exemptions:

- Personnel and Medical Records: The CPRA does not require disclosure of personnel, medical, or similar files that would constitute an unwarranted invasion of personal privacy.¹⁶
- Criminal Investigatory Records: The CPRA shields records related to criminal investigations to protect law enforcement processes and individual privacy.¹⁷
- Utility Customer Data: The CPRA does not generally require the disclosure of private information, such as a utility customer’s name, credit history, utility usage data, home address, or telephone number.¹⁸
- Pending Litigation: Records created for litigation purposes are generally exempt from disclosure; however, this exemption is not absolute and is subject to specific conditions. The exemption only applies until the subject litigation is adjudicated or otherwise settled.¹⁹

¹¹ Gov. Code, §7920.520

¹² Gov. Code, §7922.525

¹³ Gov. Code, §7922.530(a)

¹⁴ Gov. Code, §7920.520

¹⁵ Gov. Code, §7921.300

¹⁶ Gov. Code, §7927.700

¹⁷ Gov. Code, §§7923.600-7923.625

¹⁸ Gov. Code, §7927.410

¹⁹ Gov. Code, §7927.200

- Voter Information: The CPRA prohibits the disclosure of voter information, including home address, telephone number, email address, precinct number, or any other number specified by the Secretary of State for voter registration purposes.²⁰
- Taxpayer Information: The CPRA does not require disclosure of taxpayer information.²¹
- Other Records Protected by Law from Disclosure: The CPRA incorporates provisions of federal and state law that regulate the disclosure of records or information,²² including:
 - Attorney-Client Privilege
 - Attorney Work Product
 - Trade Secrets
 - Copyright
- Catch-all Exemption: The CPRA allows public agencies to justify withholding public records by independently balancing the public interests in disclosure and nondisclosure. In order to assert the catch-all exemption, a public agency must demonstrate that the public interest served by nondisclosure *clearly* outweighs the public interest served by disclosure based on the facts surrounding that particular record.²³ While the exemption is applied in good faith, an agency should be prepared to support its decision with a well-reasoned and documented justification. Consequently, agencies should exercise caution when using this exemption, as courts have consistently warned that it should not be employed as a matter of convenience or to shield records.

Unlike the more specific exemptions enumerated in the CPRA, the catch-all exemption is intentionally broad and flexible, designed to address situations the Legislature could not have anticipated.²⁴

Request Process

A CPRA request may take various forms. For example, the CPRA does not require requesters to submit their requests in writing. A request may be made in writing, verbally, or through another means of communication. While an agency may encourage written requests to promote accuracy, it cannot mandate them. Agencies may offer an online portal for submitting requests, but use of the portal must be optional. If a requester makes a verbal request, the agency may memorialize the request in writing or complete any agency-required forms on the requester's behalf.

Response Requirements: Within 10 days after a CPRA request is received, an agency must respond with one of the following²⁵:

²⁰ Gov. Code, §7924.000

²¹ Gov. Code, §7925.000

²² Gov. Code, §7927.705

²³ Gov. Code, §7922.000

²⁴ *Id.*

²⁵ Gov. Code, §7922.535

- *Production Letter*: accompanies any provided records.²⁶
- *Denial Letter*: informs the requester that the records sought do not exist or are exempt from disclosure, and provides the basis for the exemption.²⁷ The denial letter must be in writing and include the name and title of the person responsible for the denial determination.²⁸
- *Determination Letter*: alerts the requester that responsive records exist and specifies the date by which they will receive the record(s).²⁹
- *Extension Letter*: provides the requester the update that the agency will extend its response deadline by up to 14 days, citing one of the statutory and factual bases below for the extension.³⁰
 - Reasons that justify a 14-day extension:
 1. The need to search for and collect the requested records from locations or organizations that are separate from the office processing the request.
 2. The need to search for, collect, and review a large volume of records.
 3. The need to consult with another agency having substantial interest in the determination of the request.
 4. The need to compile data, to write programming language or a computer program, or to construct a computer report to extract data.
 5. The need to search for, collect, and appropriately examine records during a state of emergency proclaimed by the Governor in the jurisdiction where the agency is located when the state of emergency currently affects, due to the state of emergency, the agency's ability to timely respond to requests due to staffing shortages or closure of facilities where the requested records are located.

Production Requirements: While agencies have strict statutory timelines for *responding* to requests, there is no similarly strict timeline for *producing* records. Records shall be made available “promptly.” For voluminous requests, agencies may release the records on a rolling basis, accompanied by a production letter that identifies any asserted exemptions and specifies the next date by which additional records are to be provided.³¹

In most cases, agencies have the option to provide the requested record in either electronic or paper form. However, a responding agency must provide an electronic copy when all of the following conditions are met:³²

- an electronic copy is requested.
- the record is subject to disclosure.

²⁶ Gov. Code, §7922.535

²⁷ Gov. Code, §7922.535

²⁸ Gov. Code, §7922.540

²⁹ Gov. Code, §7922.535

³⁰ Gov. Code, §7922.535

³¹ Gov. Code, §7922.530(a)

³² Gov. Code, §7922.570

- the agency holds the record in an electronic format (e.g., can be extracted from a database).
- the release of an electronic format does not compromise the security or integrity of the original record or jeopardize the proprietary software in which it is maintained.

Clarifying Requests and Assisting the Requester: If a CPRA request is unclear, the responding agency should request clarification. When examining a request for clarity, a responding agency must determine whether it describes identifiable records. A requester may identify an exact record, but is not required to do so. A requester may seek a record based on a description of the record's general content or provide specific criteria for its retrieval.

The CPRA requires agencies to assist requesters in making focused and effective requests that reasonably describe identifiable records in the agency's possession.³³

Judicial Remedies

The CPRA provides a legal remedy to requesters who believe they have been improperly denied access to records. This remedy is by way of a writ petition filed in superior court. A CPRA writ is a special kind of lawsuit used to enforce the mandate of access to public records.³⁴ Public agencies should be mindful that prevailing petitioners are entitled to recover attorney fees and costs.³⁵ Additionally, courts may order agencies to disclose records in compliance with the CPRA.

Evaluating Legal Risk and Exposure by Agencies

Common Pitfalls

Some common legal considerations and pitfalls arise under the CPRA whenever agencies seek to deny or delay responding to requests, as unjustified delays or blanket denials can expose them to litigation. Excessive redactions may also lead to legal disputes. Similarly, failure to respond within statutory deadlines is a frequent source of litigation and liability. Cost disputes can arise if an agency attempts to charge more than what is allowable for duplication or data extraction. Questions over the proper scope of disclosure often emerge when balancing privacy, security, and transparency obligations. Agencies must also weigh the public interest in evaluating whether to disclose records, as courts generally favor disclosure when public accountability is at stake.

Below are scenarios of common CPRA pitfalls:

Denial or Delay of Requests

Pitfall: Denying access to records or delaying responses without adequate justification can prompt a lawsuit to compel compliance.³⁶

³³ Gov. Code, §7922.600

³⁴ Gov. Code, §7923.100, *et seq.*

³⁵ Gov. Code, §7923.115

³⁶ *Rittiman v. Pub. Utilities Comm.* (2022) 80 Cal.App.5th 1018,1038

Scenario: A requester submits a written CPRA request seeking copies of any and all communications between agency staff and a vendor regarding the award of a contract. The agency is concerned that the release of the emails may generate public criticism, and delays responding to the request well beyond the statutory deadline. The agency eventually issues a denial letter, but does not cite any specific exemption or provide a legal justification for denying access. The requester, aware of their rights under the CPRA, files a CPRA writ to compel disclosure. The agency is now exposed to legal liability due to its failure to meet deadlines and its unsupported denial of access to public records.

Excessive Redactions

Pitfall: Excessively redacting documents that withhold information that requesters believe should be accessible under the CPRA can lead to disputes over transparency.³⁷

Scenario: A requester calls an agency's main number and requests copies of an internal policy that is used to guide agency staff in handling public complaints. The agency provides the document, but heavily redacts large sections, including routine operational procedures and contact information for agency offices (information that is readily available on the agency's website). The requester argues that the redactions are being used to conceal dishonest practices when responding to complaints, rather than to protect confidential information. The requester challenges the response and files a CPRA writ to gain access to the unredacted records. The agency is now exposed to legal liability due to excessive redactions.

Failure to Respond

Pitfall: Failing to respond to CPRA requests within the statutorily required timeframe can prompt legal action to enforce the requester's rights. If an agency fails to respond to a request at all, it may be considered a constructive denial of the request. The requester can treat the lack of response as a denial and can pursue remedies available under the CPRA.³⁸

Scenario: A requester submits a written CPRA request for records related to the agency's recent budget adoption. The request is properly directed to the agency's designated office. Still, due to an internal miscommunication, no acknowledgment or response is ever provided within the ten-day statutory period to the requester. From the requester's perspective, the silence constitutes a constructive denial under the CPRA. As a result, the requester files a lawsuit to compel disclosure. The agency is now exposed to legal liability due to its failure to respond to the requester.

Cost Disputes

Pitfall: Disputes can arise over fees charged for records retrieval, duplication, or mailing, especially if the requester believes the fees are excessive or not justified under CPRA guidelines.

³⁷ *BondGraham v. Superior Ct.* (2023) 95 Cal.App.5th 1006,1017-1018; *Long Beach Police Officers Assn. v. City of Long Beach* (2014) 59 Cal.4th59,67

³⁸ *County of San Benito v. Superior Court* (2023) 96 Cal.App.5th 243,264

The CPRA states that “*each state or local agency, upon a request for a copy of records that reasonably describes an identifiable record or records, shall make the records promptly available to any person upon payment of fees covering direct costs of duplication, or a statutory fee if applicable. Upon request, an exact copy shall be provided unless impracticable to do so.*”³⁹

Scenario: A requester submits a CPRA request through the agency’s CPRA portal on their website. The request seeks copies of environmental reports related to a recent development project that went to the planning commission for approval. The agency agrees to provide the records but informs the requester that the cost will be several hundred dollars, citing the time spent by staff searching for and reviewing the records. The requester, familiar with the CPRA’s fee provisions, objects because agencies may charge only for the direct cost of duplication or, in limited cases, for programming or data extraction, and not for staff review time. Believing the charges to be excessive and inconsistent with the statute, the requester challenges the fees. In this case, the agency is now exposed to legal liability due to its unreasonable fee assessment.

Compliance Challenges and Agency Burdens

The CPRA presents several compliance challenges for public agencies, as the law imposes strict deadlines, broad disclosure obligations, and unpredictable legal risks. Agencies must strike a balance between transparency and legitimate confidentiality concerns, often navigating complex exemptions involving privacy, privilege, or ongoing investigations. The rise of advanced technology has further complicated compliance, as courts are less sympathetic to claims that requests are overly broad or voluminous, given the availability of modern tools such as metadata searches and automated redaction. Attorney fee awards have also become increasingly unpredictable, with courts allowing limited discovery in CPRA litigation. Together, these factors create a high-risk environment where even minor missteps, such as delayed responses, excessive redactions, or improper fee assessments, can expose agencies to costly litigation. These challenges also tend to compound one another, creating a ripple effect that increases the likelihood of additional pitfalls and escalates overall risk.

Below are common CPRA-related compliance challenges and burdens facing public agencies:

Scope of Discovery

CPRA litigation has a unique scope of discovery as compared to other writs.⁴⁰ Typically, discovery is not available in writs. It is, however, available to CPRA litigants. Because discovery is often the most expensive and time-consuming phase of litigation and because attorney fees awards are at risk in CPRA writs, it can be challenging for agencies to accurately evaluate or predict their scope of exposure. This reality places a heavy burden on agencies, as the potential for court-ordered discovery creates yet another avenue for costs to rise when compliance is questioned. The need to collect, review, and produce large volumes of records under strict legal standards can strain staff capacity, increase attorney involvement, and lead to higher overall expenses. In practice, any writ may open the door to a discovery process that magnifies both financial and operational impacts well beyond the original request. In effect, even a relatively small

³⁹ Gov. Code, §7922.530

⁴⁰ *City of Los Angeles v. Superior Ct. (Anderson-Barker)* (2017) 9 Cal.App.5th 272,288

misstep in handling a CPRA request may trigger litigation costs that balloon far beyond expectations.

Attorneys' Fees

The monetary costs associated with CPRA litigation can be unpredictable. Even if a case is dismissed as “moot” after production of the requested records, a court can still award attorneys’ fees to the prevailing party. A petitioning requester prevails in the litigation (and is entitled to recover fees) if the suit was the catalyst for disclosure of even a single record for which access was improperly denied.⁴¹ Even settlement can expose an agency to a fee motion if the fees are not addressed in the settlement agreement.⁴² This places a significant burden on agencies because it creates financial exposure even when access to the records is given. Agencies may find themselves paying attorneys’ fees despite having ultimately produced the records, which means that even technical delays, incomplete searches, or inadvertent denials can lead to costly consequences. The unpredictability of fee awards makes it challenging to budget or plan, thereby increasing overall risk and underscoring the importance of strict compliance at every stage of the CPRA process.

Technological Advances

Technology has increased the heavy burden of disclosure.⁴³ Agencies may be required to search for and collect records from a wide array of virtual spaces, including the personal devices and accounts of staff and public officials.

This requirement creates a substantial burden because agencies must not only rely on staff and elected officials to search their personal devices and accounts to identify potentially responsive records, but agencies must also ensure that staff and elected officials consistently follow records retention policies. When employees use personal devices, emails, or messaging apps for agency-related communications, it complicates compliance, increases privacy concerns, and raises the risk of incomplete searches. Agencies then face the dual challenge of safeguarding individual privacy while still ensuring full disclosure, all while monitoring and enforcing records retention policies that govern public records on personal accounts and devices. This oversight role requires ongoing training, clear policies, and, in some cases, disciplinary measures, adding yet another layer of administrative and legal burden to CPRA compliance.

These burdens are further compounded by the fact that, with the advent of new technologies, courts are less inclined to be sympathetic to the argument that a request is overly broad or voluminous. As technology has evolved, advanced search capabilities, metadata filtering, email threading, deduplication, and automated redaction are standard tools available to most agencies. Courts are increasingly unwilling to accept volume alone as a reason for delay or denial,⁴⁴ which means that even the challenges of searching across personal and official platforms cannot be used as an excuse to narrow or slow a response.

⁴¹ *Sukumar v. City of San Diego* (2017) 14 Cal.App.5th 451,462

⁴² *Galbisio v. Orosi Pub. Util. Dist.* (2008) 167 Cal.App.4th 1063,1089

⁴³ *City of San Jose v. Superior Court (Smith)* (2017) 2 Cal.5th 608, 618

⁴⁴ *Getz v. Superior Court* (2021) 72 Cal.App.5th 637,650

Managing Difficult Requesters

As discussed, public agencies are legally obligated to respond to requests made under the CPRA. While most requesters engage in good faith, agencies must also be prepared to handle difficult requesters. Some requesters may challenge staff's patience, strain agency resources, or attempt to use the law as a tool for intimidation. Understanding the types of difficult requesters, recognizing red flags, and applying professional management strategies are essential to maintaining compliance and protecting the integrity of the agency's operations.

Who Are Difficult Requesters?

Difficult requesters take several forms. Below are some common examples:

Frequent filers are requesters who submit repeated requests that often overlap or duplicate prior submissions, creating unnecessary workload.

Potential litigants are requesters that deliberately file requests with the aim of discovering technical violations that can form the basis of a lawsuit.

Intimidators are requesters who use the CPRA not as a transparency tool, but as a weapon to intimidate or punish agencies through burdensome requests.

Aggressive or hostile requesters are those who exhibit mean-spirited behavior in emails, public forums, or at government buildings or in public meetings.

Regardless of the type, agencies must remain mindful that each request, even if burdensome, is a legal obligation under the CPRA.

How to Manage Difficult Requesters?

The most effective strategy is to maintain professionalism and adhere to the law. Responses should be respectful, factual, and free from emotion, even in the face of hostility. When requests are vague, overly broad, or duplicative, agencies should seek clarification or formally note their intent to request clarification to narrow the scope of the request. This both preserves statutory compliance and protects the agency from accusations later.

Agencies should also communicate clearly with the requester, outlining the process, identifying who will follow up with the requester, and setting expectations. This reduces the likelihood of misunderstandings and ensures transparency in handling the request. Equally important is maintaining complete documentation of all correspondence and decisions made during the response process. Such documentation not only ensures continuity but also provides legal protection in the event that disputes escalate.

Finally, staff should coordinate internally to gather and produce responsive records as soon as possible. Meeting statutory deadlines is critical to avoiding legal exposure, and early coordination reduces the risk of last-minute delays.

How to Recognize Red Flags?

It would be beneficial for public agency staff to identify “red flags” or warning signs early on in the CPRA process. Red flags often signal a potentially problematic requester or a request that may pose an elevated risk of litigation.

Common “red flags” include:

- Requests marked “urgent” with demands for immediate action.
- Repetitive or boilerplate language, which may suggest mass filings.
- A legalistic tone, particularly when accompanied by citations to the CPRA or threats of legal action.
- Vague or overly broad requests, which may be strategically crafted to overwhelm staff or increase the likelihood of non-compliance.
- Requests from attorneys, law offices, or media organizations, which may warrant heightened attention due to the public or legal implications.
- Buried requests, in which the actual purpose is hidden within a lengthy or confusing submission, increase the risk that the agency may overlook an element.

Recognizing these patterns allows agencies to allocate resources appropriately, involve legal counsel early if necessary, and manage risks proactively.

Difficult requesters are unavoidable and a common element of CPRA compliance. However, with clear strategies, respectful and factual responses, clarification when needed, consistent documentation, internal coordination, and awareness of red flags, agencies can meet their legal obligations while reducing unnecessary risk. By striking a balance between transparency and professional management, public agencies not only comply with the CPRA but also safeguard public trust and protect themselves from litigation risks.

Strategies for Overall Compliance

Effective compliance requires agencies to adopt proactive strategies that strike a balance between legal rigor and operational efficiency. Agencies should establish clear internal procedures and designate trained personnel as responsible for managing requests, ensuring that statutory deadlines are consistently met. Regular staff training on CPRA requirements is essential to promote consistency, minimize errors, and reduce the risk of unlawful denials or excessive redactions.

Agencies should also leverage modern technology to streamline searches, manage large volumes of records, and facilitate rolling productions where appropriate. Legal counsel should be consulted on complex or sensitive requests to ensure that exemptions are properly asserted and defensible. Finally, agencies must reinforce the principle that records related to public business, even those on personal devices,⁴⁵ may fall within the scope of disclosure, including adopting

⁴⁵ See generally *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608

policies that govern how such records are to be stored. Together, these strategies help agencies strengthen compliance, mitigate litigation risks, and maintain public trust.

Conclusion

The CPRA is both a statutory and constitutional mandate for transparency. Failure to comply with its provisions can expose agencies to costly litigation, attorneys' fees, and possibly cause reputational harm. By understanding the CPRA's framework, anticipating compliance challenges, and implementing strategic practices, agencies can navigate complex requests, mitigate risk, and maintain public confidence in their operations.