

Public Records Requests

Cochise County

Responsibilities

The Cochise County Attorney's Office (CCAO) handles all Public Records Requests (PRRs) for the county except two offices, which manage their own systems and ensure their own prompt responses:

1. Sheriff's Office
2. Clerk of the Superior Court

The CCAO has no access to or visibility into those offices' records. Contact Carol Capas (Public Information Officer) for all Sheriff's Office PRRs.

Promptness

Arizona law requires PRRs to be handled "promptly" (A.R.S. § 39-121.01(E)), but does not define the term. Promptness is determined case-by-case and depends on:

1. Number and complexity of requests already pending;
2. Volume and complexity of the current request;
3. Difficulty in locating or retrieving the records;
4. Number of departments or personnel needed to assist; and
5. Overall workload of the involved staff and departments.

No single entity (including the CCAO) is required to oversee promptness for the entire county. Cochise County's division of responsibilities among the CCAO, Sheriff's Office, and Clerk of the Superior Court actually improves response times overall. Turnaround therefore varies by request.

Typical CCAO Turnaround

Within the CCAO, typical processing is 14–45 days. Simpler requests with low backlog are often faster; high-volume or complex requests may take longer.

No Priority for Media or Others The Public Records Law does not give media requests priority over requests from the general public. All requests are handled equitably and as promptly as possible, without regard to the requester's identity or status.

Process for Handling Requests

1. Requestor submits via NextRequest (preferred) or email (CCAO creates a NextRequest entry for emails).
2. Paralegal logs and begins processing.
3. Paralegal consults CAO Attorney if questions arise.
4. Request routed to appropriate department(s).
5. Department retrieves records promptly.
6. Paralegal reviews for required redactions and applies them.
7. CAO Attorney reviews redacted records and approves or directs changes.
8. Records delivered and request closed.

Information That MUST Be Redacted (Statutory/Mandatory Protections)

The following must be redacted before release:

Personal Identifiers & Sensitive Data

- Social Security numbers, driver's license/State ID/passport numbers
- Financial account numbers, taxpayer ID numbers, PINs, passwords, access codes

Protected Contact Information (Statutorily Protected)

- Residential addresses and phone numbers of peace officers, judges, prosecutors, and certain protected officials
- Victim contact information protected by statute

Victim & Minor Information

- Identifying information of crime victims (where protected)
- Names/identifying information of minors in protected contexts
- Child welfare/DCS records and juvenile court records

Medical & Health Information

- Protected health information (HIPAA)
- Medical and psychological records
- Autopsy photographs/digital images (A.R.S. § 11-597.02)

Personnel Records (Protected Portions)

- Confidential employee medical information
- I-9 forms and supporting documents
- Protected background check information
- Disciplinary records protected by statute

Law Enforcement Sensitive

- Criminal history record information (CHRI) from DPS/NCIC
- Information revealing confidential informants, undercover operations, tactical plans, or security vulnerabilities

Privileged Material

- Attorney-client communications and work product
- Records protected by court order

Proprietary Information

- Trade secrets (A.R.S. § 44-401 et seq.) and other statutorily protected business information

Information That MAY Be Redacted (Case-by-Case – Carlson Balancing Test)

Under *Carlson v. Pima County*, 141 Ariz. 487 (1984), even non-statutorily exempt records may be withheld or redacted if the County demonstrates that confidentiality, privacy, or the best interests of the state outweigh the policy favoring disclosure. This requires a case-specific analysis and articulation of specific, non-speculative harm.

Common Categories Evaluated Under Carlson

- Personal addresses, email addresses, and phone numbers
- Personal privacy in personnel files (e.g., non-protected employees' home addresses/phone numbers, family information)
- Ongoing internal investigative materials
- Security-sensitive infrastructure (building schematics, IT vulnerabilities)
- Graphic images with significant privacy interests
- Internal complaint records and safety concerns for employees or the public

Key Considerations

- Is there a specific, articulable harm from disclosure?
- Can redaction (instead of full withholding) protect the interest?
- Is the matter ongoing or completed?
- Does heightened public interest apply (e.g., allegations of misconduct, use of public funds, public safety)?

CATEGORIES FOR PUBLISH/DO NOT PUBLISH PUBLIC RECORDS REQUEST

CATEGORY	DESCRIPTION	PUBLISH	DO NOT PUBLISH
Personnel Records	Employee names, job titles, salaries, disciplinary actions (limited by privacy laws; redactions applied). Generally sent as excel spreadsheets minus disciplinary actions.	X	
Contracts & Procurement (post-award)	Vendor contracts, bids, RFPs/RFQs, purchase orders, payments to contractors.	X	
Financial Records & Budgets	Annual budgets, accounting reports, audits, expense reports.	X	
Emails / Communications	Emails of public officials, text messages, internal memos related to a topic. (CAO, and County Administration may request some be published due to multiple similar requests)		X

Meeting Records	Meeting agendas, minutes, attendance records, recordings.	X	
Policies, Procedures, & Manuals	Standard operating procedures, administrative rules, handbook policies	X	
Incident/Police Reports	Police reports, arrest records, call logs, dash/body cam footage (with privacy exceptions).	X	
Public Safety/Inspection Records / Reports	Fire inspection reports, building inspection results, code enforcement documents.		X
Permits, Licenses, surveys, applications	Business licenses, zoning permits, construction permits, food safety licenses.	X	
Litigation / Claims Records	Legal settlements, claims filed, court filings, correspondence regarding lawsuits.	X	
Voter Data Requests	Voter registration data (public portions), election results, precinct turnout, ballot request logs, poll worker records, vote-by-mail totals (never includes actual votes tied to individuals – only aggregated data)	CASE BY	CASE
Other sensitive materials	<ul style="list-style-type: none"> • Floorplans on doors with access control installed. • IT Contingency Plan & results • Business Impact Analysis (BIA) report • Disaster Recovery Plan (DRP) & results • Business Continuity of Operations Plan (BCP) • Employee Disciplinary actions • Job Applications 		X