

JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
www.courts.ca.gov/policyadmin-invitationstocomment.htm

INVITATION TO COMMENT

SP20-09

Title

Judicial Branch Administration: Judicial Branch Data and Information Governance Policy Concepts

Proposed Rules, Forms, Standards, or Statutes

N/A

Proposed by

Information Technology Advisory Committee
Hon. Sheila F. Hanson, Chair

Action Requested

Review and submit comments by February 11, 2021

Proposed Effective Date

N/A

Contact

Leah Rose-Goodwin, Lead Staff
Data Analytics Workstream, Information Technology Advisory Committee
itac@jud.ca.gov

Executive Summary and Origin

In 2018, the Judicial Council of California’s Information Technology Advisory Committee began work to develop and recommend for the judicial branch a data analytics strategy that included branchwide data and information governance policy. The preliminary result of that work is the attached report, *Proposed Judicial Branch Data and Information Governance Policy Concepts*. The Information Technology Advisory Committee is seeking public input at this early stage in the policymaking process to encourage public dialogue about these concepts and to incorporate feedback before the committee submits its report on the policy concepts to the Judicial Council.

Background

Over the past several years, the California judicial branch has initiated several statewide initiatives focused on using technology to help increase access to justice. At its meeting on November 30, 2018, the Judicial Council approved the *Strategic Plan for Technology 2019–2022*, which outlines the goal to Promote the Digital Court.¹ One of the main objectives of this goal is to “[i]ncrease court-to-court data sharing for data-driven decisionmaking.” Also, in 2018,

¹ Judicial Council of Cal., Technology Com. Rep., *Judicial Branch Administration: Strategic Plan for Technology 2019–2022* (Nov. 9, 2018), pp. 5, 8–9, <https://jcc.legistar.com/View.ashx?M=F&ID=6786818&GUID=8F2A8400-854F-4724-A32B-9C46FDEBF002>.

*This proposal has not been approved by the Judicial Council and is not intended to represent the views of the council, its Rules Committee, or its Legislation Committee.
It is circulated for comment purposes only.*

the Information Technology Advisory Committee (ITAC) formed a Data Analytics Workstream with coexecutive sponsors Presiding Judge Tara M. Desautels and Court Executive Officer David H. Yamasaki, as well as participants from across the judicial branch. The workstream's mission was to recommend for the branch a data analytics strategy that included developing branchwide data and information governance policy recommendations. The proposed data and information governance policy concepts represent the draft recommendations from ITAC, which will be submitted to the Judicial Council for consideration of future policy development.

The Proposal

The report on policy concepts contains recommendations for policy development in key areas of data and information governance: classification, access, use, sharing, maintenance, and disposal/retention. The report defines key concepts in each of these areas and, in some cases, provides examples to explain how the concepts apply to the judicial branch. The proposed concepts are organized around the data and information life cycle, a general organizing framework for data and information. They are intended to align with the draft vision and guiding principles, which are included in the report as reference. Also included in the proposal are definitions for key roles and responsibilities for data and information management.

ITAC will consider public comment on the proposed policy concepts, discuss and make any needed revisions to the report, and submit the report to the Judicial Council. The council will then decide if these policy concepts should be used by an appropriate advisory committee to develop data and information governance policies.

Alternatives Considered

ITAC considered various aspects of a branch strategy for data analytics and solicited input from numerous judicial branch entities to guide its work. From those discussions, data and information governance emerged as the most important area for policy development. In turn, the proposed policy concepts were identified as the most essential and fundamental components of judicial branch data and information governance.

Fiscal and Operational Impacts

The report on policy concepts is intended to guide future policy development. Therefore, there is no fiscal or operational impact at this stage.

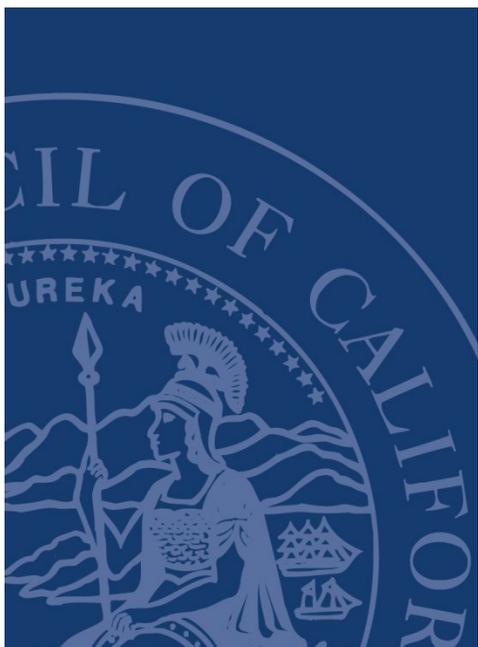
Request for Specific Comments

In addition to comments on the proposed policy concepts as a whole, ITAC is interested in comments on the following:

- Does the proposal appropriately address the stated purpose?
- Are there any additional topics that the proposed policy concepts should address to guide development of judicial branch data and information governance policies?

Attachments and Links

1. *Proposed Judicial Branch Data and Information Governance Policy Concepts*, at pages 4–13



Report on Proposed Judicial Branch Data and Information Governance

FOR 30-DAY PUBLIC COMMENT
DEC. 30, 2020, TO FEB. 11, 2021

DATA ANALYTICS WORKSTREAM



JUDICIAL COUNCIL
OF CALIFORNIA

OPERATIONS AND PROGRAMS DIVISION
INFORMATION TECHNOLOGY

Table of Contents

BACKGROUND	3
TERMINOLOGY	3
VISION AND GUIDING PRINCIPLES	4
THE INFORMATION LIFE CYCLE.....	4
PROPOSED POLICY CONCEPTS OF THE DATA AND INFORMATION LIFE CYCLE	5
Data and Information Classification Policy Concepts	5
Data and Information Access Policy Concepts	6
Data and Information Use Policy Concepts	7
Data and Information Sharing Policy Concepts	7
Data and Information Maintenance Policy Concepts	9
Data and Information Disposal/Retention Policy Concepts	10
FUTURE POLICY DEVELOPMENT.....	10
CONCLUSION	10

Background

Over the past several years, the California judicial branch has initiated several statewide initiatives focused on using technology to help increase access to justice.

At its meeting on November 30, 2018, the Judicial Council approved the *Strategic Plan for Technology 2019–2022*, which outlines the goal to Promote the Digital Court.¹ One of the main objectives of this goal is to “[i]ncrease court-to-court data sharing for data-driven decisionmaking.” Also in 2018, the Data Analytics Workstream was formed with the mission to recommend for the branch a data analytics strategy that would include governance recommendations appropriate for all courts and the Judicial Council.

The data and information governance policy concepts proposed in this document represent an evolution in thinking about judicial branch data. This work embodies numerous conversations within California’s judicial branch and considers similar efforts of federal and other state courts. It reflects a change in public expectations around the use and availability of data and recognizes the judicial branch’s responsibility as a steward of data and information.

Terminology

The following terms are used throughout this document:

data—Facts and statistics assembled for reference or analysis.

information—Data that has been validated, organized, and contextualized. It is the basis for analysis and decisionmaking. The governance policy concepts apply to both data and information.

judicial branch entity (or JBE)—The Supreme Court, each Court of Appeal, each superior court, or the Judicial Council—collectively referred to in these policies as the judicial branch.

data steward—A JBE role that determines data access and sets requirements for data quality, accuracy, and completeness. The data steward also validates data, establishes procedures and guidelines for data integrity, and addresses data sharing requests. A JBE can identify one or more data stewards from within the JBE as needed based on local resources and requirements.

data administrator—A JBE role responsible for maintaining and storing the data. It is a business role, associated with each data source, that ensures the confidentiality, integrity, and availability of data. It also implements related policies, standards, procedures, and guidelines. A

¹ Judicial Council of Cal., Technology Com. Rep., *Judicial Branch Administration: Strategic Plan for Technology 2019–2022* (Nov. 9, 2018), pp. 5, 8–9, <https://jcc.legistar.com/View.ashx?M=F&ID=6786818&GUID=8F2A8400-854F-4724-A32B-9C46FDEBF002>

JBE can identify one or more data administrators from within the JBE as needed based on local requirements.

Vision and Guiding Principles

The judicial branch will analyze, use, and share data to inform decisionmaking in order to enhance and expand vital and accessible services for all the people of California.

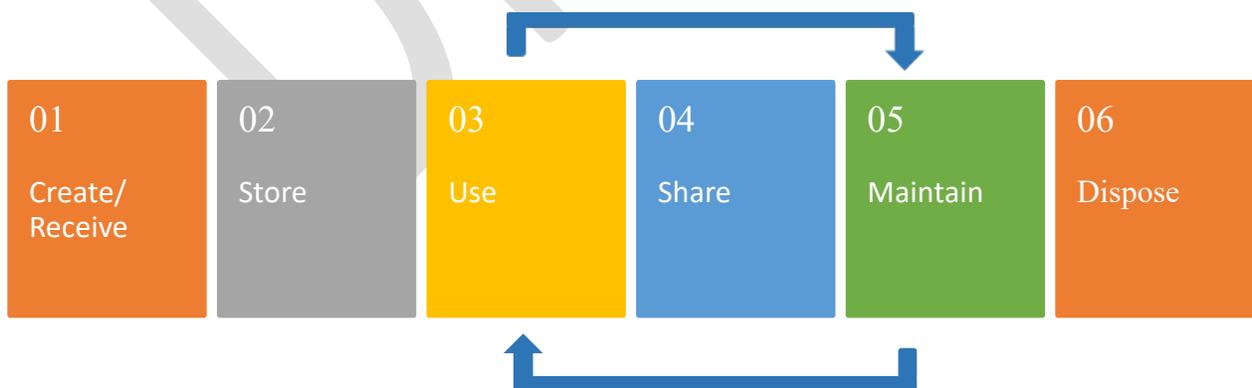
This work represents an evolution in the way the judicial branch uses and thinks about data. In support of that new mindset, the judicial branch will:

- Collect, use, and share data and information as appropriate to promote and support informed decisionmaking;
- Be clear about the use and purpose of data and information;
- Promote data transparency;
- Use high-quality, validated data and information;
- Follow published standards and governance principles when sharing data;
- Secure all data and information; and
- Manage data and information according to retention requirements.

The Information Life Cycle

Data and information are managed through a series of stages called the *information life cycle* (see graphic 1).

Graphic 1. The Data and Information Life Cycle



1. **Create/Receive**—Data is first created or received.
2. **Store**—It is then stored locally or on the internet.

3. **Use**—The data is then used in calculations or analysis, or combined with other data.
4. **Share**—It may then be provided to others internal or external to an organization.
5. **Maintain**—Data may be updated when new information is received or corrections are needed.
6. **Dispose**—When data reaches the end of its usefulness or retention period, it may be destroyed. If data must be preserved permanently, it is archived.

Data and information may cycle through steps 3–5 several times while they are used, shared, and refined before they are disposed of or archived.

Proposed Policy Concepts of the Data and Information Life Cycle

The judicial branch’s proposed data and information policy concepts are organized around the framework of the data and information life cycle. Each individual concept addresses one or more of the stages of the life cycle.

Data and Information Classification Policy Concepts



Data and information will be collected, used, and shared to promote and support informed decisionmaking. Classifications will be used to identify the source, use, and purpose of judicial branch data and information, helping to quickly and uniformly identify appropriate access and security levels.

- a. **Judicial Branch Data and Information Classifications.** Data and information should be classified as “public,” “nonpublic,” or “restricted,” based on the nature of the data or information.

Public: Most documents filed in court cases and most judicial administrative records, including data drawn from public case records, are subject to public access and, therefore, are classified as “public.”²

Nonpublic: Some case records are confidential by law or sealed by judicial order and, therefore, are classified as nonpublic (or not subject to public access).³ Information drawn from such case records would also be nonpublic—for example, parties’ personal identifying information. Similarly, some judicial administrative records may be exempt from public access and classified as nonpublic, although shareable between judicial

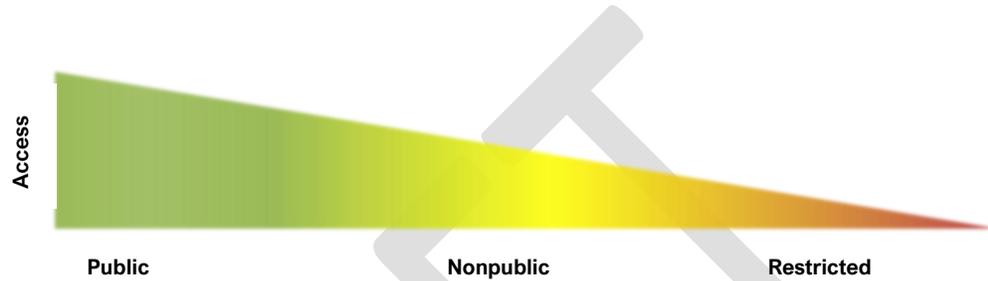
² See, e.g., Cal. Rules of Court, rule 10.500(a), (e)(1); *Estate of Hearst* (1977) 67 Cal.App.3d 777, 782–783.

³ See, e.g., Welf. & Inst. Code, § 827 [juvenile court records].

branch entities for purposes of judicial branch administration.⁴

Restricted: Some branch records require a higher level of restriction—for example, to protect privacy or security interests—dictating access limits within the judicial branch entity itself.

Graphic 2. Classifications of Branch Data



- b. **Confidentiality.** Categories of court case records that are confidential by law or may be subject to judicial sealing orders are identified in statute, the California Rules of Court, and the *Trial Court Records Manual*.
- c. **Individual Privacy Rights.** In using and sharing data and information, JBEs will strive to protect the individual privacy rights of court users. When possible, only aggregate de-identified data and information (i.e., containing no information that would identify an individual litigant, witness, or other interested party) will be shared or disclosed to non-JBEs, unless greater detail is required by law. Private personal information about people who work at the court will also be protected.

Example: The number of visitors to a JBE’s self-help center or website and the nature of the questions received would be classified as public, while visitor names and other identifying data would be nonpublic and nondisclosable.

Data and Information Access Policy Concepts



Data access policies support and promote data transparency while also safeguarding nonpublic data and information.

⁴ See Cal. Rules of Court, rule 10.500(f), (h)(2)(C).

- a. **Permissions-Based Access.** Individuals are granted access to data and information at the level appropriate for the authorized function. Unauthorized access is prevented.

Example 1: An attorney could view electronic copies of official records filed in cases in which the attorney’s clients are parties but would not have unrestricted access to all electronic case records filed with a court.⁵

Example 2: A court clerk may view public and nonpublic (or confidential) case records using the court’s case management system but may not view the personnel records of other court employees.

Data and Information Use Policy Concepts



The use and purpose of branch data should be clear, as should the responsibilities inherent in using data.

- a. **Data Possession Versus Data Viewing.** *Possessing* data (or a copy of data) confers responsibility and authority to make disclosure determinations on a request from the public. *Viewing* data does not. A judicial branch entity has authority and responsibility to make disclosure decisions about data and information in its possession on request from a member of the public—both data it has collected and copies of data provided by others. A person or entity viewing data or information does not have the same responsibilities as one who receives a physical or electronic copy of data or information. The fact that JBEs share nonpublic data with each other does not convert the nonpublic data to public data.⁶

Data and Information Sharing Policy Concepts



Better data sharing can help promote and support informed decisionmaking. Published standards and principles will facilitate sharing.

- a. **Data and Information Exempt From Public Disclosure.** Preliminary, incomplete, unvalidated, untested data and information or draft analysis and reports collected or prepared solely to inform internal decisionmaking on a specific point and which would not ordinarily be retained may be exempt from public disclosure in some circumstances if

⁵ *Id.*, rules 2.518, 2.519.

⁶ *Id.*, rule 10.500(f)(6), (h)(2)(C).

the balance of the public interest clearly favors nondisclosure.

Example: A court administrator informally collects preliminary data to quickly evaluate the impact of potential changes to the court's allocated state funding. The court administrator does not test the data or rely on it to make any decision. The data is exempt from public disclosure because it is preliminary and predecisional, and disclosure could lead to public misunderstanding regarding the court's actual budget and available resources.

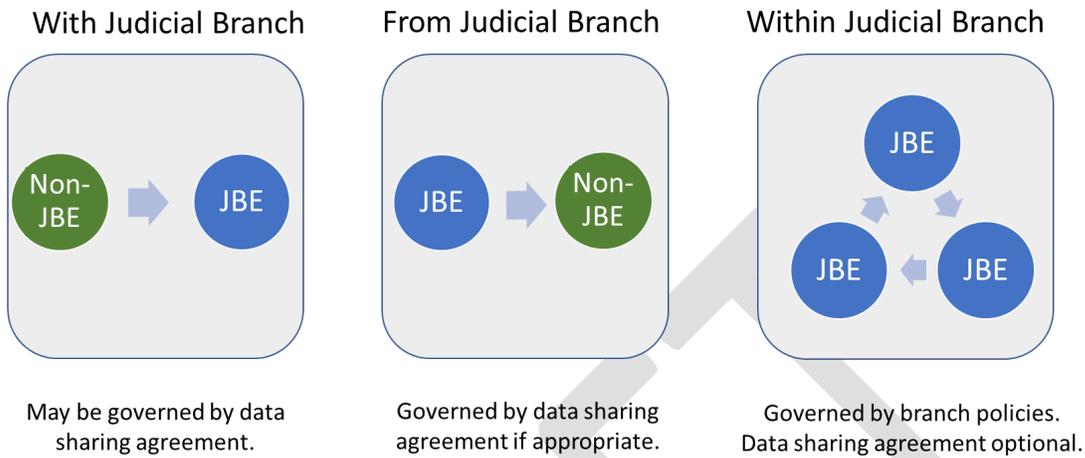
- b. **Data for Purposes of Judicial Branch Administration.** JBEs may share otherwise exempt or nonpublic data and information with each other to advance branch goals while still treating the data and information as exempt from public disclosure.⁷

Example: The court administrator in the previous example may decide to share the preliminary analyses with another court administrator in the spirit of collaboration. By sharing the exempt data within the judicial branch, the court administrator does not lose the right to treat the data as exempt from public disclosure.

- c. **Data and Information Sharing.** Standards and principles for data sharing differ based on the relationship between the sharing entities.
 - i. **Sharing judicial branch data with non-judicial branch entities.** A data sharing agreement may be appropriate.
 - ii. **Sharing non-judicial branch data with JBEs.** Such sharing may be governed by a non-JBE data sharing agreement. If one JBE receives data or information from an external source under an agreement limiting use of the data, that JBE may only share the data or information with another JBE under conditions stated in the agreement, and the use restrictions must be observed by the second JBE.
 - iii. **JBE sharing within the branch.** Data sharing among JBEs should adhere to published judicial branch policies and local policies. Typically, a data sharing agreement is optional between JBEs. However, if certain handling of the data is required, a data sharing agreement may be helpful.

⁷ See Cal. Rules of Court, rule 10.500(h)(2)(C) [waiver]; *id.*, rule 10.500(f) [exemptions].

Graphic 3. Differing Data Sharing Policies Based on the Sharing Relationship



d. Obligation to Disclose Data or Information, Consultation With Data Steward.

Existing law states that each JBE has an independent obligation to publicly disclose nonexempt data or information in its possession on request. If a JBE receives a public request for data or information that it obtained from another JBE and has not previously published or publicly disclosed the data (for example, in a report to the Legislature), the JBE that received the data or information request must (1) notify the JBE that originally provided the data of the request, (2) consider the provider’s position about disclosure, and (3) consider any corrections or updates to the data that the provider may wish to submit to accompany any disclosure of the original data.

Data and Information Maintenance Policy Concepts



High-quality, validated data and information are crucial for informed decisionmaking. Data should be secured and managed appropriately. Responsibility for maintenance of the data resides with the data administrator.

a. Data Integrity

- i. Mandatory measurement of data and information quality.** Data and information quality has many dimensions, including, for example, accuracy, reliability, and timeliness. Not all aspects of data quality will be equally relevant to all types of data. Assessing the different aspects of data quality applies to all phases of the data

life cycle and gives greater confidence in the information being used for decisionmaking.

- ii. **Standards and measurement of data quality.** Establishing data quality standards, putting mechanisms in place to measure the data against those standards, and continually monitoring performance measures and determining course corrections as needed are all part of improving data quality.
- iii. **Best practices.** Sharing best practices and techniques will facilitate data improvement.

b. **Data Availability**

- ii. **Data protection.** Data and information assets (whether in electronic or physical form) should be protected by appropriate electronic safeguards.
- iii. **Appropriate protection.** The level of security and safeguarding of data and information should be commensurate with the level of sensitivity of the content.
- iv. **Backups and disaster recovery.** Appropriate backups and disaster recovery measures should be administered and deployed for all data and information.

Data and Information Disposal/Retention Policy Concepts



- a. **Archive and Retention.** Data should be archived or disposed of according to established retention schedules.

Future Policy Development

The workstream recognizes the need for future policy development in the following areas:

- Data and information management policies
- Data and information preservation
- *Trial Court Records Manual* and California Rules of Court updates

Conclusion

The judicial branch data and information policy concepts are the foundation for the judicial branch data governance model. The policies will evolve over time and incorporate new concepts and changes as needed to accommodate and reflect any changes in the law or in branch priorities and requirements.