Judicial Council of California

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

INVITATION TO COMMENT

[ItC prefix as assigned]-__

Title
Technology: Rules Modernization Project

Proposed Rules, Forms, Standards, or Statutes
Amend Cal. Rules of Court, rules 2.250, 2.251, 2.255, and 2.257

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

Action Requested
Review and submit comments by June 8, 2018

Proposed Effective Date
January 1, 2019

Contact
Andrea Jaramillo, 916-263-0991
andrea.jaramillo@jud.ca.gov

Executive Summary and Origin

As part of the Rules Modernization Project, the Information Technology Advisory Committee recommends amending several rules related to electronic service and electronic filing. The purpose of the proposal is to conform the rules to the Code of Civil Procedure, clarify and remove redundancies in rule definitions, and ensure indigent filers are not required to have a payment mechanism to create an account with electronic filing service providers (EFSPs). The proposal includes amendments required by statute and suggested by the public.

Background

New provisions of Code of Civil Procedure section 1010.6 (section 1010.6) require express consent for electronic service, which will require rule amendments and adoption of a form for withdrawal of consent. In addition, new provisions of section 1010.6 require the Judicial Council to adopt rules of court related to disability access and electronic signatures for documents signed under penalty of perjury. Finally, the proposal includes amendments based on comments received from the public. These include amendments to the definitions and contract requirements between EFSPs and courts.

The Proposal

The proposal would make the following amendments:

- ***"Document."*** Amend the definition of "document" in rule 2.250(b). The current wording can be read to mean that a document must be a filing. The proposed amendment removes this

ambiguity by striking "filing" and replacing it with "writing" to clarify that a "document" is not necessarily a filing. The amendment was suggested by members of the public.

- ***"Electronic service," "electronic transmission," and "electronic notification."*** Amend the definitions of "electronic service," "electronic transmission," and "electronic notification" in rule 2.250(b) to refer to the definitions in section 1010.6 rather than duplicate them. This is to avoid risk of the rules and Code of Civil Procedure differing in their definitions should the Legislature amend section 1010.6.

- ***"Electronic filing manager."*** Add a definition for "electronic filing manager." The proposal includes amendments to rule 2.255 to include electronic filing managers. Accordingly, a definition was also added and is based on descriptions of electronic filing managers the Judicial Council used in a request for proposals in 2017.

- ***"Self-represented."*** Add a definition for "self-represented" to rule 2.250(b) and exclude attorneys from the definition. Rules applicable to self-represented persons were intended to add protections for those without an attorney. For example, self-represented persons are exempt from mandatory electronic filing. Attorneys acting for themselves are not acting without an attorney. Accordingly, attorneys are excluded from the definition of "self-represented" under the electronic filing and service rules. Because section 1010.6 uses the term "unrepresented" and the rules of court use the term "self-represented," the definition in the rules refers to self-represented parties or other persons as being those unrepresented by an attorney. This proposal was a suggestion from a member of the public.

- ***Express consent.*** Amend rule 2.251(b) to require express consent for permissive electronic service and add a provision for how a party or other person may manifest consent as required by statute. The current rules allow the act of electronic filing to serve as consent to electronic service. Effective January 1, 2019, section 1010.6 will no longer allow the act of electronic filing alone to serve as consent. (§ 1010.6(a)(2)(A)(ii).) Under section 1010.6, parties may still consent through electronic means by "manifesting affirmative consent through electronic means with the court or the court's electronic filing service provider, and concurrently providing the party's electronic service address with that consent for the purpose of receiving electronic service." The proposal amends the rules to remove the provision allowing the act of filing to serve as consent to electronic service and replaces it with the language for manifesting affirmative consent by electronic means from section 1010.6. The proposal also adds a provision for how a party or other person may "manifest affirmative consent."

- ***Electronic filing managers.*** Amend rule 2.255 to add electronic filing managers within the scope of the rule. Section 1010.6(g)(2) requires that "[a]ny system for the electronic filing and service of documents, including any information technology applications, Internet Web sites, and Web-based applications, used by an electronic service provider or any other vendor or contractor that provides an electronic filing and service system to a trial court" be accessible by persons with disabilities and comply with certain access standards. Vendors

and contractors must comply as soon as practicable, but no later than June 30, 2019. (§ 1010.6(g)(3).) Likewise, the statute requires the Judicial Council to adopt rules to implement the requirements as soon as practicable, but no later than June 30, 2019. (§ 1010.6(g)(1).) Section 1010.6 includes specific requirements that courts and contractors must meet. Rule 2.255 already requires courts contracting with EFSPs to comply with section 1010.6. However, because the rules of court do not account for contracts with electronic filing managers, the proposal amends rule 2.255 to include them.

- ***Payment information.*** Amend rule 2.255 to add subdivision (f) requiring require EFSPs to allow filers to create an account without having to provide a credit card, debit card, or bank account information. The amendment is based on a suggestion from the State Bar's Standing Committee on the Delivery of Legal Services. According to the standing committee, some EFSPs require such payment information even if the filer is never charged. According to the standing committee, this "creates an insurmountable barrier to those without access to credit or banking services." Subdivision (f) provides that it only applies to the creation of an account, but not to the provision of services unless the filer has a fee waiver.

- ***Electronic signatures.*** Amend rule 2.257 to create a procedure for electronically filed documents signed under penalty of perjury. Section 1010.6(b)(2)(B)(ii) provides that when a document to be filed requires a signature made under penalty of perjury, the document is considered signed by the person if, in relevant part, "[t]he person has signed the document using a computer or other technology pursuant to the procedure set forth in a rule of court adopted by the Judicial Council by January 1, 2019." Accordingly, the proposal creates a procedure where the document is deemed signed when the "declarant has signed the document using an electronic signature, and declares under penalty of perjury under the laws of the state of California that the information submitted is true and correct." The language is modeled after the requirements in the Uniform Electronic Transactions Act (UETA) for electronic signatures made under penalty of perjury. (Civ. Code, § 1633.11(b).) In addition, a definition of "electronic signature" is added to the rule, modeled after the definitions used in UETA and the Code of Civil Procedure.

Alternatives Considered

The committee considered retaining the definitions of "electronic service," "electronic transmission," and "electronic notification" in rule 2.250(b) rather than referencing section 1010.6 for the definitions. Referencing the Code of Civil Procedure will create an extra step in looking up the definitions. However, the committee opted for the proposed language to remove the risk of having differing definitions should the Legislature amend section 1010.6.

The committee considered making a technical amendment to the consent requirements in rule 2.251(b) to ensure the rules comply with section 1010.6's express consent requirements without interpreting the statute. However, the committee received public comments from the EFSP community raising concerns over uncertainty in the meaning of "manifesting affirmative

consent" in section 1010.6's express consent requirements. The public comment included a proposed interpretation, which was integrated into the proposal.

Implementation Requirements, Costs, and Operational Impacts

It is expected that the new express consent requirements will result in one-time costs to EFSPs and courts to create a mechanism to capture affirmative consent by electronic means to electronic service. It is unknown whether or how these costs will impact the fees EFSPs charge filers for their services.

Request for Specific Comments

In addition to comments on the proposal as a whole, the advisory committee is interested in comments on the following:

- Does the proposal appropriately address the stated purpose?
- The amendments to rule 2.251(b) bring the rule into compliance with section 1010.6's express consent requirements. In addition, the rule adds a provision for how a party or other person may "manifest affirmative consent."
  - Is the provision for manifesting affirmative consent clear and does it adequately capture how a party or other person may manifest affirmative consent?
  - Rule 2.251(b) does not detail (1) how notice is to be given to the court that a party or other person has provided express consent, or (2) how notice of the same is to be given to other parties or persons in the case. The committee seeks specific comments on how such notification should be addressed in the rules.

Attachments and Links

1. Cal. Rules of Court, rules 2.250, 2.251, 2.255, and 2.257, pages 5–10
2. Code of Civil Procedure section 1010.6, *http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1010.6&lawCode=CCP*

Rules 2.250, 2.251, 2.255, and 2.257 of the California Rules of Court would be amended, effective January 1, 2019, to read:

Rule 2.250. Construction and definitions

(a) * * *

(b) Definitions

As used in this chapter, unless the context otherwise requires:

(1) A "document" is a pleading, ~~a paper,~~ a declaration, an exhibit, or another writing submitted by a party or other person, or by an agent of a party or other person on the party's or other person's behalf. A document is also a notice, order, judgment, or other issuance by the court. A document may be in paper or electronic form.

(2) "Electronic service" has the same meaning as defined in Code of Civil Procedure section 1010.6 ~~is service of a document on a party or other person by either electronic transmission or electronic notification. Electronic service may be performed directly by a party or other person, by an agent of a party or other person, including the party's or other person's attorney, through an electronic filing service provider, or by a court~~.

(3) "Electronic transmission" has the same meaning as defined in Code of Civil Procedure section 1010.6 ~~means the transmission of a document by electronic means to the electronic service address at or through which a party or other person has authorized electronic service~~.

(4) "Electronic notification" has the same meaning as defined in Code of Civil Procedure section 1010.6 ~~means the notification of a party or other person that a document is served by sending an electronic message to the electronic service address at or through which the party or other person has authorized electronic service, specifying the exact name of the document served and providing a hyperlink at which the served document can be viewed and downloaded~~.

(5)–(8) * * *

(9) An "electronic filing manager" is a service that acts as an intermediary between a court and various electronic filing service provider solutions certified for filing into California courts.

(10) "Self-represented" means a party or other person who is unrepresented in an action by an attorney and does not include an attorney appearing in an action who represents himself or herself.

Rule 2.251. Electronic service

(a) * * *

(b) Electronic service by express consent ~~of the parties~~

(1) ~~Electronic service may be established by consent.~~ A party or other person indicates that the party or other person agrees to accept electronic service by:

(A) Serving a notice on all parties and other persons that the party or other person accepts electronic service and filing the notice with the court. The notice must include the electronic service address at which the party or other person agrees to accept service; or

(B) ~~Electronically filing any document with the court. The act of electronic filing is evidence that the party or other person agrees to accept service at the electronic service address the party or other person has furnished to the court under rule 2.256(a)(4). This subparagraph (B) does not apply to self-represented parties or other self-represented persons; they must affirmatively consent to electronic service under subparagraph (A).~~ Manifesting affirmative consent through electronic means with the court or the court's electronic filing service provider, and concurrently providing the party's electronic service address with that consent for the purpose of receiving electronic service.

(C) A party or other person may manifest affirmative consent under (B) by:

(i) Agreeing to the terms of service agreement with an electronic filing service provider, which clearly states that agreement constitutes consent to receive electronic service electronically; or

(ii) Filing *Consent to Electronic Service and Notice of Electronic Service Address* (form EFS-005-CV).

(2) A party or other person that has consented to electronic service under (1) and has used an electronic filing service provider to serve and file documents in a case consents to service on that electronic filing service provider as the designated agent for service for the party or other person in the case, until such time as the party or other person designates a different agent for service.

(c)–(k) * * *

Rule 2.255. Contracts with electronic filing service providers and electronic filing managers

(a) Right to contract

(1) A court may contract with one or more electronic filing service providers to furnish and maintain an electronic filing system for the court.

(2) If the court contracts with an electronic filing service provider, it may require electronic filers to transmit the documents to the provider.

(3) A court may contract with one or more electronic filing managers to act as an intermediary between the court and electronic filing service providers.

~~(3)~~(4) If the court contracts with an electronic service provider or the court has an in-house system, the provider or system must accept filing from other electronic filing service providers to the extent the provider or system is compatible with them.

(b) Provisions of contract

(1) The court's contract with an electronic filing service provider may:

(A) Allow the provider to charge electronic filers a reasonable fee in addition to the court's filing fee;

(B) Allow the provider to make other reasonable requirements for use of the electronic filing system.

(2) The court's contract with an electronic filing service provider must comply with the requirements of Code of Civil Procedure section 1010.6.

(3) The court's contract with an electronic filing manager must comply with the requirements of Code of Civil Procedure section 1010.6.

(c) Transmission of filing to court

(1) An electronic filing service provider must promptly transmit any electronic filing and any applicable filing fee to the court~~.~~ directly or through the court's electronic filing manager.

(2) An electronic filing manager must promptly transmit an electronic filing and any applicable filing fee to the court.

(d) Confirmation of receipt and filing of document

(1) An electronic filing service provider must promptly send to an electronic filer its confirmation of the receipt of any document that the filer has transmitted to the provider for filing with the court.

(2) The electronic filing service provider must send its confirmation to the filer's electronic service address and must indicate the date and time of receipt, in accordance with rule 2.259(a).

(3) After reviewing the documents, the court must promptly transmit to the electronic filing service provider and the electronic filer the court's confirmation of filing or notice of rejection of filing, in accordance with rule 2.259.

(e) Ownership of information

All contracts between the court and electronic filing service providers or the court and electronic filing managers must acknowledge that the court is the owner of the contents of the filing system and has the exclusive right to control the system's use.

(f) Establishing a filer account with an electronic filing service provider

(1) An electronic filing service provider may not require a filer to provide a credit card, debit card, or bank account information to create an account with the electronic filing service provider.

(2) This provision applies only to the creation of an account and not to the use of an electronic filing service provider's services. An electronic filing services provider may require a filer to provide a credit card, debit card, or bank account information before rendering services unless the services are within the scope of a fee waiver granted by the court to the filer.

Rule 2.257. Requirements for signatures on documents

(a) Electronic signature

An electronic signature is an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign a document or record created, generated, sent, communicated, received, or stored by electronic means.

~~(a)~~(b) Documents signed under penalty of perjury

When a document to be filed electronically provides for a signature under penalty of perjury of any person, the document is deemed to have been signed by that person if filed electronically provided that either of the following conditions is satisfied:

(1) The declarant has signed the document using an electronic signature ~~a computer or other technology, in accordance with procedures, standards, and guidelines established by the Judicial Council~~ and declares under penalty of perjury under the laws of the state of California that the information submitted is true and correct; or

(2) The declarant, before filing, has physically signed a printed form of the document. By electronically filing the document, the electronic filer certifies that the original, signed document is available for inspection and copying at the request of the court or any other party. In the event this second method of submitting documents electronically under penalty of perjury is used, the following conditions apply:

(A) At any time after the electronic version of the document is filed, any party may serve a demand for production of the original signed document. The demand must be served on all other parties but need not be filed with the court.

(B) Within five days of service of the demand under (A), the party or other person on whom the demand is made must make the original signed document available for inspection and copying by all other parties.

(C) At any time after the electronic version of the document is filed, the court may order the filing party or other person to produce the original signed document in court for inspection and copying by the court. The order must specify the date, time, and place for the production and must be served on all parties.

(D) Notwithstanding (A)–(C), local child support agencies may maintain original, signed pleadings by way of an electronic copy in the statewide automated child support system and must maintain them only for the period of time stated in Government Code section 68152(a). If the local child support agency maintains an electronic copy of the original, signed pleading in the statewide automated child support system, it may destroy the paper original.

~~(b)~~(c) * * *

~~(c)~~(d) * * *

~~(d)~~(e) * * *

~~(e)~~(f) * * *

~~**Advisory Committee Comment**~~

~~**Subdivision (a)(1).** The standards and guidelines for electronic signatures that satisfy the requirements for an electronic signature under penalty of perjury are contained in the Trial Court Records Manual.~~

Privacy Resource Guide

For the California
Trial and Appellate Courts
and the Judicial Branch

First Edition
_____, 2018

Privacy Resource Guide

Table of Contents

3. Access to Court Records

4.6.4 Use of vendors to collect fines and fees

4.7 Taxpayer Information

4.7.1 Confidential statements of Taxpayer's Social Security Numbers

4.7.2 Income tax returns in child support cases

5. Privacy in Judicial Administrative Records

5.1 Public access to judicial administrative records (rule 10.500)

5.1.1 Policy

5.1.2 Scope of access

5.1.3 Exemptions and waiver of exemptions

5.2 Criminal History Information

6. Privacy of Witnesses, Jurors, and Other Non-parties

6.1 Witness and Victim Information

6.1.1 Confidential information about witnesses and victims in police, arrest, and investigative reports

6.1.2 Victim impact statements

6.1.3 Identity of sex offense victims

6.2 Juror Information

6.2.1 Juror questionnaires of those jurors not called

6.2.2 Juror questionnaires answered under advisement of confidentiality

6.2.3 Sealed juror records in criminal courts

Appendices

Appendix A: List of statutes and rules on confidentiality and sealed records
Appendix B: Model local court privacy guide
Appendix C: Sample privacy statement for court websites
Appendix D: Sample terms of use for court websites
Appendix E: Sample notice of data breach

1. Introduction

1.1 Background

Privacy is a fundamental right guaranteed by the California Constitution. (Cal. Const., art I, § 1; see *Westbrook v. County of Los Angeles* (1994) 27 Cal. App 157, 164–166.) To protect people's privacy, numerous law have been enacted that provide for the confidentiality of various kinds of personal information. In adjudicating cases, courts have a major role in enforcing these laws and protecting the privacy rights of citizens. Courts also are involved in protecting people's privacy rights through their own day-to-day operations, including preserving the integrity of confidential and sealed records, ensuring that sensitive data is secure, and protecting private personal information.

On the other hand, access to information concerning the conduct of the public's business is also a fundamental right of every citizen. (Cal. Const., art I, § 3(b); see *NBC Subsidiary (KNBC–TV) v. Superior Court of Los Angeles County* (1999) 20 Cal.4th 1178, 1217–1218 (substantive courtroom proceedings in ordinary civil cases are "presumptively open").) Courts are obligated to conduct their business in an open and transparent manner. (See also Cal. Rules of Court, rule 10.500.) Similarly, court records are presumed to be open and must be made accessible to the public unless made confidential or sealed. (See Cal. Rules of Court, rule 2.550(c).)[1] Openness and accessibility are important to preserve trust and confidence in the judicial system; and they are necessary to carry on the regular, ongoing business of the courts.[2]

1.2 Purpose of the Privacy Resource Guide

The purpose of this resource guide is to assist the trial and appellate courts—and more generally the judicial branch— to protect the privacy interests of persons involved with the California court system while providing the public with reasonable access to the courts and the records to which they are entitled.

The resource guide provides assistance in two ways. First, it provides information about the legal requirements that guide the courts' activities and operations relating to protecting the privacy of persons involved with the court system. Second, the guide provides practical advice for courts on the best practices for carrying out their obligations to protect people's privacy.

The creation of the resource guide at this time is important, among other reasons, because of the major transition underway that is transforming the courts from a paper-based physical system to

[1] All references to rules in this Resource Guide are to the California Rules of Court, unless otherwise indicated.

[2] In recognition of the special role that courts play in conducting the people's business, the Legislature has in some instances exempted the courts from laws enacted to protect personal privacy. (See, e.g., Civ. Code, §1798.3(b)(1) [excluding from the definition of "agency" covered by the Information Privacy Act of 1977 "[a]ny agency established under Article VI of the California Constitution"—that is, the courts]).

one that relies increasingly on electronic records and other forms of technology to conduct business. With this change, much information in the courts that was practically obscure can now be made available remotely in easily searchable format. It requires careful analysis and the deliberate institution of new practices to ensure that proper privacy protections are now in place.

1.3 Key Definitions

As used in this Resource Guide, unless the context or subject matter otherwise requires:

(1) "Court record" means any document, paper, or exhibit filed by the parties to an action or proceeding; any order or judgment of the court; any item listed in Government Code section 68151, excluding any reporter's transcript for which the reporter is entitled to receive a fee for any copy. The term does not include the personal notes or preliminary memoranda of judges or other judicial branch personnel. (Cal. Rules of Court, rule 2.502.)

(2) "Electronic record" means a court record that requires the use of an electronic device to access. The term includes both a document that has been filed electronically and an electronic copy or version of a record that was filed in paper form. (See, e.g., Cal. Rules of Court, rule 8.82(2).)

(3) "Adjudicative record" means any writing prepared for or filed or used in a court proceeding, the judicial deliberation process, or the assignment or reassignment of cases and of justices, judges (including temporary and assigned judges), and subordinate judicial officers, or of counsel appointed or employed by the court. (Cal. Rules of Court, rule 10.500(c)(1).)

(4) "Confidential record" is a record that based on statute, rule, or case law is not open to inspection by the public. (See Cal Rules of Court, rule 8.45(b)(5)).)

(5) "Judicial administrative record" means any writing containing information relating to the conduct of the people's business that is prepared, owned, used, or retained by a judicial branch entity regardless of the writing's physical form or characteristics, except an adjudicative record. The term "judicial administrative record" does not include records of a personal nature that are not used in or do not relate to the people's business, such as personal notes, memoranda, electronic mail, calendar entries, and records of Internet use. (Cal. Rules of Court, rule 10.500(c)(2).)

(6) "Personally identifiable information" or "PII" includes information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of

birth, mother's maiden name, etc. (See *NIST Guide to Protecting the Confidentiality of Personally Identifiable Information* (SP 800-122).)

(7) A "redacted version" is a version of a record from which all portions that disclose materials contained in a sealed, conditionally sealed, or confidential record have been removed. (See Cal. Rules of Court, rule 8.45(b)(6).)

(8) "Rule" means a rule of the California Rules of Court.

(9) An "unredacted version" is a version of a record or a portion of a record that discloses materials contained in a sealed, conditionally sealed, or confidential record. (See Cal. Rules of Court, rule 8.45(b)(7).)

(10) "Sealed record" means a record that by court order is not open to inspection by the public. (See Cal. Rules of Court, rule 2.550(b)(2))

(11) "Writing" means any handwriting, typewriting, printing, photographing, photocopying, electronic mail, fax, and every other means of recording on any tangible thing any form of communication or representation, including letters, words, pictures, sounds, symbols, or combinations, regardless of the manner in which the record has been stored. (Cal. Rules of Court, rule 10.500(c)(6).)

2. Privacy in Court Records

2.1 Confidential and Sealed Records in the Trial Courts

Protection of privacy is an important major reason for making court records confidential or for sealing them. By making a document confidential or sealing it, the public can be prevented from obtaining access to sensitive personal information or other information that might adversely affect a person's privacy. By respecting and enforcing the confidentiality or sealing, courts assist in protecting and preserving persons' privacy. However, there may be other reasons for making a document confidential or for sealing it besides protecting privacy. For example, confidentiality or sealing may be used to ensure the safety of witnesses, to protect trade secrets, or to preserve legally recognized privileges. This section focuses on records that are confidential or sealed in the trial courts principally or at least in part for reasons of protecting privacy interests.

Subsection 2.1.1 provides a non-exhaustive list of types of cases and proceedings and of specific records[3] that are exempt from the presumption of public disclosure by statute, regulation, court rule, or case law. Some records by law are strictly confidential and others may be confidential in particular circumstances. In addition to the records described in this section, there are many other

[3] Judicial Council forms may sometimes constitute the record or part of the record in a case. Any Judicial Council form that is labeled or entitled "CONFIDENTIAL" must not be disclosed, except as authorized by law.

confidential records discussed under more specific headings later in this Resource Guide and described in the Appendix.

Sealed records in the trial courts are discussed in subsection 2.1.2

2.1.1 Confidential Records

Records of Adoption Proceedings

Documents related to an adoption proceeding are not open to the public. Only the parties, their attorneys, and the Department of Social Services may review the records. The judge can authorize review by a requestor only in "exceptional circumstances and for good cause approaching the necessitous." (Fam. Code, § 9200(a).) Any party to the proceeding can petition the court to have redacted from the records, before copy or inspection by the public, the name of the birth parents and information tending to identify the birth parents. (Fam. Code, § 9200(b).)

Records of Juvenile Proceedings

Welfare and Institutions Code section 827 and California Rules of Court, rule 5.552**,** establish broad restrictions on the disclosure of juvenile court records. These laws reflect a general policy that, with certain limited exceptions, juvenile court records should remain confidential. (*In re Keisha T.* (1995) 38 Cal.App.4th 220, 225.) Specifically, section 827(a)(1)(P) permits juvenile court records to be inspected only by certain specified persons and "any other person who may be designated by court order of the judge of the juvenile court upon filing a petition." There is also an exception to this rule of confidentiality for certain records in cases brought under Welfare and Institutions Code section 602, in which the minor is charged with one or more specified violent offenses. (Welf. & Inst. Code, § 676.) In such cases, the charging petition, the minutes, and the jurisdictional and dispositional orders are available for public inspection (Welf. & Inst. Code, § 676(d)), unless the juvenile court judge enters an order prohibiting disclosure (Welf. & Inst. Code, § 676(e)). Thus, except for records enumerated in Welfare and Institutions Code section 676, if a record is part of a juvenile court file, it should be kept confidential and disclosed only as permitted under Welfare and Institutions Code section 827 and California Rules of Court, rule 5.552. Juvenile court records may also be subject to sealing orders under Welfare and Institutions Code sections 389, 781, and 786 (see § 2.1.2, "Sealed Records").

Juvenile court records should remain confidential regardless of a juvenile's immigration status. (Welf. & Inst. Code, § 831(a).) Juvenile information may not be disclosed or disseminated to federal officials absent a court order upon filing a petition under Welfare and Institutions Code section 827(a). (Welf. & Inst. Code, § 831(b)–(c).) Juvenile information may not be attached to any documents given to or provided by federal officials absent prior approval of the presiding judge of the juvenile court under Welfare and Institutions Code section 827(a)(4). (Welf. & Inst. Code, § 831(d).) "Juvenile information" includes the "juvenile case file" as defined in Welfare and Institutions Code section 827(e), as well as information regarding the juvenile such as the juvenile's name, date or place of birth, and immigration status. (Welf. & Inst. Code, § 831(e).)

Dismissed petitions: The court must order sealed all records related to any petition dismissed under Welfare and Institutions Code section 786 that are in the custody of the juvenile court, law enforcement agencies, the probation department, and the Department of Justice. The procedures for sealing these records are stated in Welfare and Institutions Code section 786.

Special Immigrant Juvenile Findings

In any judicial proceedings in response to a request that the superior court make the findings necessary to support a petition for classification as a special immigrant juvenile, information regarding the child's immigration status that is not otherwise protected by the state confidentiality laws must remain confidential and must be available for inspection only by the court, the child who is the subject of the proceeding, the parties, the attorneys for the parties, the child's counsel, and the child's guardian. (Code Civ. Proc., § 155(c).)

In any judicial proceedings in response to a request that the superior court make the findings necessary to support a petition for classification as a special immigrant juvenile, records of the proceedings that are not otherwise protected by state confidentiality laws may be sealed using the procedure in California Rules of Court, rules 2.550 and 2.551. (Code Civ. Proc., § 155(d).)

Confidentiality of Records in Civil Cases

Unlawful Detainer Proceedings

Court files and records in unlawful detainer proceedings are not publicly available except for access to limited civil case records (including the court file, index, and register of actions) only to persons specified by statute under Code of Civil Procedure section 1161.2(a)(1)(A)-(D). (Code Civ. Proc., § 1161.2.) In addition, access to limited civil records in unlawful detainer proceedings shall be allowed only:

- To a person by order of court if judgment is entered for the plaintiff after trial more than 60 days since filing of the complaint (Code of Civ. Proc. § 1161.2(a)(1)(F));
- Except in cases involving residential property based on Section 1161a as indicated in the caption of the complaint, to any other person 60 days after the complaint has been filed if the plaintiff prevails in the action within 60 days of filing the complaint, in which case the clerk shall allow access to any court records in the action. If a default or default judgment is set aside more than 60 days after the complaint was filed, section 1161.2 shall apply as if the complaint had been filed on the date the default or default judgment is set aside (Code of Civ. Proc. § 1161.2(a)(1)(F));
- In the case of a complaint involving residential property based on Section 1161a as indicated on the caption of the complaint, to any other person, if 60 days have elapsed since the complaint was filed with the court, and as of that date, judgment against all defendants has been entered for the plaintiff, after a trial. (Code of Civ. Proc. § 1161.2(a)(1)(G).)

An exception excludes records of mobile home park tenancies from this code section if the caption in the complaint indicates clearly that the complaint seeks to terminate a mobile home park tenancy; those records are not confidential. In addition, effective January 1, 2011, access to court records in unlawful detainer proceedings is permanently limited to persons specified in the statute in the case of complaints involving residential property based on section 1161a (holding over after sale under execution, mortgage, or trust deed [foreclosures]) as indicated in the caption of the complaint, unless 60 days have elapsed since filing of the complaint and judgment has been entered, after a trial, for the plaintiff and against all defendants. (Code Civ. Proc., § 1161.2.)

The complaints in these actions shall state in the caption: "Action based on Code of Civil Procedure section 1161a."(Code Civ. Proc., § 1166(c).)

False Claims Act Cases

The documents initially filed in cases under the False Claims Act are confidential under Government Code section 12650 et seq. The complaint and other initial papers should be attached to a Confidential Cover Sheet—False Claims Action (form MC-060). The cover sheet contains a place where the date on which the sealing of the records in the case expires.

Confidential Records in Criminal Proceedings

Search warrants

It is within the court's discretion to seal the court documents and records of a search warrant until the warrant is executed and returned, or until the warrant expires. (Pen. Code, § 1534(a).) Thereafter, if the warrant has been executed, the documents and records shall be open to the public as a judicial record. Evidence Code §§ 1040 – 1041 establish exceptions to the public status of executed search warrants; these provisions allow public entities to refuse disclosure of confidential official information and an informant's identity when disclosure is against the public interest. When a search warrant is valid on its face, a public entity bringing a criminal proceeding may establish the search's legality without revealing to the defendant any confidential official information or an informant's identity. (Evid. Code, § 1042, subd. (b).) When a search warrant affidavit is fully or partially sealed pursuant to Evidence Code §§ 1040 - 1042, the defense may request a motion to quash or traverse the search warrant. The court should follow the procedure established in *People v. Hobbs* (1994) 7 Cal.4th 948.

Police reports

There is no specific statute, rule, or decision addressing the confidentiality of a police report once it has become a "court record." Generally speaking, a police report that has been used in a judicial proceeding or is placed in a court file is presumed to be open to the public. Many police reports, however, contain sensitive or personal information about crime victims, witnesses, and other third parties. Penal Code section 1054.2 provides that defense counsel may not disclose the address or telephone number of a victim or witness to the defendant or his or her family. Similarly, law enforcement agencies are prohibited from disclosing the address and phone number of a witness or victim, or an arrestee or potential defendant. (Pen. Code, § 841.5.) We suggest that courts should require that personal information be redacted *before* the report is filed with the court or used in a judicial proceeding.

Probation reports

Probation reports filed with the court are confidential *except* that they may be inspected

- by anyone up to 60 days after either of two dates, whichever is earlier: (1) when judgment is pronounced, or (2) when probation is granted;
- by any person pursuant to a court order;
- if made public by the court on its own motion; and
- by any person authorized or required by law. (Pen. Code, § 1203.05.)

Confidential Records in Family Law proceedings

Child custody evaluation reports
These reports must be kept in the confidential portion of the family law file and are available only to the court, the parties, their attorneys, federal or state law enforcement, judicial officer, court employee or family court facilitator for the county in which the action was filed (or employee or agent of facilitator), counsel for the child, and any other person upon order of the court for good cause. (Fam. Code, §§ 3025.5 and 3111.)

Child custody mediator recommendations
These recommendations must be kept in the confidential portion of the family law file and are available only to the court, the parties, their attorneys, federal or state law enforcement, judicial officer, court employee or family court facilitator for the county in which the action was filed (or employee or agent of facilitator), counsel for the child, and any other person upon order of the court for good cause. (Fam. Code, §§ 3025.5 and 3183.)

Written statements of issues and contentions by counsel appointed for child
These written statements must be kept in the confidential portion of the family law file and are available only to the court, the parties, their attorneys, federal or state law enforcement, judicial officers, court employees or family court facilitators for the county in which the action was filed (or employee or agent of facilitator), counsel for the child, and any other person, upon order of the court, for good cause. (Fam. Code, §§ 3025.5, 3151(b).)

Parentage Act documents
Records in Uniform Parentage Act proceedings, except the final judgment, are not open to the public. (Fam. Code, § 7643(a).) If a judge finds that a third party has shown good cause and finds exceptional circumstances, the court may grant that person access to the records. (*Ibid.*) This includes records from paternity actions.

Family conciliation court records
These records are confidential. The judge of the family conciliation court can grant permission for a party to review certain documents. (Fam. Code, § 1818(b).)

Proceeding to terminate parental rights
Documents related to such proceedings are confidential; only persons specified by law may review the records. (Fam. Code, § 7805.)

Support enforcement and child abduction records
Support enforcement and child abduction records are generally confidential; these records may be disclosed to persons specified by statute only under limited circumstances. In certain instances, the whereabouts of a party or a child must not be revealed to the other party or his or her attorneys. A local child support agency must redact such information from documents filed with the court. (Fam. Code, § 17212.)

Confidential Records in Probate Proceedings

Confidential Guardian Screening Form (form GC-212)

This mandatory Judicial Council form regarding the proposed guardian is confidential. It is used by the court and by persons or agencies designated by the court to assist in determining whether a proposed guardian should be appointed. (Cal. Rules of Court, rule 7.1001(c).)

Confidential Supplemental Information (form GC-312)
This form regarding the proposed conservatee is confidential. It shall be separate and distinct from the form for the petition. The form shall be made available only to parties, persons given notice of the petition who have requested this supplemental information, or who have appeared in the proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Prob. Code, 1821(a).)

Confidential Conservator Screening Form (form GC-314)
This mandatory Judicial Council form is confidential. (Cal. Rules of Court, rule 7.1050(c).)

Reports regarding proposed conservators or guardianship
An investigative report created pursuant to Probate Code section 1513 concerning a proposed guardianship is confidential and available only to parties served in the action or their attorneys (generally, parents, legal custodian of child). An investigative report created pursuant to Probate Code section 1826 regarding the proposed conservatee is confidential and available only to those persons specified by statute. Under the statute, the reports on proposed conservatees shall be made available only to parties, persons given notice of the petition who have requested the report, or who have appeared in the proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the reports on guardianships and conservatorships exclusively to persons entitled thereto. (Prob. Code, §§ 1513(d) and 1826(n).)

Investigator's review reports in conservatorships
These reports are confidential. The information in the reports may be made available only to parties, persons identified in section 1851(b), persons given notice who have requested the report or appeared in the proceeding, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interests of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Prob. Code, §§ 1851(b) and (e).) Subdivision (b) provides for special restricted treatment of attachments containing medical information and confidential criminal information from California Law Enforcement Telecommunications System (CLETS). Although the attachments are not mentioned in (e), it is recommended, to be consistent with (b), that they be treated as confidential except to the conservator, conservatee, and their attorneys.

Certification Forms
Certification of counsel of their qualifications (form GC-010) and certification of completion of continuing education (form GC-011): The forms state that they are "confidential for court use only." They are governed by rule 7.1101, which states that the certifications must be submitted to the court but not lodged or filed in a case file. (Cal. Rules of Court, rule 7.1101(h)(6).)

Confidential Records in Protective Order Proceedings

Confidential CLETS Information Form

A Judicial Council form, *Confidential CLETS Information* **(**form CLETS-001), has been developed for petitioners in protective order proceedings to use to submit information about themselves and the respondents to be entered through the CLETS (the California Law Enforcement Telecommunications System) into the California Restraining and Protective Order System (CARPOS), a statewide database used to enforce protective orders. This form is submitted to the courts by petitioners in many types of protective order proceedings, including proceedings to prevent domestic violence, civil harassment, elder and dependent adult abuse, private postsecondary school violence, and juvenile cases. The information on the forms is intended for the use of law enforcement. The form is confidential. Access to the information on the forms is limited to authorized court personnel, law enforcement, and other personnel authorized by the California Department of Justice to transmit or receive CLETS information. The forms must not be included in the court file. (Cal. Rules of Court, rule 1.51.)

Subpoenaed records

Subpoenaed business records

Subpoenaed business records of nonparty entities are confidential until otherwise agreed to by the parties, introduced as evidence, or entered into the record. (Evid. Code, § 1560(d).)

Employment records

Pitchess motions

Medical records

The following federal and California statutes limit disclosure of medical records by medical providers, health care plans, or contractors. The laws do not impose obligations on the courts as to handling, management, and retention of medical records in court records. However, courts should place appropriate protections on medical records that have been filed confidentially or under seal.

Health Insurance Portability and Accountability Act (HIPAA):

HIPAA and related federal regulations (42 U.S.C. § 1320d et seq., 45 C.F.R. § 160 et seq. and 164 et seq.) set standards for medical information held by covered entities, defined as: 1) a health plan, 2) health care clearinghouse, or 3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA provisions. (45 C.F.R. § 160.102(a).) Generally, courts participating in CalPERS Health Program, county-sponsored health plans, the Trial Court Benefits Program administered by the Judicial Council, or other fully insured plans are not covered entities subject to HIPAA and

therefore, the privacy rules of HIPAA do not directly apply to courts in their judicial function. (See 45 C.F.R. parts 160-164.) However, HIPAA prohibits covered entities from disclosing medical records or protected health information ("PHI") without a patient's signed authorization or a signed court order. (45 C.F.R. § 164.508; 45 C.F.R. §164.512(e)(1).) Parties responsible for maintaining confidentiality of information under HIPAA should request that such information be filed under seal pursuant to rules 2.550 and 2.551 of the California Rules of Court.

Because a court may meet the definition of "plan sponsor" under HIPAA (45 C.F.R.§ 164.103), a court may have to comply with two minimal privacy obligations under HIPAA: (1) the "nonwaiver" provision, which prohibits a requirement that an individual waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility; and (2) the "nonretaliation" provision, which forbids retaliatory action against individuals for exercising rights under HIPAA. Courts should consult with their Human Resources departments for appropriate personnel policy language.

California Confidentiality of Medical Information Act (Civ. Code, section 56-56.37):
The Confidentiality of Medical Information Act ("CMIA") governs the disclosure of medical information by health care providers. (Civ. Code § 56 et seq.) Courts are generally not health care providers covered by the act and are not directly subject to the law's confidentiality provisions. (Civ. Code § 56.05(m).) A limited exception may occur when a court employs a health care provider, such as a clinical social worker, to conduct assessments and other services for a collaborative court. In these limited circumstances, the medical information is likely confidential, and court staff should use an authorization for release of medical information to discuss pertinent information with other collaborative court team members. (Civ. Code, § 56.10(a).) California law prohibits medical providers, health care service plans, or contractors from disclosing a patient's medical information, without authorization, or, among other things, a court order. (Civ. Code, § 56.10(b)(1).) A party submitting such medical information should submit the information pursuant either to a protective order and/or a motion to seal. (See Rule 2.551.)

- **[Practice Tip**: When parties submit medical information without seeking a protective order or filing a motion to seal, a court may, if it identifies such information, issue on its own motion a qualified protective order filing such information under seal.]

Psychiatric records or reports

Records of mental health treatment or services for the developmentally disabled, including LPS proceedings
Under Welfare and Institutions Code sections 5328 and 5330, the following records are confidential and can be disclosed only to recipients authorized in Welfare and Institutions Code section 5328: records related to the Department of Mental Health (Welf. & Inst. Code, § 4000 et seq.); Developmental Services (Welf. & Inst. Code, § 4400 et seq.); Community Mental Health Services (Welf. & Inst. Code, § 5000 et seq.); services for the developmentally disabled (Welf. & Inst. Code, § 4500 et seq.); voluntary admission to mental hospitals (Welf. & Inst. Code, § 6000 et seq.); and mental institutions (Welf. & Inst. Code, § 7100 et seq.).

Psychiatric records or reports in criminal cases
Reports prepared at the request of defense counsel to determine whether to enter or withdraw a plea based on insanity or mental or emotional condition are confidential. (Evid. Code, § 1017.) However, most psychiatric reports prepared at the court's request are presumed open to the public. (See Evid. Code, § 1017[report by a court-appointed psychotherapist]; Evid. Code, § 730 [report by a court-appointed expert]; Pen. Code, § 288.1 [report on sex offender prior to suspension of sentence]; Pen. Code, § 1368 [report concerning defendant's competency]; and Pen. Code, §§ 1026, 1027 [report on persons pleading not guilty by reason of insanity].)

Reports concerning mentally disordered prisoners
Reports under Penal Code section 4011.6 to evaluate whether prisoners are mentally disordered are confidential. (Pen. Code, § 4011.6.)

Presentencing diagnostic reports
Under Penal Code section 1203.03, the report and recommendation from the 90-day Department of Corrections presentencing diagnosis should be released only to defendant or defense counsel, the probation officer, and the prosecuting attorney. After the case closes, only those persons listed immediately above, the court, and the Department of Corrections may access the report. Disclosure to anyone else is prohibited unless the defendant consents. (Pen. Code, § 1203.03(b).)

Medical diagnoses and test results

Substance use disorder-related information from qualifying federally assisted programs
The Code of Federal Regulations provides that information that would disclose the identity of a person receiving treatment for a substance use disorder from a qualifying federally assisted program is confidential. (42 C.F.R. § 2.12.) A "qualifying federally assisted program" subject to the regulations includes a recipient of federal financial assistance in any form, including financial assistance which does not directly pay for the substance use disorder diagnosis, treatment, or referral for treatment; or a program conducted by a state or local government unit which, through general or special revenue sharing or other forms of assistance, receives federal funds which could be (but are not necessarily) spent for the substance use disorder program. (*Id*. at § 2.12(b)(3)(i), (ii).) A "program" is defined to include "an individual or entity (other than a general medical care facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment or referral for treatment ". . . (*Id*. at. § 2.11(a).) Information from collaborative courts involving substance use disorder diagnosis or treatment, such as drug court programs, may be subject to the confidentiality provisions of the federal regulations, depending on whether the program or the court receives federal financial assistance as defined in the regulations. This may include information related to program participants and records identifying the participant and his or her diagnosis and treatment.

Infectious or Communicable Disease Information Under Health and Safety Code § 120290(h)(1) (Stats. 2017, ch. 537, § 5, operative January 1, 2018), when alleging a violation of 120290(a) (Stats. 2017, ch. 537, § 5, operative January 1, 2018), the prosecuting attorney or the grand jury must substitute a pseudonym for the true name of a complaining witness. The actual

name and other identifying characteristics of a complaining witness shall be revealed to the court only in camera, unless the complaining witness requests otherwise, and the court shall seal the information from further disclosure, except by counsel as part of discovery. Under Health and Safety Code § 120290(h)(2) (Stats. 2017, ch. 537, § 5, operative January 1, 2018), unless the complaining witness requests otherwise, all court decisions, orders, petitions, and other documents, including motions and papers filed by the parties, shall be worded so as to protect the name or other identifying characteristics of the complaining witness from public disclosure.

Under Health and Safety Code § 120290(h)(3) (Stats. 2017, ch. 537, § 5, operative January 1, 2018), unless the complaining witness requests otherwise, a court in which a violation of this section is filed shall, at the first opportunity, issue an order that prohibits counsel, their agents, law enforcement personnel, and court staff from making a public disclosure of the name or any other identifying characteristic of the complaining witness.

Under Health and Safety Code § 120290(h)(4) (Stats. 2017, ch. 537, § 5, operative January 1, 2018), unless the defendant requests otherwise, a court in which a violation of this section is filed, at the earliest opportunity, shall issue an order that counsel and their agents, law enforcement personnel, and court staff, before a finding of guilt, not publicly disclose the name or other identifying characteristics of the defendant, except by counsel as part of discovery or to a limited number of relevant individuals in its investigation of the specific charges under this section. In any public disclosure, a pseudonym shall be substituted for the true name of the defendant.

HIV Test Results or Status

No person shall disclose HIV test results without the patient's signed authorization, or except pursuant to Health and Safety Code sections 1603.1, 1603.3, or 121022, or any other statute expressly providing an exemption. (Health and Saf. Code, § 120980(g).)

Court records containing results of mandatory AIDS testing for defendants convicted of violating Penal Code section 647(b) are, with certain specified exceptions, confidential. (Former Pen. Code, § 1202.6(f), repealed and added as of January 1, 2018 (Stats. 2017, ch. 537, § 16, operative January 1, 2018).) HIV test results ordered of defendants charged with certain crimes are also confidentiall. (Pen. Code, §§ 1202.1, 1524.1.)

Penal Code section 1202.1 requires every person convicted of the following crimes to undergo an HIV test: rape in violation of Pen. Code Pen. Code sections 261 or 264.1; unlawful intercourse with a person under 18 years of age in violation of Penal Code sections 261.5 or 266c; rape of a spouse in violation of Penal Code sections 262 or 264.1; sodomy in violation of Penal Code sections 266c or 288a; or any offenses if the court finds that there is probable cause to believe that blood, semen, or other bodily fluid capable of transmitting HIV has been transferred from the defendant to the victim during certain offenses or attempts to commit such offenses (sexual penetration in violation of Penal Code sections 264.1, 266c, or 289; aggravated sexual assault of a child in violation of Penal Code section 269; lewd or lascivious conduct with a child in violation of Penal Code section 288; continuous sexual abuse of a child in violation of

Penal Code section 288.5). The clerk of the court shall transmit the HIV results to the Department of Justice and the local health officer.

Penal Code section 1524.1 provides that, where there is (i) a defendant charged with certain crimes (Penal Code sections 220, 261, 262, 264.1, 266c, 269, 286, 288, 288a, 288.5, 289.5) or with the attempt to commit any of these offenses, ***and*** is the subject of a police report alleging commission of, or of attempt to commit, a separate, uncharged offense that could be charged under those previously cited statutes; or (ii) a minor is the subject of a petition filed in juvenile court alleging commission of crimes under those cited statutes, or attempt to commit any of the offenses, and is the subject of a police report alleging commission of a separate, uncharged offense under those cited statutes, or attempt to commit any of those offenses, at the request of the victim of the uncharged offense, the court may issue a search warrant to obtain a HIV test from the charged defendant or minor upon proper findings of probable cause.
If a court orders HIV tests under Health and Safety Code sections 121055, 121056, and 121060, the court shall order that all persons receiving the results maintain the confidentiality of personal identifying data related to the test results, except as necessary for medical or psychological care or advice. (Health and Saf. Code, § 121065.)

However, HIV status and/or test results under former Penal Code § 647f and § 12022.85, and former Health and Safety Code §§ 1621.5, 120290, and 120291 are generally not confidential as they are a required element of a crime or enhanced sentencing and may become part of the public court records in these cases. (Former Penal Code section 647f was repealed as of January 1, 2018 by Stats. 2017, ch. 537, § 8; former Health and Safety Code section 1621.5 was repealed as of January 1, 2018 by Stats. 2017, ch. 537, § 2; former Health and Safety Code section 120290 was repealed as of January 1, 2018 (Stats. 2017, ch. 537, § 4) and new Health and Safety Code section 120290 was added as of January 1, 2018 (Stats. 2017, ch. 537, §5); former Health and Safety Code section 120291 was repealeded as of January 1, 2018, by Stats. 2017, ch. 537, § 6.)

Further, see above discussion regarding Medical Diagnoses and Tests for discussion about Health and Safety Code section 120290(h)(1) and requirements for sealing information in cases regarding alleged violations of section 120290(a).

2.1.2 Sealed records

General Rules on Sealed Records: Rules 2.500 and 2.551

The main rules on sealed records in the trial courts are contained in rules 2.550 and 2.551 of the California Rules of Court. The premise of these rules is that court records are presumed to be open unless confidentiality is required by law. (Rule 2.550(c).) A court may only order that a record be filed under seal if it expressly finds facts that establish:

(1) There exists an overriding interest that overcomes the right of public access to the record;

(2) The overriding interest supports sealing the record;

(3) A substantial probability exists that the overriding interest will be prejudiced if the record is not sealed;

(4) The proposed sealing is narrowly tailored; and

(5) No less restrictive means exist to achieve the overriding interest.

(Rule 2.551(d).) This substantive test is based on the Supreme Court's decision in *NBC Subsidiary (KNBC–TV) v. Superior Court of Los Angeles County* (1999) 20 Cal.4th 1178, 1217–1218.

The right of privacy may qualify as an overriding interest in the proper situation. In *In re Marriage of Burkle* (2006) 135 Cal. App.4th 1045, the court stated: "We have no doubt that, in appropriate circumstances, the right of privacy may be properly described as a compelling or overriding interest." *Id.*, at page 1063. However, the *Burkle* case involved an attempt to close financial records in divorce proceedings under a statute, Family 2024.6, which the court concluded was not narrowly tailored to serve overriding privacy interests. Because less restrictive means exist to achieve the statutory objective, the court found that section 2024.6 operates as an undue burden on the First Amendment right of public access to court records. Hence, the court concluded that statute is unconstitutional on its face. *Id.* at page 1048.

In circumstances where a court determines that sealing is appropriate, the content and scope of the sealing order is prescribed by rule. The rules provide that the court's order must (1) state the facts that support the findings, and (2) direct the sealing of only those documents and pages, or if reasonably practical, portions of those documents and pages, that contain the materials that need to be placed under seal. All other portions of each document or page must be included in the public file. (Cal. Rules of Court, rule 2.550(e).)

The procedures for filing records under seal in the trial courts are contained in rule 2.551. (Cal. Rules of Court, rule 2.551.)

Sealing of records in criminal cases

Criminal court records may be sealed upon a motion and court order under various provisions. See Appendix A.

Sealing of Records in Juvenile Cases

There is a specific statute and rule on sealing juvenile records. (Welf. & Inst. Code, § 781; Cal. Rules of Court, rule 5.830.) These allow a former ward of the court to petition the court to order juvenile records sealed. If the petition is granted, the court must order the sealing of all records described in section 781. The order must apply in the county of the court hearing the petition and all other counties in which there are juvenile records concerning the petitioner. (Cal. Rules of Court, rule 5.830(a)(4).) All records sealed must be destroyed according to section 781(d).

2.2 Confidential and Sealed Records in the Appellate Courts

For appeals and original proceedings in the Supreme Court and Courts of Appeal, specific rules have been adopted relating to sealed and confidential records: rule 8.45 (general provisions), rule 8.46 (sealed records), and rule 8.47 (confidential records).

2.2.1 General provisions

Rule 8.45 provides general requirements for the handling of sealed and confidential records by a reviewing court. These records must be kept separate from the rest of the records sent to the court and must be kept in a secure manner that preserves their confidentiality. (Rule 8.45(c)(1).) The rule prescribes the format of sealed and confidential records, and states the manner in which these records are to be listed in alphabetical and chronological indexes available to the public. (Rule 8.45(c)(2).) It describes the special treatment required for records relating to a request for funds under Penal Code 987.9. (Rule 8.45(c)(3).)

Rule 8.45 also provides guidance on the transmission of and access to sealed and confidential records. For instance, unless otherwise provided by law, a sealed or confidential record that is part of the record on appeal must be transmitted only to the reviewing court and the party or parties who had access to the record in the trial court and may be examined only by the reviewing court and that party or parties. If a party's attorney but not the party had access to the record in the trial court, only the party's attorney may examine the record. (Rule 8.45(d)(1).)

2.2.2 Sealed records

Rule 8.46 is the basic rule on sealed records in the reviewing court. First, it provides that if a record sealed by order of the trial court is part of the record on appeal, the sealed record must remain sealed unless the reviewing court orders otherwise. The record on appeal or supporting documents must include the motion or application to seal in the trial court, all documents filed in the trial court supporting or opposing the motion or application to seal, and the trial court order sealing the record. (Rule 8.46(b)((1)–(2).)

Second, a record filed or lodged publicly in the trial court and not ordered sealed must not be filed under seal in the reviewing court. (Rule 8.46(c).)

Third, the rule prescribes the procedures for obtaining an order from a reviewing court to seal a record that was not filed in the trial court. (Rule 8.46(d).)

Fourth, a sealed record must not be unsealed except on order of the reviewing court. The rule prescribes the procedures for seeking to unseal a record in the reviewing court. (Rule 8.46(e).)

Fifth, the rule prohibits the public filing in a reviewing court of material that was filed under seal, lodged conditionally under seal, or otherwise subject to a pending motion to file under seal. (Rule 8.46(f).)

2.2.3 Confidential records

Rule 8.47 governs the form and transmission of and access to confidential records (as distinguished from records sealed by court order or filed conditionally sealed) in the appellate courts. (Rule 8.47(a).) The rule includes a subdivision specifically on how to handle reporter's transcripts and documents filed or lodged in *Marsden* hearings and other in-camera proceedings. (Rule 8.47(b).) It also contains general procedures for handling other confidential records. (Rule 8.47(c).)

2.3 Privacy in Opinions of the Courts of Appeal

Based on concerns about the need for privacy protection, two rules of court have been adopted relating to the references to specific individuals in opinions and certain other records.

2.3.1 Privacy in appellate opinions

Rule 8.90, adopted effective January 1, 2017, provides guidance on the use of names in appellate court opinions, except for names in juvenile cases that are covered by rule 8.401 (discussed below). The rule states that, to protect personal privacy interests, the reviewing court should consider referring in opinions to people on the following list by first name and last initial or, if the first name is unusual or other circumstances would defeat the objective of anonymity, by initials only:

(1) Children in all proceedings under the Family Code and protected persons in domestic violence–prevention proceedings;

(2) Wards in guardianship proceedings and conservatees in conservatorship proceedings;

(3) Patients in mental health proceedings;

(4) Victims in criminal proceedings;

(5) Protected persons in civil harassment proceedings under Code of Civil Procedure section 527.6;

(6) Protected persons in workplace violence–prevention proceedings under Code of Civil Procedure section 527.8;

(7) Protected persons in private postsecondary school violence–prevention proceedings under Code of Civil Procedure section 527.85;

(8) Protected persons in elder or dependent adult abuse–prevention proceedings under Welfare and Institutions Code section 15657.03;

(9) Minors or persons with disabilities in proceedings to compromise the claims of a minor or a person with a disability;

(10) Persons in other circumstances in which personal privacy interests support not using the person's name; and

(11) Persons in other circumstances in which use of that person's full name would defeat the objective of anonymity for a person identified in (1)–(10).

2.3.2 Confidentiality in juvenile records and opinions

To protect the anonymity of juveniles involved in juvenile court proceedings, rule 8.401, adopted effective January 1, 2012, provides:

- In all documents filed by the parties in juvenile appeals and writ proceedings, a juvenile must be referred to by first name and last initial; but if the first name is unusual or other circumstances would defeat the objective of anonymity, the initials of the juvenile may be used.

- In opinions that are not certified for publication and in court orders, a juvenile may be referred to either by first name and last initial or by his or her initials. In opinions that are certified for publication, a juvenile must be referred to by first name and last initial; but if the first name is unusual or other circumstances would defeat the objective of anonymity, the initials of the juvenile may be used.

- In all documents filed by the parties and in all court orders and opinions in juvenile appeals and writ proceedings, if use of the full name of a juvenile's relative would defeat the objective of anonymity for the juvenile, the relative must be referred to by first name and last initial; but if the first name is unusual or other circumstances would defeat the objective of anonymity for the juvenile, the initials of the relative may be used.

(Rule 8.401(a).)

Rule 8.401 also contains provisions regarding access to filed documents. In general, the record on appeal and documents filed by the parties in proceedings under this chapter may be inspected only by the reviewing court and appellate project personnel, the parties or their attorneys, and other persons the court may designate. Filed documents that protect anonymity as required by subdivision (a) may be inspected by any person or entity that is considering filing an amicus curiae brief. And access to records that are sealed or confidential under authority other than Welfare and Institutions Code section 827 is governed by rules 8.45–8.47 and the applicable statute, rule, sealing order, or other authority.

Rule 8.401 also allows the court to limit or prohibit admittance to oral argument. (Rule 8.401(c).)

2.3.2 Other Privacy Concerns

In addition, the rules prohibit a document filed in the reviewing court or an appellate opinion from including social security numbers or financial account numbers. (Rules 1.201, 8.41, and 8.70(c)(2).)

The reviewing court might also consider omitting from an opinion other information that could indirectly identify a person protected under rules 8.90 or 8.401, such as dates, addresses, street names, or names of a school or business.

2.4 Redaction of Trial and Appellate Court Records

2.4.1 Redaction of Social Security numbers and financial account numbers

California Rules of Court, rules 1.201 and 8.41 impose a duty on the parties or their attorneys to redact certain identifiers (i.e., Social Security Numbers and financial account numbers) from documents filed with the court. It is the responsibility of the filers to exclude or redact the identifiers. The rules state that court clerks will not review each pleading or other paper for compliance with the requirements of the rules. In an appropriate case, the court on a showing of good cause may order a party filing a redacted document to file a *Confidential Reference List* (form MC-120) identifying the redacted information. This form is confidential.

2.4.2 Redaction of Social Security Numbers from documents filed in dissolution of marriage, nullity of marriage, and dissolution cases

In general, petitioners and respondents may redact any social security number from any pleading, attachment, document, or other written materials filed with the court pursuant to a petition for dissolution of marriage, nullity of marriage, or legal separation. (Family Code, § 2024.5(a).) However, an abstract of support judgment, the form required pursuant to Family Code section 4014, or any similar form created for the purpose of collecting child or spousal support payments may not be redacted. (Family Code, § 2024.5(b).)

2.4.3 Abstracts of judgment or decrees requiring payment of money

The contents of an abstract of judgment or a decree requiring the payment of money are prescribed by Code of Civil Procedure section 674. The section provides that any judgment or decree shall contain *the last four digits* of the social security number and the driver's license number of the judgment debtor if they are known to the judgment creditor. (Code Civ. Proc., § 674(a)(6).)

2.4.4. Redaction of information about victims or witnesses in criminal cases

Law enforcement agencies are prohibited from disclosing the address and phone number of a witness or victim to an arrestee or potential defendant. (Pen. Code, § 841.5.) Similarly, defense counsel may not disclose the address or telephone number of a victim or witness to the defendant, his or her family, or anyone else. (Penal Code, § section 1054.2) This information may be contained in police reports and other documents filed with the courts. It is recommended that courts require that the addresses and telephone numbers of victims and witnesses be redacted *before* any document containing that information is filed with the court or used in a judicial proceeding.

2.5 Destruction of Records

2.5.1 Destruction of criminal records

Records of arrest or conviction for marijuana related offenses
These records include all offenses under Health & Saf. Code § 11357, § 11360(b), and any records pertaining to the arrest and conviction of any person under 18 for violations under Health & Saf. Code §§ 11357-11362.9, except for § 11357.5. These records must be destroyed two years from either the date of conviction, the date of arrest if there was no conviction, or two years upon release from custody for persons incarcerated pursuant to the subdivision. (Health & Saf. Code, § 11361.5(a).) Records associated with violations of section 11357(d) shall be retained until the offender turns 18, at which point they are also to be destroyed. (Health & Saf. Code, § 11361.5(a).) This rule is subject to exceptions for records from judicial proceedings and records related to an offender's civil action against a public entity. (See Health & Saf. Code, § 11361.5(d).) Public agencies are prohibited from using information in records subject to destruction, even if they have not yet been destroyed. (Health & Saf. Code, 11361.7(b).)

3. Access to Court Records

3.1 Public Access to Trial Court Records

Court records are presumed to be open, unless they are confidential as a matter of law or are sealed by court order. Confidential and sealed records are described in sections 2.1 and 2.2 and Appendix 1.

3.1.1. Public access to paper court records at the courthouse

Paper records that are not confidential or sealed are available at the courthouse for public inspection and copying. These paper records in the past were often costly to locate, inspect, and copy. The difficulties and expenses involved in obtaining these paper records impeded public access but also provided an added level of privacy. This important practical effect of older court business practices was reflected in the "doctrine of practical obscurity," which recognized that obscurity could serve positive purposes with respect to protecting privacy interests.

Increasingly courts are relying on records created and maintained in electronic format. These records can be searched and made accessible remotely. Thus, if the benefits of "practical obscurity" are to be preserved, this will no longer be a by-product of old paper–based business practices. Instead, providing privacy protection through differential ease of access to court records is a conscious policy choice and requires carefully planned implementation.

3.1.2 Electronic court records

Rules 2.500–2.507 of the California Rules of Court first adopted in 2002 are intended to provide the public with reasonable access to trial court records that are maintained in electronic form while protecting privacy interests. These rules prescribe how the public may access electronic records both at the courthouse and remotely.

The rules are not intended to give the public a right of access to any electronic record that they are not otherwise entitled to access in paper form, and do not create any right of access to records sealed by court order or confidential as a matter of law. These rules apply only to trial court records and only to access to court records by the public. They do not prescribe the access to court records by a party to an action or proceeding, by the attorney for a party, or by other persons or entities that may be entitled to such access by statute or rule.

3.1.3 Courthouse and remote access to electronic records

The law requires that court records maintained in electronic form "shall be made reasonably accessible to all members of the public for viewing and duplication as the paper records would have been accessible." (Gov. Code, § 68150(*l*).) Electronic access must be available at the courthouse and may also be made available remotely.

If a court maintains records in electronic form, it must provide a means for the public to view those records at the courthouse. "Unless access is otherwise restricted by law, court records maintained in electronic form shall be viewable at the courthouse, *regardless of whether they are also accessible remotely*." (Gov. Code, § 68150(*l*) (emphasis added).

3.1.4 Access by type of record

There are some important restrictions on the records that may be made available remotely that do not apply to records at the courthouse. By rule of court, the following types of court records may not be made available remotely to the public:

(1) Records in a proceeding under the Family Code, including proceedings for dissolution, legal separation, and nullity of marriage; child and spousal support proceedings; child custody proceedings; and domestic violence prevention proceedings;
(2) Records in a juvenile court proceeding;
(3) Records in a guardianship or conservatorship proceeding;
(4) Records in a mental health proceeding;
(5) Records in a criminal proceeding;
(6) Records in a civil harassment proceeding under Code of Civil Procedure section 527.6;
(7) Records in a workplace violence prevention proceeding under Code of Civil Procedure section 527.8;
(8) Records in a private postsecondary school violence prevention proceeding under Code of Civil Procedure section 527.85;
(9) Records in an elder or dependent adult abuse prevention proceeding under Welfare and Institutions Code section 15657.03; and
(10) Records in proceedings to compromise the claims of a minor or a person with a disability.

(See rule 2.503(c).) As this list indicates, many of the types of cases whose records that are by deliberate policy not made readily available remotely to the public involve sensitive private personal and financial information about children, elderly and disabled persons, and victims of crime and violence.

3.1.5 Remote access in high-profile criminal cases

Notwithstanding the general restriction against providing criminal records remotely in rule 2.503(c), under rule 2.503(e), the presiding judge or a designated judge may order the records of

a high-profile criminal case to be posted on the court's website to enable faster and easier access to these records by the media and public. This rule specifies several factors that judges must consider before taking such action. One of the factors to be considered is: "The privacy interests of parties, victims, witnesses, and court personnel, and the ability of the court to redact sensitive personal information." (Rule 2.503(e)(1)(A).) Prior to posting, staff should, to the extent feasible, redact any confidential information contained in the court documents in accord with California Rules of Court, rule 2.503(e)(2). In addition, five days' notice must be provided to the parties and the public before the court makes a determination to provide electronic access under the rule.

3.1.6 Case-by-case access

The court may only grant electronic access to an electronic record when the record is identified by the number of the case, the caption of the case, or the name of party, and only on a case-by-case basis. (Rule 2.503(f).)

3.1.7 Bulk data

The court may provide bulk distribution of only its electronic records of a calendar, index, or register of actions. "Bulk distribution" means distribution of all, or a significant subset, of the court's electronic records. (Rule 2.503(g).)

3.1.8 Access to calendars, indexes, and registers of action

Courts that maintain records in electronic form must, to the extent feasible, provide—both at the courthouse and remotely—access to registers of action, calendars, and indexes. (Cal. Rules of Court, rule 2.503(b).) The minimum contents for electronically accessible court calendars, indexes, and registers of action are prescribed by rule. (See rule 2.507(b).) This enables the public to obtain access to court records in an effective, meaningful way.

There is also a rule on what information must be *excluded* from court calendars, indexes, and registers of action; the information to be excluded includes social security numbers, financial information, arrest and search warrant information, victim and witness information, ethnicity, age, gender, government (i.e., military) I.D. numbers, driver's license numbers, and dates of birth. (See rule 2.507(c).) Thus, the rule on court calendars, indexes, and registers of action explicitly recognizes the parties to lawsuits have important privacy rights that should not be compromised by easily and unnecessarily providing large amounts of private information.

3.1.9 Retention of user access information

[To be added. This might cross-reference website policy.]

3.2 Public Access to Records in the Courts of Appeal

Appellate court records are assumed to be open unless they are confidential as a matter of law or are sealed by court order. Confidential and sealed records on appeal are described in section 2.2 on rules 8.46 (sealed records) and rule 8.47 (confidential records). This section addresses other rules on access to appellate court records that are intended to protect persons' privacy interests.

3.2.1. The transition to electronic court records in the courts of appeal

Historically, paper records that are not confidential or sealed have been available at the appellate court for public inspection and copying. However, like the trial courts, the appellate courts are increasingly relying on records created and maintained in electronic rather than paper form. These electronic records can be made available remotely to the extent feasible and permitted by law.

The paper records used in the past were costly to locate, inspect, and copy. The difficulties and expense involved in obtaining these paper records impeded public access but also provided an added level of privacy. This important practical effect of older business practices was reflected in the doctrine of "practical obscurity," which recognized that obscurity could serve positive purposes with respect to protecting privacy interests. But as the appellate courts are shifting to electronic records, protecting privacy interests is no longer a by-product of paper-based business practices, but rather is the result of deliberate policy choices to provide differential access to electronic records. These policy choices are reflected in the rules of court on remote access to records.

3.2.2 Public access to electronic appellate court records

Public access to appellate court records are governed by rules 8.80–8.85:

- Rule 8.80. Statement of purpose
- Rule 8.81. Application and scope
- Rule 8.82. Definitions
- Rule 8.83. Public access
- Rule 8.84. Limitations and conditions
- Rule 8.85. Fees for copies of electronic records

These rules, adopted effective January 1, 2016, are intended to provide the public with reasonable access to appellate records that are maintained in electronic form while protecting privacy interests. (Rule 8.80(a).)

The rules on remote access to electronic appellate court records are not intended to give the public a right of access to any electronic record that they are not otherwise entitled to access in paper form, and do not create any right of access to records sealed by court order or confidential as a matter of law. (Rule 8.80(c).) These rules apply only to records of the Supreme Court and the Courts of Appeal and only to access to records by the public. They do not prescribe the access to court records by a party to an action or proceeding, by the attorney for a party, or by other persons or entities that may be entitled to such access by statute or rule. (Rules 8.81(a)–(b).)

3.2.3 General right of access; access to the extent feasible

Rule 8.83 provides that all electronic records must be made reasonably available to the public in some form, whether in electronic or paper form, except sealed or confidential records. (Rule 8.83(a).)

Under rule 8.83(b) to the extent feasible, appellate courts will provide, both remotely and at the courthouse, the following records provided they are not sealed or confidential:

- Dockets or registers of actions
- Calendars
- Opinions
- The following Supreme Court records:
    - Results from the most recent Supreme Court conference
    - Party briefs in cases argued in the Supreme Court in the preceding three years
    - Supreme Court minutes from at least the preceding three years

(Rule 8.83(b(1)).)

If an appellate court maintains records in electronic form in civil cases in addition to the records just listed, electronic access to these records must be provided both at the courthouse and remotely, to the extent feasible, except those records listed in section 3.2.4. (Rule 8.83(b)(2).)

3.2.4 Access by type of record

By rule, access to the electronic records listed below must be provided at the courthouse to the extent it is feasible to do so, but remote electronic access may not be provided to the following records:

- Any reporter's transcript for which the reporter is entitled to receive a fee; and

- Records other than those listed in rule 8.83(b)(1) in the following proceedings:

    - Proceedings under the Family Code, including proceedings for dissolution, legal separation, and nullity of marriage; child and spousal support proceedings; child custody proceedings; and domestic violence prevention proceedings;
    - Juvenile court proceedings;
    - Guardianship or conservatorship proceedings;
    - Mental health proceedings;
    - Criminal proceedings;
    - Civil harassment proceedings under Code of Civil Procedure section 527.6;
    - Workplace violence prevention proceedings under Code of Civil Procedure section 527.8;
    - Private postsecondary school violence prevention proceedings under Code of Civil Procedure section 527.85;

- Elder or dependent adult abuse prevention proceedings under Welfare and Institutions Code section 15657.03; and
- Proceedings to compromise the claims of a minor or a person with a disability

(Rule 8.83(c).)

3.2.5 Remote electronic access permitted in extraordinary cases

The appellate rules on remote access include a provision that allows the presiding justice, or a justice assigned by the presiding justice, to exercise discretion to permit remote access by the public to all or a portion of the public court records in an individual case if (1) the number of requests for access to documents is extraordinarily high and (2) responding to those requests would significantly burden the operations of the court. Unlike the comparable trial court records rule (see rule 2.503(c)) that is limited to extraordinary *criminal* cases, the appellate rule has no restriction on the type or types of cases to which it applies. (See rule 8.83(d).)

The appellate rule does provide: "An individual determination must be made in each case in which such remote access is provided." (Id.) It also provides guidance on the relevant factors to be considered in exercising the court's discretion to provide remote access, including "[t]he *privacy interests* of parties, victims, witnesses, and court personnel, and the ability of the court to redact *sensitive personal information*." (Rule 8.83(d)(1)(emphasis added).)

In addition, the rule provides a specific list of the information that must be redacted from the records to which the court allows remote access in extraordinary cases, including driver's license numbers; dates of birth; social security numbers; Criminal Identification and Information and National Crime Information numbers; addresses, e-mail addresses, and phone numbers of parties, victims, witnesses, and court personnel; medical or psychiatric information; financial information; account numbers; and other personal identifying information. (Rule 8.83(d)(2).)

3.2.6 Other limitations on remote access

Like the trial court rules, the appellate rules on remote access have certain additional safeguards that prevent remote access to court records from being used to thwart the privacy interests of individuals whose names appear in those records. Except for calendars, registers of action, and certain Supreme Court records, electronic access to records may be granted only if the record is identified by the number of the case, the caption of the case, the name of a party, the name of the attorney, or the date of oral argument, and only on a case-by-case basis. (Rule 8.83(e).) Also, bulk distribution is not permitted for most court records. (Rule 8.83(f).)

3.2.7 Retention of user access information

[To be added. This might cross-reference website policy.]

3.2.8 Preservation of data security in appellate court records

[To be added. This might cross-reference general sections on data security]

3.3 Remote access of parties and their attorneys to court records

[To be added to a subsequent version of the Resources Guide]

3.4 Remote access of justice partners to court records

[To be added to a subsequent version of the Resources Guide]

3.5 Remote access by other courts to a court's records

[To be added to a subsequent version of the Resources Guide]

3.6 Access to California Courts Protective Order Registry (CCPOR)

3.6.1 Access to form CLETS-001 through CCPOR

[To be added to a subsequent version of the Resources Guide]

3.7 Third-party storage

4. Financial Privacy in Civil and Criminal Cases

The constitutional right to privacy extends to one's personal financial information. (*Valley Bank of Nevada v. Superior Court* (1975) 15 Cal. 3d 652, 656).) In court proceedings, this right of financial privacy is often protected by a particular statute or rule, as illustrated by the examples below. However, the right of financial privacy is not unlimited in scope. As discussed in the example in section 4.4 below, a court has concluded that Family Code section 2014.6, the statute relied on by a participant in a divorce proceeding to close the records in that proceeding, was constitutionally overbroad. (See *In re Marriage of Burkle* (2006) 135 Cal. App.4th 1045, 1048.) Also, the Legislature has not made the Financial Privacy Act of 1977 applicable to the courts.

4.1 Fee Waivers

In civil cases, an application for an initial fee waiver, which contains personal financial information, is confidential. (Cal. Rules of Court, rule 3.54.) Only the court and authorized court personnel, persons authorized by the applicant, and persons authorized by order of the court may have access to the application. No person may reveal any information contained in the application except as authorized by law or order of the court. However, the order granting a fee waiver is not confidential.

4.2 Requests for Funds

In criminal cases, an indigent defendant requests for funds for payment of investigators, experts, and others to aid in presenting or preparing the defense in certain murder cases is confidential. This exemption applies to defendants in capital and life without parole murder cases under Penal Code section 190.05(a). (Pen. Code, § 987.9.)

4.3 Criminal Defendant's Statement of Assets

Defendant's Statement of Assets (form CR-115) is a mandatory Judicial Council form. It is confidential in the same manner as probation reports. (See Pen. Code, § 1202.4.)

4.4 Information about the Financial Assets and Liabilities of Parties to a Divorce Proceeding

In *In re Marriage of Burkle* (2006) 135 Cal. App.4th 1045, the court considered the constitutionality of Family Code section 2014.6 that requires a court, on the request of a party to a divorce proceeding, to seal any pleading that lists and provides the location or identifying information about the financial assets of the parties. The court concluded that section 2024.6 is unconstitutional on its face. The court stated: "While the privacy interests protected by section 2014.6 may override the First Amendment right of access in an appropriate case, the statute is not narrowly tailored to serve overriding privacy interests. Because less restrictive means exist to achieve the statutory objective, section 2014.6 operates as an undue burden on the First Amendment right of public access to court records." (*Id*. at page 1048.)

4.5 Information Privacy Act Not Applicable to the Courts

A general protection for individuals' privacy rights is contained in the Information Practices Act of 1977. However, recognizing the special role that courts play in conducting the people's business and the need for openness in conducting that business, the Legislature has expressly exempted the courts from the application of that Act. (See Civ. Code, §1798.3(b)(1) [excluding from the definition of "agency" covered by the Information Privacy Act of 1977 "[a]ny agency established under Article VI of the California Constitution"—that is, the courts]).

4.6 Privacy in the Payment of Fines and Fees

[To be added. Best practices consistent with Civil Code.]

4.6.1 Credit card information

4.6.1.1 Credit card information collected online

4.6.1.2 Credit card information collected at the counter

4.6.2 Retention of credit card information

4.6.3 Legal restrictions on credit card information

4.6.4 Use of vendors to collect fines and fees

4.7 Taxpayer Information

4.7.1 Confidential statements of taxpayer's Social Security Numbers

Confidential Statements of Taxpayer's Social Security Number on mandatory Judicial Council forms (forms WG-021 and WG-025) for use in connection with wage garnishments are confidential.

4.7.2 Income tax returns in child support cases

In a proceeding involving child, family, or spousal support, if a judge finds that a tax return is relevant to disposition of the case, the tax return must be sealed and maintained as a confidential record of the court. (Fam. Code, § 3552.)

5. Privacy in Judicial Administrative Records

5.1 Public access to judicial administrative records (rule 10.500)

Rule 10.500 provides for public access to "judicial administrative records" (Rule 10.500(c)(2)), which includes records of budget and management information related to the administration of the courts.

5.1.1 Policy

The rule is based on the California Public Records Act ("CPRA") (Government Code section 6250 et seq.) and is intended to be broadly construed to further the public's right of access. Unless otherwise indicated, the terms used in this rule have the same meaning as under the Legislative Open Records Act (Gov. Code, § 9070 et seq.) and the California Public Records Act (Gov. Code, § 6250 et seq.) and must be interpreted consistently with the interpretation applied to the terms under those acts.

5.1.2 Scope of access

Rule 10.500 covers only judicial administrative records and does not govern the public's right to access "adjudicative records," which are "writings" prepared, used, or filed in a court proceeding, relate to judicial deliberation, or the assignment or reassignment of cases of justices, judges, subordinate judicial officers, and the assignment or appointment of counsel by the court. (Rule 10.500(c)(1).) As discussed above, adjudicative records, or court records, are presumptively public, subject to exceptions as discussed in Sections 2-3 above.

Disclosable judicial administrative records include any non-adjudicative records (writings) containing information that relates to "the conduct of the people's business that is prepared, owned, used, or retained by a court, regardless of the writing's physical form or characteristics." (Rule 10.500(c)(2).) However, personal information that is not related to the conduct of the people's business—or material falling under a statutory exemption (see below) —is not

disclosable and can be redacted from the public records that are produced or presented for review. (See *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608.) This limitation on disclosure protects the privacy rights of government employees involved in creating public records.

Even if electronic communications are conducted on an agency employee or official's personal device or personal email account, they are disclosable if they pertain to the people's business and are prepared, owned, used, or retained by a court or its personnel. (See Rule 10.500(b)(5); *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608.) On the other hand, if the documents relate to purely personal information, that content is not disclosable. Pursuant to a 10.500 request, courts may ask their employees to search their own files, segregate public records from personal records, and submit an affidavit with sufficient factual basis for determining whether the contested item are public records or personal materials. (*Id.*)

5.1.3 Exemptions and waiver of exemptions

Rule 10.500(f) provides 12 categories of records that a court may exempt from disclosure. For the purpose of this Resource Guide, the most important of these categories is the exemption for personnel, medical, or similar files, or other personal information whose disclosure would constitute an unwarranted invasion of personal privacy. (Rule 10.500(f)(3).) Some of the other exempt categories include records that relate to pending or anticipated claims or litigation to which a judicial branch entity or its personnel are parties (Rule 10.500(f)(2)); disclosure that is exempt or prohibited under state or federal law, including under the California Evidence Code relating to privilege or by court order in a court proceeding (Rule 10.500(f)(5); records that would reveal or compromise court security or safety of court personnel (Rule 10.500(f)(6)); trade secrets, or confidential commercial or financial information (Rule 10.500(f)(10) and the catch-all exemption where, on the facts of a specific request, the public interest in withholding the record clearly outweighs the public interest in disclosure. (Rule 10.500(f)(12).)

A judicial branch entity's or judicial branch personnel's disclosure of a judicial administrative record that is exempt from disclosure pursuant to rule 10.500(f) or law waives the exemptions as to that specific record. (Rule 10.500(h).) However, waiver does not apply to disclosures made in certain contexts as discussed in rule 10.500(h).

5.2 Criminal History Information

Summaries of criminal history information (criminal history information rap sheets) are confidential. (*Westbrook v. Los Angeles* (1994) 27 Cal.App.4th 157, 164; Pen. Code, §§ 11105 and 13300–13326.) Public officials have a duty to preserve the confidentiality of a defendant's criminal history. (*Craig v. Municipal Court* (1979) 100 Cal.App.3d 69, 76.) Unauthorized disclosure of criminal history violates a defendant's privacy rights under the California Constitution. *(Ibid.)* Courts have upheld the confidentiality assigned to criminal history records. (See, e.g., *Westbrook v. Los Angeles* (1994) 27 Cal.App.4th 157 [unauthorized private company was denied access to municipal court information computer system].)

6. Privacy of Witnesses, Jurors, and Other Non-parties

6.1 Witness and Victim Information

6.1.1 Confidential information about witnesses and victims in police, arrest, and investigative reports

The court and the district attorney shall establish a mutually agreeable procedure to protect the confidential information of any witness or victim contained in police reports submitted to the court in support of a complaint, indictment, information, search warrant or arrest warrant. (Pen. Code, § 964.)

6.1.2 Victim impact statements

Victim impact statements filed with the court must remain under seal until imposition of judgment and sentence, except that the court, the probation officer, and counsel for the parties may review such statements up to two days before the date set for imposition of judgment and sentence. (Pen. Code, § 1191.15(b).) Victim impact statements shall not be otherwise reproduced in any manner. (Pen. Code, § 1191.15(c).)

6.1.3 Information about victims, witnesses, and others

Law enforcement agencies are prohibited from disclosing the address and phone number of a witness or victim, or an arrestee or potential defendant. (Pen. Code, § 841.5.) Similarly, defense counsel may not disclose the address or telephone number of a victim or witness to the defendant or his or her family. (Penal Code, § section 1054.2.) If this information is contained in documents filed with the courts, it should be redacted before the documents are filed.

6.1.4 Identity of sex offense victims

At the request of a victim of an alleged sexual offense, the court may order that the victim be treated anonymously. Upon a proper showing, the judge may order the identity of the victim in all records and during all proceedings to be either "Jane Doe" or "John Doe" if the judge finds that such an order is reasonably necessary to protect the alleged victim's privacy and that such measures will not unduly prejudice the prosecution or defense. (Pen. Code, § 293.5.)

6.2 Juror Information

6.2.1 Juror questionnaires of those jurors not called

The questionnaires of jurors not called to the jury box for voir dire are not open to the public. (*Copley Press, Inc. v. Superior Court* (1991) 228 Cal.App.3d 77, 87–88); but cf. *Bellas v. Superior Court of Alameda County* (2000) 85 Cal.App.4th 636, 645, fn. 6 [suggesting a contrary rule].)

6.2.2 Juror questionnaires answered under advisement of confidentiality

These records are not open to the public. (*Pantos v. City and County of San Francisco* (1984) 151 Cal.App.3d 258, 493-494 [jurors were told their answers on questionnaire were confidential].)

6.2.3 Sealed juror records in criminal courts

After the jury reaches a verdict in a criminal case, the court's record of personal juror identifying information (including names, addresses, and telephone numbers) must be sealed. (Code Civ. Proc., § 237(a)(2).) This is often accomplished by replacing juror names with numbers. Indeed, that is how appellate court records contain the relevant information while conforming to the requirements of Code of Civil Procedure section 237. The defendant or his or her counsel can petition the court for access to this information to aid in developing a motion for a new trial or for any other lawful purpose. (Code Civ. Proc., § 206(f).)

6.2.4 Records of grand jury proceedings

These records are not open to the public unless an indictment is returned. If an indictment is returned, records of the grand jury proceeding are not open to the public until 10 days after a copy of the indictment has been delivered to the defendant or his or her attorney. (Pen. Code, § 938.1(b); *Daily Journal Corp. v. Superior Court* (1999) 20 Cal.4th 1117, 1124–1135.) If there is a "reasonable likelihood" that release of all or part of the transcript would prejudice the accused's right to a fair trial, a judge may seal the records. (Pen. Code, §§ 938.1, 929; see *Rosato v. Superior Court* (1975) 51 Cal.App.3d 190.) Notwithstanding the confidential status of a record, in civil grand juries, a judge may order disclosure of certain evidentiary materials, as long as information identifying any person who provided information to the grand jury is removed. (Pen. Code, § 929.) Also, after an indictment is returned, the judge may order disclosure of nontestimonial portions of the grand jury proceedings to aid preparation of a motion to dismiss the indictment. (*People v. Superior Court (Mouchaourab)* (2000) 78 Cal.App.4th 403, 434–436.)

6.2.5 Courts' inherent power to protect jurors

Courts may exercise their discretion to seal juror records where a "compelling interest" exists, such as protecting jurors' safety or privacy, protecting litigants' rights, or protecting the public from injury. (*Pantos v. City and County of San Francisco* (1984) 151 Cal.App.3d 258, 262; Code Civ. Proc., § 237; see *Townsel v. Superior Court* (1999) 20 Cal.4th 1084, 1091.) Thus any juror information that a judge orders sealed is not open to the public.

6.3 Attorney information

6.4 Vexatious litigant list

7. Privacy Protection for Judicial Officers

7.1 Privacy Protection Guidance for Judicial Officers

Government Code section 6254.21 prohibits persons or businesses from publicly posting or displaying on the Internet the home address and phone number of a judicial officer, if he or she has made a written demand of that person or business not to disclose that information. Upon request of a California trial court judge, commissioner, or referee, the Judicial Privacy Protection

Program of the Judicial Council's Security Operations unit will make such written demand to a predetermined list of major online data vendors. (See Appendix__ for attached form authorizing the Judicial Council to make written demand on behalf of a trial court judge, commissioner, or referee.) For further information, contact *securityoperations@jud.ca.gov*.

8. Privacy and the Electronic Court: Best Practices

8.1 Electronic Filing and Service, and Access to Protected Private Information

8.1.1 Electronic identification and verification

[Text to be added] (For possible SRL principles, see http://www.srln.org/system/files/attachments/LSC%20Best%20Practices%20in%20E-Filing.pdf**]**

8.1.2 E-filing directly with the court

8.1.3 E-filing through EFSPs and vendors

8.1.4 E-service lists and other information

8.2 Protected Personal Information Held in Cloud-based Storage Systems

8.3 Case and Document Management Systems

8.3.1 Vendor-serviced CMS/DMS

8.3.2 Metadata

9. Privacy and Court-related Services: Best Practices

9.1 California Court Self-help Centers

9.2 Family Law Facilitator Offices

9.3 Family Court Services

9.4 Civil Court-ordered Mediation Services

9.5 Document Assembly Programs

10. Privacy and Data Exchanges with Justice Partners

10.1 Data Exchanges with Local Justice Partners

10.2 Data Exchanges with State Justice Partners

10.3 Data Exchanges with Federal Justice Partners

10.4 Inter-state Data Exchanges

10.5 Intra-branch Data Exchanges

10.6 CCPOR

10.7 Data Exchange of Juvenile Delinquency Information

11. Court Websites: Best Practices

California courts use public websites extensively to conduct their business. All the trial and appellate courts have websites. These websites perform essential services. For example, they provide the public with key information about the courts. They provide access to local rules and forms needed to carry on cases. They provide litigants with information about hearing dates and other calendar information. And they provide information to jurors about when and where to appear. Recently, websites have also become an increasingly important means for transacting business, such as paying for traffic tickets or scheduling hearings.

11.1 Privacy Statements

Like other institutions employing websites, courts need to advise the public and other users of the court's privacy policies with regard to the use of their websites. Court need to inform users about the information that is collected. A privacy statement on the website will explain how the court gathers information, how it uses it, and how the court will protect users' privacy.

Each court will develop its own Privacy Statement relating to its website. For courts to consider as they develop or revise their statements, a Model Privacy Statement is attached as Appendix __. In addition, a Model Terms of Use is attached as Appendix _.

11.2 Retention and Tracking of User Information and Data

11.2.1 Use of cookies on court websites

11.2.2 Self-help center portals

12. Video and Surveillance: Best Practices

12.1 Photographing, Recording, and Broadcasting in Court

California Rules of Court, rule 1.150 permits photographing, recording, and broadcasting of courtroom proceedings pursuant to a judge's ruling on media requests and sets forth factors to be considered by a judge in determining whether to grant media requests for such activity. A judge may not permit media coverage of proceedings held in chambers; proceedings closed to the public; jury selection; jurors or spectators; or conferences between an attorney and a client, witness, or aide; between attorneys; or between counsel and the judge at the bench. (Rule 1.150(e)(6).)

12.2 Video Remote Interpreting

12.3 Security Cameras in Public Areas

The Judicial Council has recommended best practices and policies for security camera recordings in the courthouse, covering the retention schedule, downloading, disclosures to the public or other parties; and retention schedules for downloaded recordings. (See Fact Sheet: Recommendations on Security Camera Recordings Policy and Best Practices (Oct. 2015).) Further questions may be directed to Ed Ellestad, Supervisor, Judicial Council Security Operations.

13. Privacy and Information Security: Best Practices

13.1 Information Systems Controls Framework Template

13.2 How to Use the Information Systems Control Framework

14. Responding to Data Breaches: Best Practices

14.1 Developing an incident response plan

14.2 Noticing affected persons

[Note: Review Civil Code 1798.92 governing business security breach notices]

14.2.1 Contents of notice

14.2.2 Means of providing notice

14.3 Contacting Law Enforcement

14.4 Contacting credit reporting agencies

15. Court Management of Protected Private Information: Best Practices

[[To be added. Best practices following Civil Code section 1798 et seq.]]

15.1 Developing a Local Court Privacy Guide

15.2 Establishing Local Privacy Procedures and Systems

15.3 Identifying Key Court Personnel

15.4 Training Court Staff

15.5 Periodic Review of Privacy Procedures and Systems

Appendices

Appendix A: List of relevant statutes and rules
Appendix B: Model local court privacy guide
Appendix C: Sample privacy statement for court websites
Appendix D: Sample terms of use for court websites
Appendix E: Sample notice of data breach