

ATTACHMENT*

RULES OF THE SUPREME COURT

* * *

Rule 123. Public Access to the Judicial Records of the State of Arizona

(a) [No change in text.]

(b) Definitions.

(1) Bulk Data. As used in this rule “Bulk Data” means all, or a significant subset, of the non-confidential case data maintained in a court case management system, either with or without modification or customized compilation.

(2) Closed or Confidential (Records). “Closed” or “Confidential,” when used in this rule in reference to records, means that members of the public may not inspect, obtain copies of, or otherwise have access to such records unless authorized by law.

~~(2)~~(3) Commercial Purpose. [No change in text.]

~~(3)~~(4) Court. [No change in text.]

~~(4)~~(5) Court Administrator or Clerk of the Court. [No change in text.]

~~(5)~~(6) Criminal History Record Information (CHRI). [No change in text.]

~~(6)~~(7) Custodian. [No change in text.]

(8) Custodian of Bulk Data. In a superior court or appellate court, “Custodian of Bulk Data” means, depending on local practice, either the clerk of court or the presiding judge. In a justice of the peace or municipal court, the custodian is the sitting justice of the peace and the presiding judge of the municipal court, respectively.

(9) Dissemination Contract and Disclaimer. “Dissemination Contract and Disclaimer” means a contract between a custodian of court records and a person or entity requesting bulk data.

~~(7)~~(10) Information. [No change in text.]

* Changes or additions in text are indicated by underlining and deletions from text are indicated by ~~strikeouts~~.

~~(8)-(11)~~ *Judge*. [No change in text.]

~~(9)-(12)~~ *Law*. [No change in text.]

~~(10)-(13)~~ *Presiding Judge*. [No change in text.]

~~(11)-(14)~~ *Public*. [No change in text.]

(15) *Public Purpose Organization*. “Public Purpose Organization” means a private organization that serves a public purpose, such as criminal justice, child welfare, licensing, mental health treatment, or that engages in research for scholarly, journalistic, or governmental purpose.

~~(12)-(16)~~ *Record*. [No change in text.]

(A) *Administrative Record*. [No change in text.]

~~(B) *Case Record*. “Case record” means any record pertaining to a particular case or controversy.~~

(B) *Case Record*. “Case Record” means:

(1) any record that is collected, received, or maintained by a court or clerk of court in connection with a judicial proceeding;

(2) any order, judgment, or minute entry that is related to a judicial proceeding; and

(3) any index, calendar, docket, or register of actions associated with a case or in connection with a judicial proceeding.

(17) *Remote Electronic Access*. “Remote Electronic Access” means access by electronic means that permits the viewer to search, inspect, or copy a record without the need to physically visit a court facility.

(18) *Sensitive Data*. “Sensitive Data” means social security number, bank account number, credit card number, and any other financial account number.

(c) General Provisions.

(1) [No change in text.]

(2) *Creation, Production and Management of Records*.

(A) Court personnel, who generate or receive paper or electronic records known or marked as containing confidential information, shall identify and segregate the

confidential information from the public record whenever practicable.

(B)-(C) [No change in text.]

(3)-(4) [No change in text.]

(5) *Judicial Officers and Employees.* Arizona judicial officers, clerks, administrators, professionals or other staff employed by or working under the supervision of the court shall have such access as needed to carry out their assigned duties and as directed by their supervisor.

(6) *Employees of Government Agencies and Private Organizations.* Employees of federal, state, tribal, and local government agencies and political subdivisions, and private organizations, the objective of which is to serve a public purpose, such as criminal justice, child welfare, licensing, mental health treatment, or research for scholarly, journalistic, or governmental purposes, may be granted such access to court records as required to serve that purpose according to this rule or as provided by any supplemental supreme court policies or court order.

(7) *Access To Bulk Data.* Persons who execute a dissemination contract and disclaimer containing provisions specified by the supreme court may have such access as permitted by paragraph (j) of this rule.

(d) Access to Case Records.

All case records are open to the public except as may be closed by law, or as provided in this rule. Upon closing any record the court shall state the reason for the action, including a reference to any statute, case, rule or administrative order relied upon.

(1) *Juvenile Delinquency Proceedings Records.*

(A)-(B) [No change in text]

(C) All information and records obtained in the course of evaluation, examination or treatment of juveniles who have been referred to a treatment program funded by the juvenile probation fund (pursuant to ~~ARS § 8-230.01, or renumbered as~~ ARS § 8-321, ~~effective June 30, 1998~~) or the family counseling fund (ARS § 8-261 et seq.) are confidential and shall not be released unless authorized by rule or court order. These records include, but are not limited to, clinical records, medical reports, laboratory statements and reports, or any report relating to diagnostic findings and treatment of juveniles, or any information by which the juvenile or his family may be identified, wherever such records are maintained by the court.

(2)-(4) [No change in text.]

(e) Access to Administrative Records.

All administrative records are open to the public except as provided herein:

(1)-(6) [No change in text.]

(7) *Library Patron Records.* Records maintained in any court law library, clerk's office or court that ~~which~~ link a patron's name with materials requested or borrowed by the patron, or ~~that which~~ link a patron's name with a specific subject about which the patron has requested information or materials are closed. This provision shall not preclude a library, clerk's office or court from requiring that the request specify any commercial use intended for the records as provided in paragraph (f) of this rule.

(8) *Remote Electronic Access User Records.* Data or information that would disclose that a user of a remote electronic access system has accessed a particular court record is closed. Record access information shall be accessible by the public only on a showing of good cause pursuant to the process set forth in paragraph (f) of this rule.

~~(8)-(9)~~ *Attorney and Judicial Work Product.*

(A)-(B) [No change in text.]

~~(9)-(10)~~ *Juror Records.* [No change in text.]

~~(10)-(11)~~ *Proprietary and Licensed Material.* [No change in text.]

~~(11)-(12)~~ *Copyrighted Documents and Materials.* Documents and materials produced and copyrighted by the court are ~~public records that~~ open to public inspection but may not be re-published without proper authorization from the court.

(13) *Judicial Branch Training Materials and Records.* Evaluation materials and records generated by participants in judicial education programs such as test scores, educational assessments, practical exercise worksheets, and similar materials are closed.

(14) *Certification Records.* Proprietary materials required to be submitted to the Supreme Court by applicants for certification or licensing are closed. Applicants for certification or licensure shall be responsible for clearly identifying any material they consider to be proprietary at the time the material is submitted.

(f) Access to Records in Paper Medium.

(1)-(4) [No change in text.]

(5) *Review of Denials to Access Records.*

(A) Any applicant who is denied ~~the right to inspect, receive copies or access any~~

~~record~~ access to or copies of any record, bulk data, or compiled data pursuant to the authority of this rule, shall be entitled to an administrative review of that decision by the presiding judge. The request for review must be filed in writing with the custodian who denied the request within 10 business days of a denial made under Paragraph (f)(4) above. The custodian shall forward the request for review, a statement of the reason for denial, and all relevant documentation to the presiding judge or a designee within 3-5 business days of receipt of the request for review. The presiding judge or designee shall issue a decision as soon as practicable considering the nature of the request and the needs of the applicant, but not more than 10 business days from the date the written request for review was received.

(B) Any party aggrieved by the decision of the presiding judge or designee may seek review by filing a special action ~~in the Court of Appeals~~ pursuant to the Rules of Procedure for Special Actions. If the decision challenged by the special action was issued by a judge of the superior court or court of appeals, the special action shall be filed in the court of appeals. If the decision was issued by a supreme court justice, the special action shall be filed in the supreme court.

(g) Remote Electronic Access to Case Records.

(1) A court may provide remote electronic access to case records as follows:

(A) Parties, Attorneys, and Arbitrators. Parties, attorneys, and arbitrators may be provided remote electronic access, upon registering, to case records which are not sealed in all case types in which the person is an attorney of record, arbitrator, or named party, including an individual, partnership, corporation, association, or public or private organization. An attorney of record on the staff of a public or private law firm may extend access to any other attorney or person working for or on behalf of that public or private law firm, upon the other attorney's or person's registration.

(B) Governmental Entities and Public Purpose Organizations. Any federal, state, tribal, or local governmental entity or public purpose organization may be provided remote electronic access to any case records necessary to carry out a particular governmental or public purpose responsibility. The terms of such access shall be set forth in a memorandum of understanding between the entity or organization and the custodian that includes provisions for safeguarding the confidentiality of any closed records.

(C) General Public, Registered Users.

(i) Members of the public who hold an Arizona driver license or nonoperating identification license may be provided remote electronic access, upon registering and paying any established fee, to all of the following

categories of case records unless sealed or otherwise made confidential by rule or law:

(a) Civil case records in any action brought to enforce, redress, or protect a private or civil right but not:

- Juvenile dependency and delinquency or other matters brought under ARS Title 8;
- Family law, paternity, or other matters arising out of ARS Title 25;
- Orders of protection, injunctions against harassment and all proceedings, judgments or decrees related to the establishment, modification or enforcement of such orders, including contempt; or
- Probate proceedings brought under ARS Titles 14 and 36.

(b) Civil traffic case records in any action brought as such under ARS Titles 28 or 41 or a matter expressly designated as a civil traffic violation by a traffic ordinance of a city or town, and any boating violation punishable by a civil sanction under ARS Title 5, chapter 3, articles 1 through 11, or a non-traffic ordinance expressly designated a civil violation or a boating ordinance by a city or town.

(c) Criminal case records in any action instituted by the government to punish offenses classified as a misdemeanor or felony brought pursuant to ARS Titles 4, 13, 28, or local ordinance and case records in any action instituted to punish petty offenses classified by ARS § 13-601.

(d) Case records in any action instituted by a county to enforce an ordinance that provides for criminal and civil penalties pursuant to ARS §§ 11-251 and 11-808.

(ii) The following documents shall not be accessible by remote electronic access to users registered under paragraph (g)(1)(C) due to the inability to protect sensitive data that is likely to be contained within these documents:

(a) booking-related documents;

(b) warrants, including search warrants, confidential wiretaps, pen registers, handwriting exemplars, trap and trace, and bench warrants;

(c) charging documents, including criminal and civil traffic charging documents;

(d) pre-sentence reports;

(e) defendant's financial statement;

(f) disposition report;

(g) transcripts; and

(h) all documents in criminal cases in which a juvenile is alleged to be the victim of any offense listed in ARS Title 13, chapters 14 or 35.1. The prosecuting agency, upon filing a charging document described in this paragraph, shall advise the clerk that the case is subject to this provision.

(i) the probate information form required to be filed pursuant to Rule 6, Arizona Rules of Probate Procedure.

Upon motion by a party, by any person, or upon the court's own motion, and for good cause shown, the court in which such action is pending may issue an order to allow remote electronic access to members of the public, as provided in paragraph (g)(1)(C), to any case in which a juvenile is alleged to be the victim under paragraph (g)(1)(C)(ii)(h). The order may include any appropriate provision required to protect the juvenile from embarrassment or oppression. The burden of showing good cause for an order shall remain with the person seeking remote electronic access to the case record. Irrespective of an order limiting electronic access under this paragraph, the clerk shall provide non-registered users remote electronic access as set forth in paragraph (D)(ii) herein when the court generally provides such non-registered user access in other cases.

(D) General Public, Non-Registered Users. Unless otherwise provided by rule or law, members of the public may be provided remote electronic access, without registering, to:

(i) the following data elements in closed cases, including juvenile delinquency, mental health, probate, and criminal cases in which a juvenile is alleged to be the victim, as identified in paragraph (g)(1)(C)(ii)(h) above:

- party names,
- case number,
- judicial assignment, and
- attorney names

(ii) individual case information extracted from a case management system in all civil, criminal, and civil traffic cases identified in paragraphs (g)(1)(C)(i)(a) through (d), and family law cases, including a list of documents filed, events, dates, calendars, party names, month and year of birth, residential city, state and zip code, case number, judicial assignment, attorneys, charges filed or claims made, interim rulings, and case outcomes, including sentence, fines, payment history, minute entries, and notices.

(iii) court of appeals and supreme court opinions and decisions in all case types, except that any appendix in criminal cases in which a juvenile is alleged to be the victim, as identified in paragraph (g)(1)(C)(ii)(h) above, shall not be provided by remote electronic access.

(2) Registration and fees. The registration process and fees for remote electronic access to case records shall be established by the Supreme Court upon the recommendation of the Arizona Judicial Council, and shall be an amount as reasonable as possible to develop, implement, maintain, and enhance the remote electronic access to case records system. All information provided by a potential user for registration purposes shall be closed. Remote access provided pursuant to paragraph (g)(1)(B) shall not require registration or payment of any fees.

(3) Courts and clerks of court shall not display case records online except as provided herein, as provided by ARS § 12-283(I), or as ordered by the court in a particular case. Any remote electronic access shall be conditioned upon the user's agreement to access the information only as instructed by the court, not to attempt any unauthorized access, and to consent to monitoring by the court of all use of the system. The court will also notify users that it will not be liable for inaccurate or untimely information, or for misinterpretation or misuse of the data. Such agreement and notices shall be provided to the users in any manner the court deems appropriate. The court may deny access to users for failure to comply with such requirements. The court or clerk of court that establishes remote electronic access to case records may also establish limitations on remote electronic access based on the needs of the court, limitations on technology and equipment, staff resources and funding.

(4) Courts and clerks of court must clearly and prominently display current charge dispositions for any case that the court or clerk of court makes publicly available online.

(5) Removing case records from online access.

(A) Courts or clerks of court may remove case management system data and case records from online display once the applicable records retention schedule period is met.

(B) For cases scheduled to be retained more than 25 years, courts or clerks of court may remove case management system data and case records from online display after 25 years, provided the data and records are then retained through an electronically preserved method. In place of the records, the court or clerk of court shall display a notice online which directs the viewer to contact the court or clerk for access to the case record.

(6) The clerk of the court, court, court agency, or their employees shall be immune from suit for any conduct relating to the electronic posting of case documents in accordance with this rule.

(7) Data or information that would disclose that a user of a remote electronic access system has accessed a particular court record is closed. Record access information shall be accessible by the public only on a showing of good cause pursuant to the process set forth in paragraph (f) of this rule.

(8) This paragraph (g) shall not limit the public's right of access to records at a court designated facility, whether in paper or electronic format.

(g)-(h) Access to Audiotape, Videotape, Microfilm, Computer or Electronic Based Records.

(1)-(2) [No change in text.]

(3) *Cost to Obtain Copies.*

(A) [No change in text.]

(B) Unless otherwise prescribed by law relating to the collection and deposit of fees by the custodian, the custodian may retain the fees collected pursuant to paragraph ~~(g)~~~~(h)~~(3)(A) to compensate for the expenses related to reproduction of electronic records.

(4) [No change in text.]

~~(5) Remote Electronic Access to Records and Cost.~~

~~(A) Pursuant to the provisions of this paragraph, every presiding judge may authorize on-line, remote electronic access to both case and administrative records in their respective courts. Fees may be charged for the value added and custom-remote electronic access service as authorized by ARS §§ 12-119.02, 12-120.31, 22-281.01, 22-404.01 and 12-284.02. The fees shall be based on the recovery of costs incurred in the provision of remote electronic access, including the cost of providing a general public access information system, but shall not exceed the applicable statutory limits. For the supreme court, court of appeals and superior~~

~~court records, the fees shall be paid to the clerk of each respective court. For justice and municipal court records, the fees shall be paid to an appropriate official designated by the court. The presiding judge of the superior court will consult with the local funding authority before any municipal court fee is imposed.~~

~~(B) Prior to establishing value added remote electronic access for which fees are charged, each court shall establish a remote electronic access information system that, subject to available funding, will be available to the general public without additional court fees. At a minimum, both the public remote electronic access system and the value added remote electronic access shall permit access to information by case number, party name and counsel name, if maintained electronically. Both systems shall contain the same case data elements. Any difference between the two systems shall be limited to providing enhanced services in the value added remote electronic access, such as guaranteed response times and service levels, search and reporting tools, help desk services, etc. Courts are encouraged to make data elements available to both systems at the same time. If a court chooses to make additional data elements available in the value added remote electronic access system first, the same data elements must be made available in the public remote electronic access system within six months.~~

~~(C) Additional policies and procedures for remote electronic access to court records shall be adopted when necessary by the supreme court through subsequent rules or separate administrative orders after considering applicable comments and recommendations, including those of the court's Commission on Technology and the Arizona Judicial Council.~~

~~(D) Any on-line electronic access shall be conditioned upon the user's agreement to access the information only as instructed by the court, to not attempt any unauthorized access, and to consent to monitoring by the court of all use of the system. The court will also notify users that it will not be liable for inaccurate or untimely information, or for misinterpretation or misuse of the data. Such agreement and notices shall be provided to the users in any manner the court deems appropriate. The court may deny access to users for failure to comply with such requirements.~~

~~(E) For value added or custom remote electronic access, each court will utilize a published standard fee schedule or written contracts with each subscriber. The fee schedule or contract shall set forth the services and service levels to be provided, the fee structure, manner of billing, payment requirements, and grounds for termination of the service. The state of Arizona, its county and municipal governments and agencies shall be exempt from such fees.~~

~~(F) The presiding judge of each court may establish limitations on remote electronic access based on the needs of the court, limitations on technology and equipment, staff resources and funding.~~

~~(G) All courts and clerks of court shall employ appropriate security measures, procedures, devices and software to protect assets and records and to prevent unauthorized access.~~

~~(J) Communication protocols shall be adopted that are consistent with standards adopted for the Arizona Judicial Information Network (AJIN) as reflected in Supreme Court Administrative Order 95-37. Free public remote electronic access shall, at a minimum, be available by means of standard telenet or an industry-standard hypertext mark up language (HTML) browser. By December 31, 1999, a single non-proprietary, open systems communications protocol for value added and custom remote electronic access shall be determined by the Commission on Technology. By January 30, 2004, all courts shall comply with and use the communication protocols and standards adopted for remote electronic access by the Commission on Technology.~~

(5) Correcting Data Errors; Administrative Review.

(A) Data entry inaccuracies in court calendars, case indexes, or case dockets in a court's case management system may be corrected at any time by the custodian of the record on the custodian's own initiative or on request of an individual as provided in paragraph (h)(5). Clerical errors in judgments, orders, or other parts of the record may be corrected as provided by the applicable rules of procedure.

(B) An individual seeking to correct a data error or omission in an electronic case record shall be entitled to apply for relief with the court in which the original record was filed. The individual shall submit the request to correct the error to the clerk of the court, if any, or to the justice of the peace or municipal court judge. If the custodian to whom the request was submitted determines that the data entry is inaccurate, the custodian shall correct the error as soon as practicable.

(C) If the request is denied by the clerk of an appellate court, the individual may apply for administrative review of the denial by the designated appellate judge or justice. If the request is denied by the clerk of a superior court or by a justice of the peace or municipal court judge, the individual may apply for administrative review of the denial by the presiding superior court judge. The request for administrative review must be filed in writing with the custodian who denied the request within 10 business days of issuance of a denial. The custodian shall forward the request for review, a statement of the reason for denial and all relevant documentation to the presiding or designated judge or justice within 5 business days of the request for

review. The presiding or designated judge or justice shall issue a decision as soon as practicable considering the nature of the request and the needs of the applicant, but not later than 10 business days from the date the written request for review was received by the custodian. If the decision of the presiding or designated judge or justice is that the data entry is inaccurate, the custodian shall correct the error as soon as practicable.

(D) Any party aggrieved by the decision of the judge or justice may seek review by filing a special action pursuant to the Rules of Procedure for Special Actions. If the decision challenged by the special action was issued by a judge of the superior court or court of appeals, the special action shall be filed in the court of appeals. If the decision was issued by a supreme court justice, the special action shall be filed in the supreme court.

~~(h)~~ **(i) Inspection and Photocopying.** [No change in text.]

(j) Bulk or Compiled Data Dissemination in Bulk.

(1) Requests for bulk or compiled court data.

(A) A custodian may release bulk data to an individual, a private company, or a public organization under this policy. Before releasing bulk data, a custodian shall require the recipient to execute a dissemination contract and disclaimer containing provisions specified by the supreme court.

(B) A custodian may contract with a private company or public organization to provide specialized reports to those requesting them.

(2) Denying requests for bulk data. The custodian may deny a request for bulk data in compliance with paragraphs (c), (f)(4), and (h)(4)(A).

(3) Personal identifiers available in bulk court data. The custodian of bulk data may release data that contains the following personal identifying information about a petitioner, plaintiff, respondent, or defendant other than a petitioner seeking an order of protection:

(A) name,

(B) address,

(C) date of birth, and

(D) last four digits of the social security or driver license number.

(4) Dissemination of bulk or compiled data is not permitted except as provided in this

rule or as permitted by court order.

* * *

[2009] Court Comment to Paragraph (h)(5)

This provision is intended to allow individuals to seek correction of data entry errors appearing in case management system data likely to be displayed online or disseminated in bulk or compiled fashion. The process for correcting errors appearing in judgments, orders, and other parts of the record is governed by current rules, including Rule 60, Rules of Civil Procedure, Rule 24.4, Rules of Criminal Procedure, and Rule 85, Rules of Family Law Procedure.

ARIZONA RULES OF CRIMINAL PROCEDURE

* * *

Rule 2.3. Content of complaint

a. A complaint is a written statement of the essential facts constituting a public offense, that is either signed by a prosecutor, or made upon oath before a magistrate, or made in accordance with A.R.S. § 13-3903.

b. Upon filing a charging document in a criminal case in which a juvenile is alleged to be the victim of any offense listed in A.R.S Title 13, chapters 14 or 35.1, the prosecuting agency shall advise the clerk that the case is subject to the provisions of Supreme Court Rule 123(g)(1)(C)(ii)(h).

* * *

ARIZONA RULES OF CIVIL PROCEDURE

* * *

Rule 5. Service and filing of pleadings and other papers

* * *

Rule 5(f). ~~Vacated~~ Sensitive Data

(1) A person making a filing with the court shall refrain from including the following sensitive data in all pleadings or other documents filed with the court, including exhibits thereto, whether filed electronically or in paper, unless otherwise ordered by the court or as otherwise provided by law:

(A) Social Security Numbers. If an individual's social security number must be included in a pleading or other document, only the last four digits of that number shall be used.

(B) Financial Account Numbers. If financial account records are relevant or set forth in a pleading or other document, only the last four digits of these numbers shall be used.

(2) The responsibility for redacting sensitive data shall rest solely with a person making a filing with the court. The clerk of the court or the court is not required to review documents for compliance with this rule, seal documents that contain sensitive data on the clerk's own initiative, or redact pleadings or other documents. However, if a document is subject to availability by remote electronic access pursuant to Rule 123, Rules of the Supreme Court of Arizona, any party or their attorney may request that the court order, or the court on its own initiative may order, that the document be sealed and/or replaced with an identical document with the sensitive data redacted or removed.

(3) For violation of this rule, the court may impose sanctions against counsel or the parties to ensure future compliance with this rule.