

## RULES OF JUDICIAL ADMINISTRATION

### RULE 14. SENSITIVE DATA IN COURT CASE RECORDS

**14.1 Defined.** The following data is sensitive:

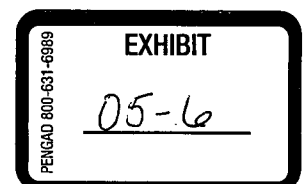
- (a) social security numbers;
- (b) bank account, credit card, or other financial account numbers;
- (c) driver's license numbers, passport numbers, and similar government-issued personal identification card numbers;
- (d) date of birth, except the date of birth of a defendant in a criminal matter;
- (e) the address and phone number of a person who is a crime victim, as defined by Article 56.32, Code of Criminal Procedure, in the proceeding in which the case record is filed or a related proceeding; and
- (f) the name and address of a minor child.

### 14.2 Duty of Parties.

- (a) Sensitive data must not be filed or included in a case record, as defined by Rule of Judicial Administration 15.2, except in a separately filed Sensitive Data Form approved by the Supreme Court of Texas and printed on pink paper. Sensitive Data Forms must not be electronically filed.
- (b) If a court rule, court order, or statute requires sensitive data to be filed or included in a case record, the following abbreviations must be used:
  - (1) only the last four digits of social security numbers and financial account numbers.
  - (2) only the initials of minor children.
  - (3) only the month and year of an individual's birth date.
- (c) A party must file the Sensitive Data Form at the same time the first case record containing the abbreviated sensitive data is filed. A party must file additional Sensitive Data Forms in a particular cause only if a case record is filed containing abbreviated sensitive data not previously included in a Sensitive Data Form.

### 14.3 Duty of Court and Court Clerk.

- (a) The court or court clerk must keep Sensitive Data Forms physically separated from case records.
- (b) The court or court clerk must limit access to the forms to a party or an attorney of record in the cause in which the sensitive data form is filed, and court officials, court personnel, or other governmental entities, including a Title IV-D agency and law enforcement agencies, whose duties require access to this sensitive data. However, a court or court clerk may compare information



provided by a third party to information in a Sensitive Data Form and confirm or affirmatively negate that the third party's information matches the information in the Sensitive Data Form.

(c) The court or court clerk has no obligation to review a case record for sensitive data.

**14.4 Sanctions.** A court may impose appropriate sanctions for a party's violation of this rule.

## **RULE 15. REMOTE ACCESS TO COURT CASE RECORDS**

**15.1 Scope.** This Rule covers remote access to case records in all Texas courts. The rule does not govern access to records that are governed by Rule of Judicial Administration 12 or other non-adjudicatory records such as title records, vital statistics, birth records, naturalization records, voter records, and instruments recorded for public notice.

### **15.2 Definitions.**

(a) *Case record* means a document filed in a matter before a court pertaining to acting in its adjudicative function and a court index, calendar, docket, minute, or register or actions.

(b) *Remote access* means searching, inspecting, printing or copying information in a case record through an internet or other electronic connection other than through a public-access terminal supplied by a court, a court clerk, or a governmental entity.

### **15.3 Remote Access permitted.**

(a) A court or court clerk may allow remote access to case records. If remote access is allowed, procedures for such access must

(1) use appropriate security measures, procedures, devices and software to ensure records are maintained in the form as originally filed,

(2) permit access only by case number, caption, or the first and last name of a party, unless the case record is an index, calendar, docket, minute, or register of actions, and

(3) otherwise comply with this rule.

(b) If a court or court clerk allows remote access, the court or court clerk has the discretion to adopt a system that requires users to register with the court or court clerk, obtain a log-in and password, and pay a fee authorized by law.

**15.4 Case Records Excluded from Remote Access.** Notwithstanding anything in Rule 15.3, a court or court clerk must not allow remote access to the following case records:

(a) a document to which access is restricted by law or court order;

(b) a medical, psychological or psychiatric record, including an expert report based on a medical, psychological or psychiatric record;

- (c) a pretrial bail or pre-sentence investigation report;
- (d) a statement of reasons or defendant stipulations in a criminal case, including attachments;
- (e) an income tax return;
- (f) a case record in a Family Code proceeding, other than a case record, such as a judgment, index, calendar, docket, minute, or register of actions, created by a court in its adjudicative function;
- (g) an exhibit tendered or admitted at a hearing or during a trial;
- (h) a document filed with a court in camera, solely for the purpose of obtaining a ruling on the discoverability of such documents; and
- (i) any other document excluded from remote access by court order for good cause shown.

**15.5 Procedures If Remote Access Allowed.**

- (a) A party filing a case record containing information excluded from remote access under Rule 15.4 must type or stamp in 36-point font “CONTAINS INFORMATION EXCLUDED FROM REMOTE ACCESS” at the top of the first page of the case record.
- (b) A court or court clerk has no duty to review a case record that does not contain a notice under Rule 15.5(a) to determine whether it contains information excluded from remote access under Rule 15.4.

**15.6 Third-Party Technology Providers.** If a third party is under contract to provide remote access to case records for a court or court clerk, the contract must require the third-party to comply with this rule.

**15.7 Exempt Individuals and Entities.**

- (a) This rule does not limit an individual’s remote access to case records filed in a proceeding in which the individual is a party or an attorney.
- (b) This rule does not limit remote access to case records by court officials and personnel or governmental entities entitled to access by law or court order.

**15.8 Requests for Deviations.** A court may submit for approval a written request to the Supreme Court of Texas to deviate from this rule.

**15.9 Sanctions.** A court may impose appropriate sanctions for a party’s violation of this rule.

\*\*\*\*\*

Rules 14 and 15 of the Texas Rules of Judicial Administration are added as follows. The rules, with any changes made after public comments are received, take effect on January 1, 2006.<sup>1</sup> Earlier compliance with these rules is strongly encouraged.

---

<sup>1</sup> The Supreme Court must publish amendments to the Rules of Judicial Administration at least 120 days before their effective date and must provide at least 60 days for review and comment on the amendments. TEX. GOV'T CODE § 74.024(d).

**Minority Report on Bulk Distribution of Court Case Records**  
*Subcommittee on Rules of Judicial Administration*  
**March 30, 2005**

Frequently, court clerks receive requests for exact copies of certain case records in a large number of cases. For example, a corporate representative might ask for all criminal dispositions, including the name, date of birth, and address of the criminal defendant, over a number of years, or a list of all filings on a given day (or every day), or dispositions in a certain type of case, such as an eviction proceeding, for a given month. The majority of these requests are limited to court-created case records such as information in an index, calendar, docket, minute or register of action, not case records filed by a party such as pleadings or motions. These requests are commonly referred to as requests for bulk access or bulk distribution.

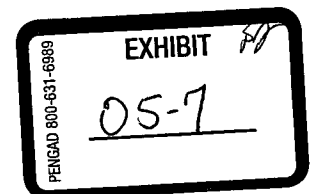
Bulk distribution of court case records is a controversial topic currently being considered by courts across the nation. According to the Texas Judicial Council's report, of the handful of states who have even address the issues surrounding remote access, Arizona, California, Indiana, Utah, and Washington have decided to regulate bulk access in some way. The debate is (hopefully, fairly) characterized as follows:

Advantages to bulk distribution:

- Allowing the public to obtain information from court records from a third party may reduce the number of requests to the court for the records. Fewer requests mean less court staff resources devoted to answering inquiries and requests.
- Access to multiple records broadens the public's ability to monitor performance of the judiciary.
- Government and law enforcement use business databases to further governmental interests. Individuals also rely on business databases when hiring nannies, home nurses, house cleaners, etc.
- Arguments that data in private databases can become "stale" are misplaced. Data furnishers are prohibited from furnishing data they know is inaccurate; they have an affirmative duty to correct information. 15 USC §§ 1681 *et seq.* (Fair Credit Reporting Act).

Disadvantages to bulk distribution:

- Public confidence in judiciary may diminish if a third-party database contains inaccurate, stale or incorrectly linked information derived from court records.
- Court relinquishes control over accuracy of information, including information that may later be removed from the court's records (*e.g.*, expungement).
- Court resources may be required to "refresh" information on a frequent, periodic basis (cutting against argument that third-party databases decrease court staff resources).
- Counties who have invested in electronic databases may not be given the opportunity to recoup their costs.





**PAUL WOMACK, JUDGE,  
COURT OF CRIMINAL APPEALS OF TEXAS.**

**P.O. Box 12308,  
Austin, Texas 78711.  
(512) 463-1595. Fax: 463-7061.  
E-mail: Paul.Womack@cca.courts.state.tx.us**

April 1, 2005

To the Supreme Court Advisory Committee:

Thank you for giving me the opportunity to see the amended drafts of RJA's 14 and 15.. Here are some comments and questions, from the criminal-law side.

*Three Substantive Matters*

*1. Names of minors.* Rule 14.1(f) includes "the name ... of a minor child" in the definition of sensitive data. Rule 14.2(b)(2) says that if a statute requires filing of a minor child's name, only the initials must be used.

The question arises, what about the names of children in indictments?

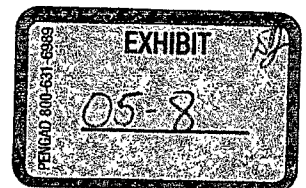
All minor children aged 17, and some who are younger, may be defendants in criminal cases. (See Penal Code section 8.07.) Should the rule except the names of criminal defendants and the names of persons who are alleged to have acted with criminal defendants?

No small number of indictments allege that children were victims of crimes.

For sex-offense victims, Chapter 57 of the Code of Criminal Procedure establishes a system for confidentiality of files and records that contain identifying information of victims. The system permits a victim to choose a pseudonym which replaces the victim's name in the records of law-enforcement agencies and legal proceedings. By the usual doctrine that statutes trump court rules, this statute would seem to control in the case of a sex-offense victim who has chosen a pseudonym.

In other cases in which a minor child is a victim, statutes may require more than initials in an indictment. Article 21.02(7) of the Code of Criminal Procedure requires, "The offense must be set forth in plain and intelligible words." Article 21.03 says, "Everything should be stated in an indictment which is necessary to be proved." Due-process requirements of notice to a defendant also are involved.

Perhaps the rule should exclude indictments (and their misdemeanor equivalents: complaints and informations).





2. *Pre-sentence investigation reports.* Rule 15.4(c) excludes pre-sentence investigation reports from remote access. I do not question that they should be excluded from such access, but a statute already excludes them from any public access. See Code of Criminal Procedure Article 42.12, section 9(j) (making such reports “confidential” and permitting them to be released to only the parties and certain licensed counselors).

3. *Statement of reasons or defendant stipulations.* Rule 15.4(d) excludes from remote access “a statement of reasons or defendant stipulations, including attachments.” Two questions:

What is meant by a “statement of reasons”? This is not a term that I have heard used in Texas criminal procedure. I believe it has several meanings in federal criminal procedure, some of which include statements that district courts make for the appellate record, and others that include statements that the government makes to the district court.

Why would stipulations be excluded from remote access? Ninety-seven per cent of felony convictions are the result of guilty pleas (see Office of Court Administration, *Annual Report of the Texas Judicial System Fiscal Year 2004* at 42). Almost all of them are based on judicial confessions and stipulations of evidence, which are routinely included in the clerk’s records.

*Formal Matters (Just One Reader’s Reactions.)*

Rule 14.1 says, “The following data is sensitive.” I thought “data” was plural. The following data *are* sensitive?

Rule 14.3(b) requires a clerk to confirm or affirmatively negate a match of information. “Affirmatively negate” sounds oxymoronic. Like “fully empty.” How about “expressly negate”?

Is there a typo at the end of Rule 15.2(a), where its says “register or actions”? Register of actions?

With best wishes, I am,

Yours truly,

Paul Womack, Judge.

Copies:

Sharon Keller, Presiding Judge;

Larry Meyers, Judge;

Barbara Hervey, Judge;

Cathy Cochran, Judge;

Nathan Hecht, Justice.