

The Sedona Conference WG1 Brainstorming Group Draft Outline on the Need for Guidance and Uniformity in Filing ESI Under Seal (Oct. 2019)

Brainstorming Group Members:

A.J. de Bartolomeo (Group Leader)

Ronald J. Hedges (Group Leader)

John M. Conlon

Hon. Joy Flowers Conti

Lucy A. Dalglish

David M. Fry

Anne Bentley McCray

Karen Mitchell

Jennifer A. Nelson

Tony R. Petruzzi

Kelli L. Sager

Jeffrey R. Schaefer

David A. Schulz

Heather Kolasinsky (Steering Committee Liaison)

Timothy M. Opsitnick (Steering Committee Liaison)

Martin T. Tully (Steering Committee Liaison)

Copyright 2019, The Sedona Conference. All Rights Reserved.



**THE SEDONA CONFERENCE WG1 BRAINSTORMING GROUP ON
THE NEED FOR GUIDANCE AND UNIFORMITY IN FILING ESI UNDER SEAL
(DRAFT OUTLINE, OCTOBER 2019)**

INTRODUCTION

The charge of this Brainstorming Group (BG), as described originally to the discussion leaders and entire BG, was to focus on “the potential need for guidance and uniformity in the process for filing ESI under seal.” The BG itself is at the “intersection” of WG2 and WG11. The intent of the BG in this Discussion Draft is to present viewpoints for consideration at the WG1 meeting in St. Louis, with a goal of reaching consensus on whether Sedona should or should not proceed to develop the guidance and uniformity (“guidance”) suggested above. With all this in mind, the BG proposes the following viewpoints for consideration in St. Louis.

This Discussion Draft includes two appendices. The first is a set of “Common Features of Recently-Developed Court Rules and Policies on Public Access to Court Records” developed by WG2. The second is a draft model rule.

Some introductory questions are appropriate:

1. Who is the intended audience for a potential paper on this topic?
 - a. Outside litigation counsel tasked with the many challenges of court filings and the need to protect appropriately non public or statutorily protected private information
 - b. In-house counsel (General Counsel, Privacy and Compliance) tasked with protecting the private information of third parties
2. Why do they need it? What are the challenges being addressed?
 - a. Traditional challenges
 - There has always been a tension between the public’s right to access the information presented to our courts and litigants’ legitimate desire or obligation to protect and keep private their information and that of non-parties.
 - It can be difficult to file ESI under seal. Yet, in many civil cases, there is little public interest in the case or in the information of the parties. To

force every civil litigant who wants to protect confidential or protected information to spend significant time and expense in doing so may be antithetical to Rule 1 of the Federal Rules of Civil Procedure.

b. New challenges protecting third party privacy

- Civil cases can involve protected information of non-parties, such as PI or PHI, that litigants who are the custodians of such data are obligated to take certain measures to protect from unauthorized disclosure.
- Tensions can arise between the need to adequately protect non-party information and the public's entitlement to judicial records and proceedings.
- Especially for non-parties, the risk of unauthorized access to that protected information compounds the "risk" posed by the public's right to know.

3. Why and how is this topic of interest?

a. Historical inconsistency among federal and state courts

- There is considerable disparity among federal courts in handling requests to file ESI under seal, from where courts look for authority to do so, the standards by which that authority is applied. The process and burden of proof can vary considerably from jurisdiction to jurisdiction, and from court to court. This disparity gives rise to the potential for the same ESI being allowed to be sealed in one place but not elsewhere.

b. New challenges of data privacy

- The scope of protected ESI has expanded and continues to expand. Statutes such as the California Consumer Privacy Act (CCPA) broaden the definition of Personal Information to include data not traditionally considered as "private" under, for example, most state data breach notification statutes.

VIEWPOINTS

1. Is there a need for, and a realistic opportunity to develop, a uniform approach to sealing for all the federal and state courts in the Nation? On the one hand, the goal of the Federal Rules of Civil Procedure, as described in Rule 1, is to “secure the just, speedy, and inexpensive determination of every action and proceeding” in the federal trial courts. A uniform approach among the federal trial-level courts within the scope of the Civil Rules would appear to further those goals. Moreover, for attorneys and parties (or nonparties) who litigate in more than one federal judicial district, uniformity would help avoid varying and possibly conflicting local rules. On the other hand, why is a uniform approach among the federal courts desirable? Should individual judicial districts have the discretion to set their own procedural rules related to sealing that might be consistent with the practices of the states in which those courts are located?

At the state level, the question of a uniform approach becomes even more problematic. Should Sedona suggest the equivalent of a uniform rule for adoption by the states on an individual basis? Again, uniformity might be desirable. However, should we expect that the states would adopt a uniform rule?

2. Assuming that Sedona does proceed further, should any Guidance be limited to ESI or should it encompass physical things such as paper? We already have a uniform standard that addresses loss of ESI, under Rule 37(e), and a standard that varies across the circuits for the loss of physical things. Does the experience to date with these separate standards warrant a continued “bifurcation” based on the nature of what might be sealed, or should any Guidance suggest one approach for everything?

At the state level, as noted above, might uniformity be desirable? If so, might Sedona contribute toward uniformity or should the states each go their own way?

3. Assuming that Sedona proceeds further, should any Guidance incorporate cybersecurity standards or goals? Cybersecurity is at the forefront of discussion at the federal and state levels today (examples including the California CPA and the New York SHIELD Act). Plainly, Sedona cannot make any suggestions as to whether courts should develop in-

house cybersecurity or rely on particular vendors to do so. However, might Sedona suggest certain “reasonable” standards that courts might aspire to? Such suggestions would, in turn, raise issues of competence to develop standards and what those standards might be.

4. Assuming that Sedona proceeds further, should any Guidance address some or all of the following?
 - a. What might be the relationship between confidentiality/protective orders under Rule 26(c) and its state equivalents and sealing orders? Should the latter include a provision that a receiving party give notice to a producing party that the former intends to move ESI produced by the latter into evidence at trial or on a motion, dispositive or non-dispositive?
 - b. Assuming there is a notice as described above, should the order also provide a procedure to bring the question of sealing before the court at a particular time (for example, “X” days before a substantive motion might be heard or a trial commenced)?
 - c. Should any sealing motion be docketed in such a manner so as to give notice and sufficient time to allow a non-party to move to intervene under Rule 24, either on a “of-right” or permissive basis?
 - d. Might the Guidance suggest some mechanism that would allow a court to “lodge” rather than “file” something that a party wishes to file under seal? If so, is there a distinction for First Amendment and common law rights of access between the two?
 - e. Should any Guidance include a “sunset” date on which a sealing order would expire? If so, should that date reflect a time when ESI should be “destroyed” or returned to a party? If the latter, to which party, the one that proffered it or the one that produced it?
 - f. Should the Guidance differentiate between ESI that is protected as a matter of law (for example, PHI under HIPAA) as opposed to ESI which a party contends is a

trade secret or otherwise confidential (for example, financial information or other business-related projections)?

- g. Should any Guidance reflect distinctions between ESI that might be exchanged or filed as opposed to events, such as oral argument and trial? If so, should the Guidance address closure of trial or other in-court proceedings?
- h. Should any Guidance recognize a distinction between ESI that might be filed under seal and redacted versions that would be filed and available to the public?
- i. Should any guidance address highly technical issues involving ESI? ESI orders and production agreements increasingly specify that some or all ESI be produced in native format rather than be printed out as hard copies or converted to static image files (e.g., TIFF or PDF). In view of this, should ESI continue to be converted to a static image format or printed out in order to be filed under seal, or should courts move toward accepting --- or even requiring --- ESI in native format?
 - i. What should be considered “under seal” when ESI is involved? Is the native ESI file also considered to be under seal after filing only an imaged version?
 - ii. If native ESI is to be considered under seal when only an imaged version is filed, how should native ESI that is under seal be designated? Should some identifying marker be made of record that identifies the native ESI with precision (e.g., an original file name, URL or a hash value)? Would precise identification of ESI filed under seal be problematic since near-duplicate (i.e., substantively identical) versions of ESI can have different files names, and hashes?
 - iii. Even if imaging ESI for submission under seal remains a default standard, how should ESI that cannot be usefully imaged (e.g., large Excel files, database files, proprietary file types (e.g., SAS datasets), audiovisual media materials) be submitted under seal? Is uniformity in this regard a useful goal?

5. Underlying this Discussion Draft is a broader question: Should Sedona look at any Guidance as a vehicle to go beyond procedural questions such as set forth above and instead address substantive questions such as standards for confidentiality and sealing orders? It appears that some BG members would prefer to do so. Others are opposed to doing so and, among other things, point to Sedona's earlier efforts in WG2.

DRAFT

APPENDIX A

The Sedona Guidelines: Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases v-vi (Mar. 2007)

Common Features of Recently-Developed Court Rules and Policies on Public Access to Court Records

1. A statement of the overall purpose for the rule or policy.
2. Definitions of key terms used in the rule.
3. A procedure to inform litigants, attorneys, and the public that (a) every document in a court case file will be available to anyone upon request, unless sealed or otherwise protected; (b) case files may be posted on the Internet; and (c) the court does not monitor or limit how case files may be used for purposes unrelated to the legal system.
4. A statement affirming the court's inherent authority to protect the interests of litigants and third parties who may be affected by public disclosure of personal, confidential, or proprietary information.
5. A list of the types of court records that are presumptively excluded (sealed) from public access by statute or court rule.
6. A statement affirming that the public right to access court records and the court's authority to protect confidential information should not, as a general matter, vary based on the format in which the record is kept (e.g., in paper versus electronic format), or based on the place where the record is to be accessed (i.e., at the courthouse or by remote access).
7. As an exception to feature 6 above, a list of the types of court records that—although not sealed—will not be available by remote electronic public access.
8. A list of the types of information that either: a) must not be filed in an open court record, or b) if filed, must be redacted or truncated to protect personal privacy interests. These provisions mainly apply to personal identifiers such as the SSN, account numbers, and home addresses of parties.

9. Procedure for a court to collect and maintain sensitive data elements (such as SSN) on special forms (paper or electronic) that will be presumptively unavailable for public access. Such procedures generally build on technology to segregate sensitive information so that public access can be restricted in appropriate situations.
10. Procedure to petition for access to records that have been sealed or otherwise restricted from public access, and a statement of the elements required to overcome the presumption of nondisclosure.
11. Procedure to seal or otherwise restrict public access to records, and a statement of the burden that must be met to overcome the presumption of disclosure.
12. An affirmation that a rule on public access to court records does not alter the court's obligation to decide, on a case-by-case basis, motions to seal or otherwise restrict public access to court records.
13. Guidance to the courts concerning data elements that are contained in electronic docketing systems that must (or must not) be routinely made available for public access.
14. Guidance for attorneys and/or litigants concerning: (a) the extent to which public case files will be made available electronically; and (b) the need to exercise caution before filing documents and information that contain sensitive private information, which is generally defined elsewhere in the rule.
15. An explanation of the limits, if any, on the availability of "bulk" and/or "compiled" data from public court records. Some rules specify that such data will only be made available to certain entities, for certain defined purposes, and pursuant to agreements to refrain from certain uses of the records obtained.
16. A statement concerning the fees that a court may charge for public access to court records.

APPENDIX B

Draft model local rule submitted by Karen Mitchell (with comments in italics):

LR 5.2: Filings Made Under Seal.

- a. Sealed filings by law. A party may make a filing under seal if a statute or rule requires or permits the filing to be made under seal. The party should state in docket text the specific authority under which the filing is made under seal. Filings made under this subsection will remain restricted from public access under the applicable statute or rule, or as otherwise ordered by the court.

Comments: Sealed filings authorized by law and discretionary sealed filings should be addressed separately. The legal authority for any sealed filings should be noted in docket text.

- b. Discretionary sealed filings. If no statute or rule requires or permits a filing to be made under seal, a party may not make a filing under seal without permission of the court.

- (1) To request permission to make a filing under seal, a party must file a motion for leave to file. The party must attach the proposed sealed filing as a sealed exhibit to the motion for leave to file.

Comments: Our court has permitted sealed filings to be made electronically for many years. The process of attaching a sealed filing as an exhibit to a motion for leave to file has worked well. Parties in NDTX may also file the motion for leave under seal, which may be controversial, but it has worked well in NDTX.

- (2) The motion for leave to file must include the following:

- A. the reasons for filing under seal, supported by specific factual representations, including a description of potential harm to any party or non-party if not made under seal;
- B. an explanation of why alternatives to filing under seal would not provide sufficient protection;
- C. a description of any portion of the filing that has previously been designated as privileged, confidential, or proprietary under a protective order or non-disclosure agreement; and
- D. a certification that the party has conferred with all other parties in an attempt to reach an agreement on the need to file the document under seal and to explore redaction and other alternatives.

Comments: It is important that the motion justify the reasons for sealing to respect the right of public access and prevent abuse. It is also important to require the parties to confer and explore other alternatives.

- (3) The court may, after weighing the reasons to permit a sealed filing against the right of public access, grant leave to make the filing under seal. In making this decision, the court should consider individual privacy rights and interests, proprietary business information, security concerns, and any other factors that might demonstrate harm to a party or non-party.

Comments: I cannot speak to the appropriate legal standard, but it seems that the court should weigh each of these common concerns in deciding whether to grant any discretionary request to seal. Perhaps “may” should be changed to “should.”

(4) In granting leave, the court will specify the conditions under which a filing may be made under seal, including:

A. whether the filing may be made entirely under seal, or whether a redacted version must be filed in the public record with an unredacted version filed under seal;

B. whether and to what extent the party must provide summary information about the filing in publicly available docket text;

Comments: In NDTX, the public docket text indicates the nature of each sealed document without revealing any protected content. This kind of transparency is good, and it has not created any problems.

C. whether the filing is to be permanently sealed or scheduled to be automatically unsealed 120 days following case disposition;

Comments: If the clerk's office can work with a date certain (such as 120 days following case disposition), we should be able to develop a programmatic solution that will generate both automatic notices at case closure and automatic unsealing after the expiration of a specific number of days.

D. whether the filing should, as an alternative to sealing, be made in the public record but with remote electronic access restricted to the parties only; and

Comments: Information that is highly sensitive, which would have been "practically obscure" in the world of paper files, will be broadcast on the World Wide Web when filed electronically if

not protected from remote public access. In some instances, restricting the information so that it is not remotely publicly available (but available to the public in the clerk's office) might be a reasonable solution.

E. any other conditions the court deems appropriate.

(5) If a party has been granted leave to make a filing under seal or with restricted remote public access, the party must make the filing as directed by the court.

Comments: The sealed exhibit filed with the motion will not have been docketed as a "filing," so the party must file it in the record once leave has been granted. If the file date becomes an issue, the judge may deem the document filed as of the date the motion for leave to file was filed or any other date the judge decides is appropriate.

(6) If a party has not been granted leave to make a filing under seal or with restricted public access, the sealed exhibit attached to the motion for leave to seal will, on request to the clerk, be deemed stricken from the record unless the court otherwise directs.

Comments: This should not be a gotcha. If leave to file under seal is not granted, the party should be able to request that the sensitive exhibit be stricken.

(7) If a filing has been made under seal without proper authority or permission, the court may, without prior notice to the filing party, strike the filing or direct that it be unsealed.

Comments: Parties should be warned about making filings under seal without proper authority to do so.

(8) At the conclusion of a civil action, including all appeals, parties will receive notice if any filings remain under seal that were not permanently sealed by the court. The notice will include the date that the filings will be automatically unsealed.

Comments: It is important for documents under seal that are not permanently sealed to be addressed soon after case closure. This notice to parties should be programmed into CM/ECF so that it is distributed automatically. A party may move for relief if the 120-day period after final disposition is insufficient to protect the filing.

(9) The clerk will unseal any filings not permanently sealed 120 days following case disposition unless otherwise directed by the court.

Comments: The unsealing should occur automatically. This functionality should be programmed into CM/ECF.