EXPLANATORY REPORT

PUBLIC ACCESS POLICY OF THE UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA: CASE RECORDS OF THE APPELLATE AND TRIAL COURTS

GENERAL INTRODUCTION

Recognizing the importance of the public's access to the courts, the Administrative Office of Pennsylvania Courts (AOPC) has developed statewide policies governing access to court records. With the Supreme Court’s approval, protocols have been implemented for access to electronic case records in the Judiciary's statewide case management systems, magisterial district court case records, and financial records of the Unified Judicial System (UJS). In 2013, the AOPC embarked on the next phase of policy development designed to address access to case records of the trial and appellate courts.

This latest effort is necessitated by the confluence of several factors. The proliferation of e-filing systems and related decisions to post (or not post) case records online (as part of document imaging or e-filing systems) on a county-by-county basis has resulted in disjointed accessibility to the UJS's trial court case records. A county may post all divorce and custody records online for viewing, perhaps for free, and a neighboring county may not. Online posting of sensitive information contained in case records, such as social security numbers, currently depends upon geography. Surveys conducted by the AOPC also revealed the treatment of sensitive information contained in paper case records maintained by the filing offices varies widely. For example, whether a social security number is available to a member of the public who wishes to view the records of a particular case in a filing office depends upon local practices.

The ongoing initiative to implement e-filing in Pennsylvania's appellate courts -- the PACFile project -- is also a catalyst for policy development. While appellate court opinions, orders and dockets have been online via the UJS’s website for over a decade, the e-filing of appellate briefs and related legal papers raises basic questions that should be considered when a court undertakes such a project, such as: What sensitive information must be redacted? Who is responsible for ensuring the appropriate information is redacted?

At the state and local level, the Judiciary is moving forward into the digital age, and it clearly needs to give thoughtful consideration to its systems and procedures to ensure equal access to the UJS's trial and appellate case records. Disparate filing and access protocols certainly impede the statewide practice of law in the Commonwealth. Litigants and third parties, some of whom are unrepresented or are not voluntary participants in the judicial process, may be left in the dark as to whether their private, personal identifiers and intimate details of their lives will be released (online) for public viewing.
Government and the private sector collect extensive amounts of personal data concerning individuals' finances, unique identifiers, and medical history and so on. Many of these types of data are relevant to the cases that are before the courts for decision, and some data is provided in court filings even though irrelevant to the matter before the court. Therefore, like other branches of government and the private sector, the courts are constantly considering issues regarding the need for openness and transparency and the concern for personal privacy and security.

With regard to the courts, however, the constitutional and common law presumption of openness has to be carefully weighed against relevant practical, administrative considerations when crafting solutions to avert breaches of privacy and security. Striking the right balance is not an easy task.

The public's right to access court proceedings and records is grounded in the First and Sixth Amendments of the U.S. Constitution, Article I §§ 7, 9, and 11 of the Pennsylvania Constitution, and the common law. While there is overlap between the common law and constitutional analyses, there is a distinction between the two. Specifically, the constitutional provisions provide a greater right of access than the common law.\(^1\) However, these constitutional and common law rights are not absolute and may be qualified by overriding interests. A more extensive discussion of the right to access is contained in the *Explanatory Report of the Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania*.\(^2\)

Therefore, with the approval of the Supreme Court, the Court Administrator of Pennsylvania convened a working group to study and develop a proposed policy for public comment. Under the experienced and dedicated leadership of Commonwealth Court Judge Renée Cohn Jubelirer and Montgomery County Court of Common Pleas Judge Lois E. Murphy, the working group undertook its charge with an open mind and an aim to appropriately balance the competing interests at hand. The group consisted of judges, appellate court filing office personnel, local court personnel, two Prothonotaries/Clerks of Courts, one Register of Wills/Clerk of Orphans’ Court, and representatives from the Pennsylvania Bar Association and the rules committees of the Supreme Court, as well as AOPC staff.

Before developing a proposed policy, the working group studied and discussed the different types of records pertaining to criminal, domestic relations, civil, juvenile, orphans’ court and appellate matters filed in the courts. Tackling each case type individually, the working group considered existing legal restrictions and other jurisdictions' access policies on the release of data and documents. In formulating whether information and documents should be considered confidential, the group also determined how access would be limited. There are categories of information that are completely restricted, such as social security numbers, and categories that are restricted

---

\(^1\) See *Commonwealth v. Long*, 922 A.2d 892 (Pa. 2007).

from online viewing by the public but remain available for public inspection at a court facility, such as original and reproduced records filed in the appellate courts.

In crafting its proposal, the group was guided at all times by the long-standing tradition of access to court records and the important interests it serves, as follows:

to assure the public that justice is done even-handedly and fairly; to discourage perjury and the misconduct of participants; to prevent decisions based on secret bias or partiality; to prevent individuals from feeling that the law should be taken into the hands of private citizens; to satisfy the natural desire to see justice done; to provide for community catharsis; to promote public confidence in government and assurance that the system of judicial remedy does in fact work; to promote the stability of government by allowing access to its workings, thus assuring citizens that government and the courts are worthy of their continued loyalty and support; to promote an understanding of our system of government and courts.


However, the group also recognized that transparency of judicial records and proceedings must be balanced with other considerations in this Internet age. The group endeavored to strike the appropriate balance between access and interests involving the administration of justice, personal privacy and security -- particularly with regard to online records. Also essential to the group's evaluation were practical considerations, such as the methods of redaction to be implemented and identification of various "best practices" that should be instituted statewide.

The working group provides the following relevant commentary for the sections of the proposed policy.

**SECTION 1**

The definitions incorporate elements of those found in existing UJS public access policies and other legal authorities.

Case records of the Traffic Division of the Philadelphia Municipal Court are not governed by this policy. The working group recommends that the Public Access Policy of the Unified Judicial System of Pennsylvania: Official Case Records of the Magisterial District Courts (hereinafter referred to as “MDC Paper Policy”) be amended to govern access to those records.

It is important to note how this proposed policy would intersect with existing UJS policies, namely the Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania (hereinafter referred to as “Electronic Policy”) and MDC Paper Policy. The Electronic Policy governs access to the electronic case record information,
excluding images of scanned documents, residing in the three statewide case management systems: Pennsylvania Appellate Courts Case Management System, Common Pleas Case Management System and the Magisterial District Judge System. Put simply, the Electronic Policy governs what information resides on the public web docket sheets accessible via the UJS web portal or is released to a member of the public requesting electronic case record information from one of the systems.

The MDC Paper Policy governs access to the paper case records on file in those courts.

This proposed policy governs access to (1) official paper case records of appellate courts, courts of common pleas, and Philadelphia Municipal Court, (2) images of scanned or e-filed documents residing in the three statewide case management systems, (3) images of scanned or e-filed documents residing in the case management systems of the judicial districts, and (4) case record information posted online by judicial districts via their own “local” case management systems. This proposal ensures a more equitable and systematic approach to the case records filed in and maintained for the trial and appellate courts.

The definition of “financial source document” is derived from the definition of “sealed financial source documents” used in Minnesota (Minn.G.R.Prac. Rule 11.01) and Washington (WA.R.Gen. Rule 22(b)).

SECTION 2

Section E provides that the policy applies to case records created on or after its effective date. The working group recognizes that there will be a period of transition prior to full implementation of this policy; that is, some cases commenced prior to the effective date of the policy will contain information that the policy restricts from public access. To expect full and complete implementation of the policy by applying it retroactively to existing records is impractical and burdensome.

The working group anticipates recommending a delayed implementation date when it submits the proposal to the Supreme Court for approval. This will afford the time necessary for court personnel, attorneys, and members of the public to familiarize themselves with the policy's provisions and make necessary adjustments to existing forms, protocols and systems. A similar approach was taken when the Supreme Court adopted the public access policy for magisterial district courts. The group will also recommend that the AOPC, perhaps in partnership with bar associations and other stakeholders, develop educational tools so that litigants, attorneys, court personnel, vendors, and members of the general public can be made aware of the policy's provisions. This would include Commonwealth agencies that conduct administrative proceedings to ensure that the agency's record on appeal can be filed without delay.
Notice to litigants can be an important tool for educational purposes. The public, and litigants in particular, may assume some or all of the information in court records is private. A notice about the existence of this policy may serve to educate litigants so that when they file pleadings and legal documents, they will be acting with knowledge, and in turn they can make informed decisions about what to include in their filings with the court. By way of example, Commonwealth Court provides the following notice to unrepresented parties in appeals from Commonwealth agencies:

Unless sealed by statute or court order, all dockets, filings and orders and opinions of the Court in your case will be public records and subject to public inspection. The Court's public dockets are available on the Court's website and are searchable on-line. The Court's opinions, which generally include a summary of the case including the identity of the parties and the relevant factual background, also are available on the Court's website and searchable on-line. Generally, the Court will seal or restrict public access to dockets or opinions only upon motion and only for good cause.

Additionally, upon adoption of the MDC Paper Policy, the AOPC revised its criminal, civil and landlord-tenant complaint forms to include notice as to the policy's general prohibition on inclusion of social security numbers and financial information. 204 Pa. Code §§ 213.1 - 213.7.

The working group notes that this section's provisions are similar to those contained in the MDC Paper Policy, which have been successfully implemented.

SECTION 4

The working group acknowledges that requestors may be unable to complete a written request, if required by a court. In such circumstances, access should not be denied but may be delayed until the custodian or designated staff is available to assist the requestor. If the request is granted, it may be necessary for the custodian or designated staff to sit with the requestor and monitor the use of the file to ensure its integrity. This is consistent with the responsibility placed upon the custodian and designated staff for the security, possession, custody and control of case records in Section 2.0(B). Such a practice is also consistent with the requirement that addressing requests for access cannot impede upon the administration of justice or the orderly operation of a court, pursuant to Section 2.0(C).

The working group notes that this section's provisions are similar to those contained in the MDC Paper Policy, which have been successfully implemented.

SECTION 5

While implementing the provisions of this policy should not unduly burden the courts and custodians or impinge upon the delivery of justice, it is reasonable for the public to expect that courts and custodians shall respond to requests for access in a
consistent fashion. This section brings uniformity, in general, as to when and how courts and custodians shall respond to requests. Similar sections are found in the Electronic Policy and MDC Paper Policy.

SECTION 6

The surveys conducted by the working group regarding the public access protocols of the judicial districts revealed different approaches to imposition of fees, especially with regard to remote access to court records. Some impose a fee for providing remote access because the costs associated with building and maintaining such systems are often substantial. Given that remote access is a value-added service, not a requirement, it is thought that those who avail themselves of this service should be charged for the convenience of maintaining these systems.

Others do not impose fees for remote access because providing this service reduces the “foot traffic” in the filing offices for public access requests. This, in turn, frees staff to attend to other business matters, resulting in a financial benefit by reducing costs associated with dealing with the requests over the counter. The AOPC has provided “free” online access to public web docket sheets for cases filed in the appellate courts, criminal divisions of the courts of common pleas and Philadelphia Municipal Court, as well as the magisterial district courts for years. In 2014, 59 million of those web docket sheets were accessed online.

The working group recognizes that local factors play a part in these decisions; however, it is interesting to note that the two largest judicial districts in the Commonwealth are at opposite ends of the spectrum (i.e. one has posted virtually all dockets and documents for free, and the other posts some dockets for free but not documents). While the working group recognizes that other factors play into these determinations (such as, technological capabilities, statutorily mandated fees) and the simple distinction drawn above requires further study, the working group questions if the public would benefit from some standardization in this area to ensure that fees do not become a financial barrier to access.

The working group notes that Section 6's provisions are similar to those contained in the MDC Paper Policy.

SECTION 7

The working group observes that the concept of restricting access to particular, sensitive identifiers is not novel. The Electronic Policy and MDC Paper Policy restrict access to social security numbers and financial account numbers, for example. The federal courts, and many state court systems, have restricted access to the types of identifiers that are listed in Section 7.0.

At the outset, the working group noted that Electronic Policy and MDC Paper Policy provide that access to social security numbers is shielded from release. Moreover,
there are scores of authorities at both the federal and state level that protect the release of this information. While some of these authorities are not applicable to court records, they require access to this information in government records be limited or wholly restricted. For example: 65 P.S. § 67.708(b)(6)(i)(A), 74 P.S. § 201, 42 U.S.C.A. § 405(c)(2)(C)(viii), F.R.Civ.P. 5.2(a)(1), F.R.Crim.P. 49.1(a)(1), Alaska (AK R Admin Rule 37.8(a)(3)), Arizona (AZ ST S CT Rule 123(c)), Arkansas (Sup. Ct. Admin. Order 19(VII)(a)(4)), Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(iii)), Idaho (ID R Admin Rule 32(e)(2)), Indiana (Ind. St. Admin. Rule 9(G)(1)(d)), Maryland (MD. Rules 16-1007), Michigan (Administrative Order 2006-2), Minnesota (Minn.Gen.R.Prac. Rule 11.01(a)), Mississippi (Administrative Order dated August 27, 2008 paragraph 8), Nebraska (Neb Ct R § 1-808(a) and Neb. Rev. Stat § 84-712.05(17)), New Jersey (NJ R GEN APPLICATION Rule 1:38-7(a)), North Dakota (N.D.R.Ct. Rule 3.4(a)(1) and A.R. 41(5)(B)(10)(a)), Ohio (OH ST Sup Rules 44(h) and 45(d)), South Dakota (SDCL § 15-15A-8), Texas (TX ST J ADMIN Rule 12.5(d)), Utah (UT R J ADMIN Rules 4-202.02(4)(i) and 4-202-03(3)), Vermont (VT R PUB ACC CT REC § 6(b)(29)), Washington (WA. R. Gen. Rule 31(3)(1)(a)) and West Virginia (WV R RAP Rule 40(e)(3)).

With regard to financial account numbers, the working group noted that Electronic Policy and MDC Paper Policy provide that access to this information should not be accessible. Many other jurisdictions have taken a similar approach. For example: F.R.Civ.P. 5.2(a)(1), F.R.Crim.P. 49.1(a)(1), Alaska (AK R Admin Rule 37.8(a)(5)), Arizona (AZ ST S CT Rule 123(c)), Arkansas (Sup. Ct. Admin. Order 19(VII)(a)(4)), Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(iii)), Idaho (ID R Admin Rule 32(e)(2)), Indiana (Ind. St. Admin. Rule 9(G)(1)(f)), Minnesota (Minn.Gen.R.Prac. Rule 11.01(a)), Nebraska (Neb Ct R § 1-808(a) and Neb. Rev. Stat § 84-712.05(17)), New Jersey (NJ R GEN APPLICATION Rule 1:38-7(a)), North Dakota (N.D.R.Ct. Rule 3.4(a)(1) and A.R. 41(5)(B)(10)(a)), Ohio (OH ST Sup Rules 44(h) and 45(d)), South Dakota (SDCL § 15-15A-8), Texas (TX ST J ADMIN Rule 12.5(d)), Utah (UT R J ADMIN Rules 4-202.02(4)(i) and 4-202-03(3)), Vermont (VT R PUB ACC CT REC § 6(b)(29)), Washington (WA. R. Gen. Rule 31(3)(1)(b)) and West Virginia (WV R RAP Rule 40(e)(4)).

Concerning driver license numbers, the working group noted that Electronic Policy provides that driver license numbers should be protected. Moreover, there are many authorities at both the federal and state level that protect the release of this information. While some of these authorities are not applicable to court records, they require access to this information in government records be limited or wholly restricted. For example: 65 P.S. § 67.708(b)(6)(i)(A), 18 U.S.C. § 2721 – 2725, 75 Pa.C.S. § 6114, Alaska (AK R Admin Rule 37.8(a)(4)), Idaho (ID R Admin Rule 32(e)(2)), New Jersey (NJ R GEN APPLICATION Rule 1:38-7(a)), Utah (UT R J ADMIN Rules 4-202.02(4)(i) and 4-202-03(3)), Vermont (VT R PUB ACC CT REC § 6(b)(29)) and Washington (WA. R. Gen. Rule 31(3)(1)(c)).

State Identification Numbers (“SID”) have been defined as "[a] unique number assigned to each individual whose fingerprints are placed into the Central Repository of the State Police. The SID is used to track individuals for crimes which they commit, no matter how many subsequent fingerprint cards are submitted." See 37 Pa. Code § 58.1.
The *Electronic Policy* prohibits the release of these numbers. Furthermore, in *Warrington Crew v. Pa. Dept. of Corrections*, 1006 C.D. 2010, the Commonwealth Court upheld a ruling by the Office of Open Records that a SID number is exempt from disclosure through a right-to-know request because such numbers qualify as a confidential personal identification number (opinion unreported).

The working group noted that other jurisdictions also provide similar protections to minors’ names and/or dates of births. For example: F.R.Civ.P. 5.2(a)(1), F.R.Crim.P. 49.1(a)(1), Alaska (AK R Admin Rule 37.8(a)(6)), North Dakota (N.D.R.Ct. Rule 3.4(a)(3) and A.R. 41(5)(B)(10)(c)), Utah (UT R J ADMIN Rules 4-202.02(4)(I) and 4-202-03(3)) and West Virginia (WV R RAP Rule 40(e)(1)).

With regard to abuse victims' address and other contact information, Pennsylvania through the enactment of various statutes has recognized the privacy and security needs of victims of abuse. For example, Pennsylvania’s Domestic and Sexual Violence Victim Address Confidentiality Act (23 Pa.C.S. §§ 6701 – 6713) provides a mechanism wherein victims of domestic and sexual violence can shield their physical address (even in court documents) and hence protect their ability to remain free from abuse. The Pennsylvania Right To Know Law (65 P.S. §§ 67.101 – 67.1304) recognizes the potential risk of harm which can be caused by the disclosure by the government of certain personal information. For example, 65 P.S. § 67.708(b)(1)(ii) prohibits the disclosure that “would be reasonably likely to result in a substantial and demonstrable risk of physical harm to or the personal security of an individual.” Moreover, 23 Pa.C.S. § 5336(b) prohibits the disclosure of the address of a victim of abuse in a custody matter to the other parent or party. 23 Pa.C.S. § 4305(a)(10)(ii) and (iii) provides that the domestic relations section shall have the power and duty to:

“implement safeguards applicable to all confidential information received by the domestic relations section in order to protect the privacy rights of the parties, including: prohibitions against the release of information on the whereabouts of one party or the child to another party against whom a protective order with respect to the former party or the child has been entered; and prohibitions against the release of information on the whereabouts of one party or the child to another person if the domestic relations section has reason to believe that the release of the information may result in the physical or emotional harm to the party or the child.”

In addition, other jurisdictions have taken a measure to protect similarly situated individuals, such as: Alaska (AK R Admin Rule 37.8(a)(2)), Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(iii)), Indiana (Ind. St. Admin. Rule 9(G)(1)(e)(i)), New Jersey (NJ R GEN APPLICATION Rule 1:38-3(c)(12)), and Utah (UT R J ADMIN Rules 4-202.02(8)(E)(i) and 4-202-03(7)).

The working group proposes two approaches to maintaining the confidentiality of the information listed in subsection (A). Parties and their attorneys can set forth the listed information on a Confidential Information Form, designed and published by the AOPC.
This is akin to the procedure set forth in the MDC Paper Policy; the Confidential Information Form used by that policy is posted on the UJS's website at [www.pacourts.us](http://www.pacourts.us).

The alternative approach identified by the working group is for litigants and attorneys to file two versions of each document with the court/custodian – one with sensitive information redacted (“redacted copy”) and the other with no information redacted (“unredacted copy”). The redacted copy shall omit any information not accessible under this policy and be available for public inspection. The unredacted copy shall not be accessible by the public. At least one other jurisdiction has implemented a similar approach. See WA. R. Gen. R. 22(e)(2) (Washington). Some contend that a redacted copy of a document will be more readable than an unredacted copy containing monikers as placeholders for sensitive information not included in the document. This approach may have merit particularly in an e-filing context and was identified as a more amenable solution given the current design of the PACFile project.

While a court or custodian is not required to review any pleading, document, or other legal paper for compliance with this section, such activity is not prohibited. If a court or custodian wishes to accept the burden of reviewing such documents and redacting the same, such a process must be applied uniformly across all documents or cases.

**SECTION 8**

The protocol of submitting to a court or custodian certain documents under a cover sheet so that the documents are not accessible to the public has been instituted in other jurisdictions, such as Minnesota (Minn.G.R.Prac. Rule 11.03), South Dakota (SDCL § 15-15A-8), and Washington (WA.R.Gen. Rule 22(b)(8) and (g)). The working group noted with favor, these protocols and incorporated that concept into this policy. One manner in which to implement this protocol (e.g. the need to separate a confidential document within a file accessible to the public) is to maintain a confidential electronic folder or confidential documents file within the case file, thus ensuring that the file folder with the non-public information can be easily separated from the public case file, when access is requested.

Concerning financial source documents, other jurisdictions have similar provisions regarding such documents including Minnesota (Minn.G.R.Prac. Rule 11.03), South Dakota (SDCL § 15-15A-8), and Washington (WA.R.Gen. Rule 22(b)(8) and (g)).

Similar protocols with regard to minors’ education records are found in other jurisdictions, such as Nebraska (Neb Ct R § 1-808(a) and Neb. Rev. Stat § 84-712.05(1)) and Wyoming (WY R Gov Access Ct Rule 6(a) and WY ST § 16-4-203(d)(viii)).

With regard to medical records, the working group noted that other jurisdictions have similar provisions including Indiana (Ind. St. Admin. Rule 9(G)(1)(b)(xi)), Maryland (MD. Rules 16-1006(i)), Nebraska (Neb Ct R § 1-808(a) and Neb. Rev. Stat § 84-712.05(2)), Utah (UT R J ADMIN Rules 4-202.02(4)(k) and 4-202-03(3)), Vermont
Section 7111 of the Mental Health Procedures Act, 50 P.S. § 7111 provides that all documentation concerning an individual’s mental health treatment is to be kept confidential and may not be released or disclosed to anyone, absent the patient’s written consent, with certain exceptions including a court’s review in the course of legal proceedings authorized under the Mental Health Procedures Act (50 P.S. § 7101). While it is unclear if this provision is applicable to the public accessing an individual mental health treatment records in the court’s possession, the working group believes this provision provides guidance on the subject. Thus, such records should not be available to the public except pursuant to a court order. See Zane v. Friends Hospital et al, 575 Pa. 236, 836 A.2d 25 (2003). Other jurisdictions have similar protocols, such as Maryland (MD. Rules 16-1006(i)), New Mexico (NMRA Rule 1-079(c)(5)), Utah (UT R J ADMIN Rules 4-202.02(4)(k) and 4-202-03(3)), Vermont (VT R PUB ACC CT REC § 6(b)(17)) and Wyoming (WY R Gov Access Ct Rule 6(t)).

Children and Youth Services' records introduced in juvenile dependency or delinquency matters are not open to public inspection. See 42 Pa.C.S. § 6307 as well as Pa.Rs.J.C.P. 160 and 1160. Introduction of such records in a different proceeding (e.g., a custody matter) should not change the confidentiality of these records; thus, the records should be treated similarly. These records are treated similarly by other jurisdictions, such as Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(i)), Indiana (Ind. St. Admin. Rule 9(G)(1)(b)(iii)) and New Jersey (NJ R GEN APPLICATION Rule 1:38-3(d)(12) and (15)).

As required by Pa.R.C.P. No. 1920.33, a marital property inventory includes “a specific description of all marital property in which either or both have a legal or equitable interest individually or with any other person and the name of such other person; and a specific description of all property in which a spouse has a legal or equitable interest which is claimed to be excluded from marital property and the basis for such exclusion.” The extent of the financially sensitive information required to be listed on this document rivals that of the information contained in a financial source document. Therefore, this document should also be treated as confidential. The working group notes that a similar protocol is found in Vermont (VT R PUB ACC CT REC § 6(b)(33) and 15 V.S.A. § 662).

**SECTION 9**

This section safeguards certain sensitive information that is already protected by existing legal authority or was deemed to require protection by the working group from access at the court facility. The latter category included three specific types of records: birth records, incapacity proceeding records and family court transcripts except portions of transcripts when attached to a motion or other legal paper filed with the court.
The working group noted that access to a birth certificate from the Department of Health, particularly an amended birth certificate, such as in an adoption case, is limited pursuant to various statutes. 35 P.S. §§ 450.603, 2915 and 2931. The working group was concerned that unrestricted access to records filed in proceedings about birth records could have the unintended effect of circumventing the purposes of the confidentiality provisions of the above statutory framework. Moreover, at least one jurisdiction, Florida (FL ST J ADMIN Rule 2.420(d)(1)(B)(vi)), provides similar protections to these records. However, concerned that the lack of transparency may erode the public’s trust and confidence, the working group proposes the release of dockets and any court order, decree or judgment. Releasing the dockets as well as any order, decree or judgment disposing of the case is believed to strike the appropriate balance between access to the court's decision, and hence the public's understanding of the judicial function, and personal privacy, or the intimate details of a person's ability to function.

Given the extent of financial and sensitive information that is provided in order that a court may determine whether a person is incapacitated and, if so, that must subsequently be reported in a guardian's report, the working group opined that these records should not be accessible. The working group noted that similar provisions are found in many other jurisdictions including: California (Cal. Rules of Court, Rule 2.503(c)(3)), Florida (F.S.A. §§ 744.1076 and 744.3701), Georgia (Ga. Code Ann. § 29-9-18), Idaho (ID. R. Admin. Rule 32), Maryland (MD. Rules 16-1006), New Jersey (NJ R GEN APPLICATION Rule 1:38-3(e)), New Mexico (NMRA Rule 1-079(c)(7)), South Dakota (SDCL § 15-15A-7(3)(m)), Utah (UT R J Admin. Rule 4-202.02(4)(L)(ii)), Washington (WA.R.Gen. Rule 22(e)) and Wyoming (WY R Gov Access Ct Rule 6(g)). For the reasons of transparency, the working group proposes that the case docket and any court order, decree or judgment be accessible for these cases.

The provisions of Subsection H are consistent with those contained in the Electronic Policy, MDC Paper Policy and Rule of Judicial Administration 509. The Judiciary’s commitment to the principle of open and accessible case records is reflected in the inclusion of a publication requirement.

SECTION 10

Any information to which access is limited pursuant to Sections 7, 8 or 9 is also not accessible remotely pursuant to Subsection A(1). As to Subsections A(2) through (A)(7), it is important to note that this information will remain available at the courthouse or court facility wherein access has been traditionally afforded. The working group believes there is a difference between maintaining “public” records for viewing/copying at the courthouse and “publishing” records on the Internet. Thus, there is certain information for which at the present time courthouse access remains the appropriate forum.

Concerning Subsection A(2)'s restriction on remote access to information that identifies jurors, witnesses, and victims in criminal cases, similar provisions have been implemented by other jurisdictions, including Alaska (AK R ADMIN Rule 37.8(a)(1) and
(2)), Indiana (Ind. St. Admin. Rule 9(G)(1)(e)), Mississippi (Administrative Order dated August 27, 2008 paragraph 8), Nebraska (NE R CT § 1-808(b)(3)), Texas (TX ST J ADMIN Rule 12.5(d)) and Utah (UT R J ADMIN Rules 4-202.02(8)(e) and 4-202-03(7)).

As pertains to Subsection A(5), in considering family court records (i.e. divorce, custody, and support), the working group is cognizant that individual courts have implemented protocols to shield some of these records from access. Some suggest that these cases are essentially private matters involving painful recollections of failed family relationships and hence are “nobody’s business.” Sensitive to these concerns, the working group believes that prohibiting online posting of any family court records (save for a docket, court orders and opinions), along with the requirements that certain information and documents filed with the court or custodian be shielded from access via the use of a Confidential Information Form, redacted filings and/or a Confidential Document Form, removes a significant amount of the personal, sensitive information from access, while allowing public access to ensure accountability and transparency of the judicial system.

With regard to Subsection A(6), the working group noted that New Mexico has a similar protocol protecting Older Adult Protective Services Act matters (NMRA Rule 1-079(c)(4)). For the reasons expressed above, the working group proposes remote access to dockets, court orders and opinions in these cases, to the extent that the judicial districts have developed systems and procedures that facilitate such access.

It is essential that courts and/or custodians in designing systems, such as those for document imaging and/or e-filing, give ample consideration to the requirements of this policy and ensure such systems are in compliance. This is imperative as the Judiciary moves toward statewide e-filing for all levels of courts.

As for systems currently in existence, the working group recognizes that this policy may require changes to current protocols and processes. Thus, as noted earlier, a delayed implementation date will be recommended to allow for necessary adjustments.

SECTION 11

The working group noted with favor a similar provision included in the Electronic Policy. The working group proposes that this policy should also delineate a procedure by which an individual may correct a clerical error that appears in a case record accessible remotely. As noted in the Explanatory Report to the Electronic Policy, these provisions borrow heavily from the correction provisions in the Criminal History Record Information Act. The working group was persuaded, for the same reason outlined in the Explanatory Report, that a similar protocol should be included in this policy.
OTHER COMMENTS

During the course of its deliberations, the working group identified various ancillary recommendations that merit consideration. Some are directly related to the policy provisions, while others may be categorized as "best practices" that should be considered by the courts and practitioners. Overall, these recommendations are intended to promote the successful implementation of this proposed policy.

1. The working group recommends the establishment of an ad hoc committee to monitor the implementation of this policy and to propose revisions to the policy necessitated by legal, technological and administrative changes.

2. The working group recommends that the Civil Procedural and Minor Court Rules Committees consider amending the rules setting forth the requirements for in forma pauperis petitions to remove the requirement that children’s full names appear on petitions and only require the minors' initials on the forms. This will ensure compliance with the restriction of Section 7.0(A)(5). The relevant rules are Pa.R.C.P. 240(h) and Pa.R.C.P.M.D.J. No. 206(E)(vi).

3. The working group recommends that the Appellate Procedural Rules Committee consider a protocol permitting the extension of a protective order issued by a lower court during the pendency of an appeal. For example, parties may be granted a certain time period within which to file a new application for protective order; such a protocol may also address whether certain court personnel are exempted, perhaps at the discretion of the court. In addition, instituting a methodology, automated or otherwise, by which the lower court signals to the appellate court that it issued an order to seal, is also recommended. See also MI R ADMIN Rule 8.119(D)(Michigan).

4. The working group recommends that the courts, AOPC and rules committees remain cognizant of this policy as they develop e-filing and case management systems, procedures and forms in the future. It may be helpful to litigants and practitioners to include mention of this policy on pertinent forms, as was done by the AOPC for the criminal, civil and landlord-tenant complaint forms when the MDC Paper Policy was adopted. In addition, the following "best practices" should be considered as courts develop systems for e-filing:

   a. Access to the courts should be promoted by the e-filing processes;
   b. Court control over its own records should be preserved;
   c. Systems should have consistent functionality, compatible protocols and rules to facilitate statewide practice;
   d. Processes for pro se litigants should be defined to provide equal and secure access to the system;
   e. Issues involving public access to e-documents, and the sensitive data that may be contained therein, should be fully studied before the e-filing system is developed;
f. Payment of any required filing fees should be accomplished via electronic methods;
g. Bi-directional exchange of data should be facilitated between e-filing and case management systems; and
h. Maximum flexibility in the design of a system should be sought to accommodate future evolutions of technology.

5. In order to facilitate online access to case records, courts and custodians should procure software to ensure sensitive data is appropriately redacted. While this proposed policy puts the onus on parties and their attorneys for redacting specified information, the working group considers implementation of redaction software to be a "best practice" and perhaps a necessity for those courts and custodians that intend to post records online, especially those records that pre-date the policy's effective date. This best practice has already been adopted by a number of judicial districts and further safeguards the publication of sensitive data, like that outlined in Section 7.0.

6. As previously expressed, the working group regards education as an essential component to the successful implementation of this policy. As officers of the court, attorneys must familiarize themselves with and heed the UJS's public access policies, particularly given the certification of compliance required by Sections 7.0(D) and 8.0(D). The working group noted the amendments to the commentary to Rule of Professional Conduct 1.1 pertaining to technology:

   To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject (emphasis added).

It may be advisable for the Rules of Professional Conduct to provide additional guidance to attorneys regarding their special responsibility in protecting their clients' sensitive information and documents, in addition to being informed about other technological matters, such as meta-data in e-filed documents.

7. The working group advises that technology and internal procedures may assist the courts and custodians with complying with this proposed policy and the Judiciary's commitment to open records.

   a. It is recommended that application of "optical character recognition" (OCR) software be employed. OCR software facilitates the search and retrieval of documents, as well as "copy and paste" of text that may be helpful for attorneys.

   b. It is recommended that exhibits should be separately e-filed from pleadings and other legal papers to easily safeguard those that are
restricted pursuant to policy or subject to an order to seal from public view. Relatedly, as pertains to the preparation of a transcript, it is recommended that the Rules of Judicial Administration require that a list of exhibits appear at the beginning of the transcript.

c. Due consideration and routine review should be given to the standards for record retention as applied to those in paper form and electronic form by records custodians.
### LIMITS ON PUBLIC ACCESS TO UNIFIED JUDICIAL SYSTEM CASE RECORDS OF THE APPELLATE AND TRIAL COURTS

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Record Description</th>
<th>Accessibility</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal</td>
<td>Sealed affidavit of probable cause for a search warrant.</td>
<td>No Public Access while sealed. The affidavit may not be sealed for more than 60 days unless an extension is received. Extensions may not be longer than 30 days, but an unlimited number of extensions are available. Public may access the affidavit after it has been unsealed.</td>
<td>Pa.R.Crim.P. 211.</td>
</tr>
<tr>
<td>Criminal</td>
<td>Arrest Warrant Information.</td>
<td>A court may delay public access for good cause for up to 72 hours. In addition, a court may seal arrest warrant information for a longer period of time.</td>
<td>Pa.R.Crim.P. 513(C), Pa.R.Crim.P. 513.1</td>
</tr>
<tr>
<td>Criminal</td>
<td>Motion filed by attorney for the Commonwealth to present the matter to an indicting grand jury and subsequent order.</td>
<td>No Public Access - the motion and order are sealed.</td>
<td>Pa.R.Crim.P. 556.2.</td>
</tr>
<tr>
<td>Subject Area</td>
<td>Record Description</td>
<td>Accessibility</td>
<td>Authority</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
<td>---------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Criminal</td>
<td>Sealed written statements pertaining to protective orders.</td>
<td>No Public Access. The entire text of the statement shall be sealed and preserved in the records of the court to be made available to the appellate court(s) in the event of an appeal.</td>
<td>Pa.R.Crim.P. 573(F).</td>
</tr>
<tr>
<td>Criminal</td>
<td>Juror information questionnaires.</td>
<td>No Public Access. Questionnaires are retained in a sealed file and shall be destroyed upon completion of the jurors' service, unless otherwise ordered by the trial judge.</td>
<td>Pa.R.Crim.P. 632(B),(C),(F),(G).</td>
</tr>
<tr>
<td>Criminal</td>
<td>Records revealing the names of human trafficking victims.</td>
<td>No Public Access, unless otherwise ordered by a court in a prosecution involving a victim of human trafficking.</td>
<td>18 Pa.C.S. § 3019(a).</td>
</tr>
<tr>
<td>Criminal</td>
<td>Wiretap applications, final reports and orders.</td>
<td>No Public Access except upon showing of good cause before a court of competent jurisdiction.</td>
<td>18 Pa.C.S. § 5715.</td>
</tr>
<tr>
<td>Subject Area</td>
<td>Record Description</td>
<td>Accessibility</td>
<td>Authority</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Criminal</td>
<td>Names of minor victims of sexual or physical abuse.</td>
<td>No Public Access. Records revealing a victim's name are sealed. A minor victim who is 18 years of age or older at the time of the commencement of the prosecution may waive this protection and allow the court to release the name of the minor victim.</td>
<td>42 Pa.C.S. § 5988.</td>
</tr>
<tr>
<td>Domestic Relations</td>
<td>Information regarding the registration, filing of a petition for, or issuance of a protection from abuse in either the issuing or enforcing State.</td>
<td>No Public Access via internet publication, if such publication would be likely to publicly reveal the identity or location of the protected party.</td>
<td>18 U.S.C. § 2265(d)(3).</td>
</tr>
<tr>
<td>Domestic Relations</td>
<td>Social security number of any individual subject to a divorce decree, support order, paternity determination, or acknowledgement of paternity, which is required in all records of those matters.</td>
<td>No Public Access.</td>
<td>23 Pa.C.S. § 4304.1(a)(3).</td>
</tr>
</tbody>
</table>
Domestic Relations

(a) Subject to any inconsistent general rules and to the supervision and direction of the court, the domestic relations section shall have the power and duty to:

(10) Implement safeguards applicable to all confidential information received by the domestic relations section in order to protect the privacy rights of the parties, including:

(ii) prohibitions against the release of information on the whereabouts of one party or the child to another party against whom a protective order with respect to the former party or the child has been entered; and

(iii) prohibitions against the release of information on the whereabouts of one party or the child to another person if the domestic relations section has reason to believe that the release of the information may result in physical or emotional harm to the party or the child.

No Public Access.

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Record Description</th>
<th>Accessibility</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domestic Relations</td>
<td>List of weapons ordered to be relinquished by the defendant in an action for protection from abuse.</td>
<td>No Public Access, except (A) upon an order of the court granted upon cause shown; (B) as necessary, by law enforcement and court personnel; or (C) after redaction of information listing any firearm, other weapon or ammunition.</td>
<td>23 Pa.C.S. § 6108(a)(7)(v).</td>
</tr>
<tr>
<td>Domestic Relations</td>
<td>All records pertaining to a confidential address for individuals participating in the Office of Victim Advocate's Address Confidentiality Program.</td>
<td>No Public Access, except for the substitute address provided by the Office of Victim Advocates.</td>
<td>23 Pa.C.S. § 6703(d); see also 23 Pa.C.S. § 5336(b)(2).</td>
</tr>
<tr>
<td>General</td>
<td>Records concerning persons in treatment under the Mental Health Procedures Act.</td>
<td>Limited Public Access in compliance with the Mental Health Procedures Act and controlling case law.</td>
<td>50 P.S. § 7111.</td>
</tr>
<tr>
<td>General</td>
<td>Court documents, rules, or orders in Gaming Law proceedings.</td>
<td>Any party may request proceeding and record to be sealed if in best interest of any person or Commonwealth.</td>
<td>4 Pa.C.S. § 1518.2(b).</td>
</tr>
<tr>
<td>General</td>
<td>Proceedings and records involving juveniles charged with a summary offense before the minor judiciary, the Philadelphia Municipal Court or a Court of Common Pleas.</td>
<td>No Public Access.</td>
<td>42 Pa.C.S. §§ 6303(c), 6307(c), and 6336(g).</td>
</tr>
<tr>
<td>Subject Area</td>
<td>Record Description</td>
<td>Accessibility</td>
<td>Authority</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
<td>---------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Orphans' Court</td>
<td>Proceedings related to appointment of guardianship for incapacitated persons.</td>
<td>Shall be closed to the public upon request of the alleged incapacitated person or his counsel. After the individual's death his/her estate may access the record of the guardianship proceedings.</td>
<td>20 Pa.C.S. § 5511(a); <em>In re Estate of DuPont</em>, 2 A.3d 516 (Pa. 2010).</td>
</tr>
<tr>
<td>Orphans' Court</td>
<td>Records required for foreign adoption decrees.</td>
<td>No Public Access unless a court order is granted upon good cause.</td>
<td>23 Pa.C.S. § 2908(F); Pa.OC.R. 15.7.</td>
</tr>
<tr>
<td>Orphans' Court</td>
<td>Adoption records.</td>
<td>No Public Access unless otherwise ordered.</td>
<td>23 Pa.C.S. § 2915; see also 23 Pa.C.S. § 2906; Pa.OC.R. 15.7.</td>
</tr>
<tr>
<td>Orphans' Court (Family Court in Philadelphia County or Juvenile Court Section of Family Division in Allegheny County Pa.R.J.A. 2157)</td>
<td>Applications of a minor for judicial approval of decision to have an abortion, under the Abortion Control Act, as well as proceedings and the name of the minor.</td>
<td>No Public Access; sealed dockets, and documents shall be maintained in a closed file marked &quot;confidential&quot; and identified by case number only.</td>
<td>Supreme Court Orphan's Court Rule 16.6.</td>
</tr>
</tbody>
</table>

*Note this may not be a complete listing; the public and court staff are directed to consult federal and state statutes, court rules or case law.