EXPLANATORY REPORT

CASE RECORDS PUBLIC ACCESS POLICY OF THE UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA

GENERAL INTRODUCTION

Recognizing the importance of the public's access to the courts and with the Supreme Court's approval, the Administrative Office of Pennsylvania Courts (AOPC) has developed statewide policies governing access to court records. 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 implementation of e-filing in Pennsylvania's appellate courts and future initiatives at other court levels 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, for instance: 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, 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

[1] See *Commonwealth v. Long*, 922 A.2d 892 (Pa. 2007).
[2] Explanatory Report is found at: http://www.pacourts.us/assets/files/page-381/file- 833.pdf?cb=1413983484884

are restricted 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.

The working group published its proposal for a 60-day public comment period[3] and received thirty-two submissions. The comments reflected diverse, and sometimes conflicting, viewpoints, which helped the working group define the issues and find solutions. In doing so, the working group endeavored to find as much "common ground" as it could in reviewing and addressing the various comments.

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. *Commonwealth v. Fenstermaker*, 530 A.2d 414, 417 (Pa. 1987) (citing *Commonwealth v. Contankos*, 453 A.2d 578, 579-80 (Pa. 1982)).

However, the group also recognized that transparency of judicial records and proceedings must be balanced with other considerations in this Internet age. The group attempted 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 policy.

SECTION 1

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

This policy governs access to (1) official paper case records of appellate courts, courts of common pleas, Philadelphia Municipal Court, and magisterial district courts, (2) images of scanned or e- filed documents residing in the three statewide case management systems, (3)

[3] http://www.pabulletin.com/secure/data/vol45/45-6/222.html

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 approach ensures a more equitable and systematic approach to the case records filed in and maintained for the trial and appellate courts.

It is important to note how this policy intersects with the *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania* (hereinafter referred to as "*Electronic Policy*") as well as the recently rescinded *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"). 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* had governed access to the paper case records on file in a magisterial district court, but was rescinded when this Policy was amended in 2018 to govern public access to those records.

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

This section's provisions are similar to those contained in the rescinded *MDC Paper Policy,* which had been successfully implemented.

SECTION 4

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 the administration of justice or the orderly operation of a court, pursuant to Section 2.0(C).

This section's provisions are similar to those contained in the rescinded *MDC Paper Policy*.

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 must respond to requests. Both the *Electronic Policy* and the rescinded *MDC Paper Policy* contained similar sections.

SECTION 6

Judicial districts have adopted 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 dockets sheets were accessed online.

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), judicial districts should ensure that fees do not become a barrier to public access. Completion of statewide case management systems in all levels of court will likely bring about standardization in remote access to case records.

The working group notes that this section's provisions are similar to those contained in the rescinded *MDC Paper Policy.*

SECTION 7

The concept of restricting access to particular, sensitive identifiers is not novel. The *Electronic Policy* and the rescinded *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.

The *Electronic Policy* and the rescinded *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)(3)), 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 *Electronic Policy* and the rescinded *MDC Paper Policy* provide that this information is not 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)(3)), 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), 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 *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), 75 Pa.C.S. § 6114, 18 U.S.C. §§ 2721 – 2725, 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 SID. Furthermore, in *Warrington Crew v. Pa. Dept. of Corrections*, (Pa. Cmwlth., No. 1006 C.D. 2010, filed Nov. 19, 2010)[4], 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.

Other jurisdictions provide similar protections to minors' names, dates of births, or both. 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)(l) 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 whereby 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)).

To maintain 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 rescinded *MDC Paper Policy*.

[4] Pursuant to Section 414(a) of the Commonwealth Court's Internal Operating Procedures, an unreported panel decision issued by the Court after January 15, 2008 may be cited "for its persuasive value, but not as binding precedent." 210 Pa. Code § 69.414(a).

Alternatively, parties and their attorneys can 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 in a visibly evident manner, 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 was also identified as a more amenable solution given the current design of the statewide e-filing initiative.

This option is not applicable to filings in a magisterial district court, rather filers must use the Confidential Information Form as provided in subsection (A). However, most of the forms that are found within the case files of a magisterial district court are statewide forms that are generated from the Magisterial District Judge System (a statewide case management system for these courts). The protection of confidential information captured on current MDJS forms requires a multi-faceted approach that takes into account how each form that contains such information is used. For example, AOPC has removed or suppressed social security numbers and operator license numbers from various forms when such information is extraneous to the court's adjudication of the case or the collection of the information is not otherwise required. In some instances, the filer will be responsible for placing the confidential information on the Confidential Information Form.

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. This provision, however, does not alter or expand upon existing legal authority limiting a custodian's authority to reject a document for filing. *See Nagy v. Best Home Services, Inc.*, 829 A.2d 1166 (Pa. Super. 2003).

Courts that permit e-filing should consider the development of a compliance "checkbox" whereby e-filers could indicate their compliance with this policy.

This section only applies to documents filed with a court or custodian on or after the effective date of this policy. There will be a period of transition prior to full implementation of this policy; that is, some documents filed with a court or custodian prior to the effective date of this policy will contain information that the policy restricts from public access. To expect full and complete implementation of this policy by applying it retroactively to those documents filed prior to the effective day of this policy is impractical and burdensome.

However, it is important to remember with regard to pre-policy records, a party or attorney always has the option to file a motion with a court of record to seal, in whole or part, a document or file. This includes the ability to request sealing and/or redaction of only some information that resides on a document in the court file (e.g., a social security number on a document).

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)). 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, 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 (VT R PUB ACC CT REC § 6(b)(17)), West Virginia (WV R RAP Rule 40(e)(1)) and Wyoming (WY R Gov Access Ct Rule 6(t)).

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's 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*, 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(p)).

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)).

The extent of financially sensitive information required by Pa.R.C.P. No. 1910.27(c) and 1920.33 that must be listed on income and expense statements, marital property inventories and pre-trial statements rivals information contained in a financial source document. Therefore, these documents should also be treated as confidential. Vermont has a similar protocol (VT R PUB ACC CT REC § 6(b)(33) and 15 V.S.A. § 662).

Courts that permit e-filing should consider the development of a compliance "checkbox" whereby e-filers could indicate their compliance with this policy.

This section only applies to documents filed with a court or custodian on or after the effective date of this policy. There will be a period of transition prior to full implementation of this policy; that is, some documents filed with a court or custodian prior to the effective date of this policy will contain information that the policy restricts from public access. To expect full and complete implementation of this policy by applying it retroactively to those documents filed prior to the effective day of this policy is impractical and burdensome.

However, it is important to remember with regard to pre-policy records, a party or attorney always has the option to file a motion with a court of record to seal, in whole or part, a document or file. This includes the ability to request sealing and/or redaction of only some information that resides on a document in the court file (e.g., a social security number on a document).

SECTION 9

This section safeguards certain sensitive information that is already protected by existing authority or was deemed to require protection by the working group from access at the court facility. The latter category included two specific types of records: birth records and incapacity proceeding records.

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. 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, dockets and any court order, decree or judgment in these cases are exempted by the policy. 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.

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, these records are not be accessible. 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 case docket and any court order, decree or judgment for these cases is exempted pursuant to this policy.

The provisions of Subsection G are consistent with those contained in the *Electronic Policy*, the rescinded *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 where access has been traditionally afforded. 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 provision exist in the *Electronic Policy* and 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), individual courts have implemented protocols to shield some of these records from access. Sensitive to these concerns, 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 restricted from access via the use of a Confidential Information Form, redacted filings 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), New Mexico has a similar protocol protecting Older Adult Protective Services Act matters (NMRA Rule 1-079(c)(4)). For the reasons expressed above, remote access should be afforded 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.

While case records remotely accessible to the public prior to the effective date of this policy may remain online in unredacted form, judicial districts are not prohibited from taking steps to safeguard sensitive case records designated by this section. To expect full and complete implementation of the policy by applying it retroactively to records remotely accessible prior to the effective date of this policy is impractical and burdensome.

However, it is important to remember with regard to pre-policy records, a party or attorney always has the option to file a motion with the court to seal, in whole or part, a document or file. This includes the ability to request sealing and/or redaction of only some information that resides on a document in the court file (e.g., a social security number on a document).

It is essential that courts and custodians in designing systems, such as those for document imaging, e-filing, or both consider 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 policy may require changes to current protocols and processes.

SECTION 11

A similar provision is included in the *Electronic Policy.* This policy delineates 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. For the same reasons outlined in the *Explanatory Report*, a similar protocol was included in this policy.

BEST PRACTICES

The following are various "best practices" that should be considered by the courts, parties and their attorneys to promote the successful implementation of this policy.

1. The Judiciary should remain cognizant of this policy in the development of e- filing and case management systems, procedures and forms. 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 (e.g., separate e-filing of exhibits from other documents);
    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.

2. Compliance with this policy and the Judiciary's commitment to open records may be assisted by various technological and administrative solutions, such as:

    a. Implementation of redaction and "optical character recognition" software may assist parties and their attorneys in complying with the policy. Some judicial districts also employ redaction software to protect sensitive data as a "best practice."
    b. Due consideration and routine review by custodians should be given to the standards for record retention as applied to those records in paper form and electronic form.