New Jersey Courts
Independence • Integrity • Fairness • Quality Service

Administrative Office of the Courts

GLENN A. GRANT, J.A.D.
Acting Administrative Director of the Courts

www.njcourts.com • phone: 609-984-0275 • fax: 609-984-6968

Directive # 01-14

To: **Hon. Carmen Messano**
Assignment Judges
Hon. Patrick DeAlmeida
AOC Directors and Assistant Directors
Clerks of Court
Trial Court Administrators

From: **Glenn A. Grant, J.A.D.**

Date: **February 6, 2014**

Subj: **Electronic Records Management Guidelines**

This directive promulgates the attached Electronic Records Management Guidelines (ERM Guidelines), to be effective immediately.

The ERM Guidelines, as approved by the Supreme Court, establish minimum requirements for the creation, utilization, maintenance, retention, preservation, storage and disposal of electronic records maintained in Judiciary applications. The purpose of the ERM Guidelines is to ensure that records contained in the Judiciary's systems, whether in the form of images or data, and whether for the purpose of case processing or court administration, are legally acceptable, authentic, accessible, secure, and properly retained until such time as they should be destroyed.

Please share the ERM Guidelines with your judges and managers. Questions or concerns regarding the ERM Guidelines may be directed to Michelle M. Smith, Superior Court Clerk, by phone at 609-984-4200 or by email at michelle.smith@judiciary.state.nj.us.

G.A.G

Attachment (ERM Guidelines)

cc: Chief Justice Stuart Rabner
Steven D. Bonville, Chief of Staff
Directors, Dedicated Funds
Jennifer M. Perez, Chief, ATCSU
Gurpreet M. Singh, Special Assistant
Mary B. Patterson, Assistant Chief, SCCO
ATCAs/Operations Managers

NEW JERSEY JUDICIARY GUIDELINES FOR ELECTRONIC RECORDS MANAGEMENT IN INFORMATION TECHNOLOGY SYSTEMS DEVELOPMENT ("ERM GUIDELINES")

Promulgated by Directive #01-14
(as approved by the Supreme Court)

February 6, 2014

Introduction

The purpose of this document is to set forth guidelines for the development and enhancement of information technology systems used in the management of cases or the administration of judiciary business. These guidelines establish minimum requirements for the creation, utilization, maintenance, retention, preservation, storage and disposition of the electronic records that are collected and maintained in judiciary applications. Our core values of independence, integrity, fairness and quality service could not be achieved without attention to the preservation of records. Sound policies and procedures, such as those set forth in these guidelines, ensure the trustworthiness and credibility of our records and provide transparency and accessibility to the judicial branch of government.

The Supreme Court, in its adoption of Rule 1:38 (Public Access to Court Records and Administrative Records), has recognized that both court and administrative records constitute vital documentation of decisions made, policies promulgated and actions taken. In fact, Rule 1:38-2 broadly defines a "court record" as including:

> (1) any information maintained by a court in any form in connection with a case or judicial proceeding, including but not limited to pleadings, motions, briefs and their respective attachments, evidentiary exhibits, indices, calendars, and dockets;
>
> (2) any order, judgment, opinion, or decree related to a judicial proceeding;
>
> (3) any official transcript or recording of a public judicial proceeding, in any form;
>
> (4) any information in a computerized case management system created or prepared by the court in connection with a case or judicial proceeding;
>
> (5) any record made or maintained by a Surrogate as a judicial officer.

In addition, Rule 1:38-4 broadly defines an "administrative record" as including "[a]ny information maintained in any form by the judiciary that is not associated with any particular case or judicial proceeding." Since the Court has broadly defined judiciary records to include any and all information maintained by the judiciary in any format, a system or application used to conduct either case management or administrative functions essentially contains and constitutes the court's "record."

The Court's authority to manage judiciary records is set forth in N.J.S.A. 2B:1-2 (Preservation of Court Records), which provides that "[t]he Supreme Court may adopt regulations governing the retention, copying and disposal of records and files of any court or court support office." The regulation of records by the Court is governed by Rule 1:32-2 (Books and Records) and Rule 1:32-2A (Electronic Records, Electronic Filing,

and Electronic Court Systems). These Rules are together broad in scope in order to address records in any medium:

Rule 1:32-2 (Books and Records)

> **(a) Recordkeeping by Clerk.** The clerks of all courts shall keep such books and records and may microfilm or electronically retain or destroy the same as the Administrative Director of the Courts with the approval of the Chief Justice may prescribe.
> **(b) Municipal Court Books and Records.** Judges or presiding judges of the municipal court shall be responsible for the keeping of such prescribed books and records for the municipal courts.
> **(c) Retention Schedules and Purging Lists.** Retention schedules identifying the length of time court records must be kept prior to destruction and purging lists identifying documents to be removed from case files before storage or replication shall be adopted by administrative directive. For purpose of this rule, "purging" means the removal and destruction of documents in the case file which have no legal, administrative or historical value.
> **(d) Reproduction of Original as Evidence.** In the event of any destruction or other disposition of court records pursuant to this rule, the photographic or electronic reproduction or image of the original or a certified copy of same shall be receivable in evidence in any court or proceeding and shall have the same force and effect as though the original public record had been there produced and proved.

Rule 1:32-2A. (Electronic Records, Electronic Filing, Electronic Court Systems)

> **(a) Authorization of Electronic Court Systems.** The Administrative Director of the Courts, with the approval of the Chief Justice, may develop and implement electronic court systems, including applications or systems for the purpose of electronic filing, electronic record keeping, or electronic indexing of data and documents.
> **(b) Force and Effect of Data and Documents Submitted or Maintained Electronically.** Data and documents, whether originating in paper or digital form, submitted electronically to the clerks of court or maintained electronically by the clerks of court in a system or application authorized pursuant to this rule shall have the same force and effect as data and documents maintained by the clerks of court in an original paper format.
> **(c) Electronic Signatures.** Where an electronic system or application has been authorized pursuant to this rule, and where the system or application is secured by an authentication method in accordance with the protocols established and approved by the Administrative Director of the Courts, an electronic signature shall have the same force and effect as an original handwritten signature. Upon submission to the clerk of court, an electronically signed document shall not be deleted or altered in any manner without order of the Court for good cause.

Although the judiciary continues to conduct court business in a paper environment, case and administrative records increasingly originate in electronic form, and existing paper records can be more easily digitized. The organization has already realized worthwhile efficiencies by capturing, storing, retrieving, and sharing electronic records. Through the use of digital imaging systems and data, we have seen a decrease in physical storage space requirements and an improvement in court and administrative operations.

Since any system or application used by the judiciary constitutes the court's record, the future of records management – electronic records management – seeks to manage data and digitized/imaged documents from creation, to access, use, storage, retention, migration and final disposition. In essence, we must ensure that the data and images contained in all judiciary applications, whether court-related or administrative, will be properly secured, accessible, and preserved now and throughout their proper retention and destruction lifecycle. To accomplish this, consideration must be given to hardware and software configurations, multiple imaging components, regular migration of data and images, and documentation of record destruction in accordance with approved retention schedules.

The challenge of electronic records management is to balance our historical commitment to actively managing and preserving the court's record with our technological capability to quickly make records available electronically. When striking this balance, we cannot compromise planning and adherence to set procedure for the sake of expedient electronic access. Policies, processes, and technology must align and be applied from the point at which a system is upgraded or designed in order to accomplish the following:

(1) Guarantee the legal acceptability and reliability of judiciary records.

(2) Guarantee that the content of data and documents upon capture is secure, authentic and closely resembles the original without any material alteration.

(3) Guarantee the accessibility of electronic records for both general daily operations and emergent continuing operations plans.

(4) Guarantee that procedures and controls are in place to make available open records while securing those records that are confidential or exempt from public access in accordance with Rule 1:38.

(5) Guarantee the ongoing and future accessibility and usability of electronic records through routine migration of content and adherence to an approved destruction schedule for unnecessary records.

The goal is to make certain that the records contained in our systems, whether in the form of images or data, whether for the purpose of case processing or court administration, are legally acceptable, authentic, accessible, secure, and properly retained until such time as they should be destroyed.

Guideline #1:

Records retention and destruction schedules must be planned for at the inception of any new electronic systems or the revision of a legacy system.

When developing or updating a judiciary application, a plan for electronic records retention and disposal should be included and approved before implementation of the application. Pursuant to Rule 1:32-2(c), all records, including the data and images that make up electronic records, must be preserved and retained for the period required by the applicable Judiciary Records Retention Schedule. Preservation in the digital world means ensuring continuing access to high quality, eye-readable original source documents. Permanent records will require a well-developed migration strategy and the most diligent efforts to keep them accessible. As much contextual information as possible must be captured to ensure the historical meaning of the image is not distorted or compromised.

Records may be destroyed only in accordance with the retention schedules applicable to court and administrative records. At a minimum, the judiciary must make certain that electronic records scheduled for destruction are disposed of in a manner that ensures that any information that is confidential or exempt from disclosure, including proprietary or security information, cannot be read or reconstructed. Moreover, recording media previously used for electronic records containing information that is confidential or exempt from disclosure, including proprietary or security information, are not reused if the previously recorded information can be compromised in any way by reuse.

Guideline #2:

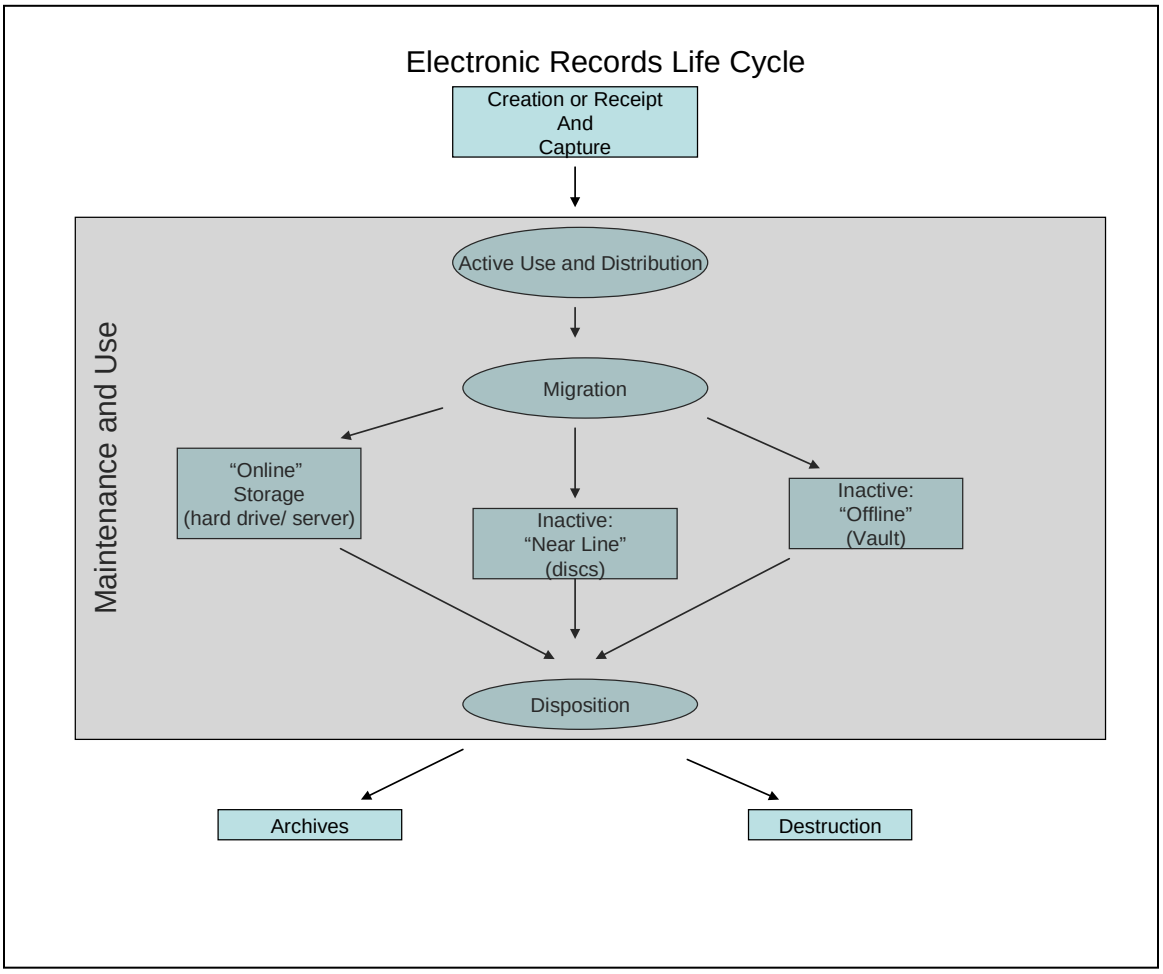
Consideration must be given to the electronic records life cycle.

A records life cycle is the life span of a record from its creation or receipt to its final disposition. It is usually described in three stages: (1) creation, (2) maintenance and use, and (3) final disposition. Creation is the point of origination of the records. Maintenance and use is the portion of the records life cycle in which the record is either in active use and frequently accessed, or is inactive and infrequently accessed and may be maintained off-line. The final stage of the records life cycle, final disposition, describes the ultimate fate of the record, including destruction, long-term retention, or permanent retention.

It should be noted that electronic records have a more complicated lifecycle than non-electronic records because of the system issues associated with electronic records. For example, once a record is created, it must then be captured by either imaging the record or importing it electronically. Active use and distribution of the record requires a process of disseminating electronic information through automated means. The electronic record must be migrated, meaning the application must be able to transfer digital materials from one hardware/software configuration to another. Storage plans must include online storage, which allows information to be stored on hard drive or on a server; near-line storage, which allows information that is accessed less frequently to be stored on disks or

other medium that may not be immediately accessible; and off-line storage, which allows long-term electronic records to be preserved in a vault or some other secure location

The chart below details the phases to consider in a record's life cycle.



Source: The National Archives and Records Administration
"Electronic Records Management" Participant Guide
Revision January 2011, PG 1-10

Guideline #3:

The content of an original record or an electronically executed document must be secure and shall not be altered or enhanced.

Trustworthiness and credibility are the foundation of proper electronic records management, with the very authenticity of records being dependent on whether they have been maintained in the original format. The substance of a record received by the court or created by the court – whether that record consists of data or whether that record is an image – should not be altered in any way. Any modification to a record, whether data or image, must be accompanied by an audit history record that records the change, the author of the change, and the date/time of the change.

Data and images received by the court are both electronic records. As such, they are records that must be captured and stored at the point of creation and must not be alterable. Enhancement techniques utilized in many applications allowing users to modify and update documents in draft format must be restricted once a record is in its final format and committed to the docket or electronic records management system.

In addition, if data is used to create an image (such as a PDF), that image is a separate electronic record and, as such, it must be captured at the point of creation and must not be alterable. If there is a revision(s) to the data that would in turn revise the image, each version of the image must be captured, each version of the image must be unalterable, and, if the image itself is produced upon request from the data, each version of the image must be reproducible in the future.

The appearance of the electronic record when displayed or printed throughout its lifecycle must closely resemble the original without any material alteration. Digitized record enhancement techniques commonly used in scanning software cannot be used to alter the original content of the document.

Finally, if an electronic document is subject to redaction, a clear notation should be made indicating the content that was removed or blocked out. Techniques to hide content without notation should not be used.

Guideline #4:

The judiciary must have systems in place to track, audit, certify and secure an electronic signature based on a user ID and personal identification number/password.

Similarly, the judiciary must vigorously ensure the security and authenticity of electronic signatures, which by their very nature capture the intent and consent of the signer to approve a document and/or submit a document for filing. An electronic signature is defined by N.J.S.A. 12A:12-2 as "an electronic sound, symbol, or process attached to or

logically associated with a record and executed or adopted by a person with the intent to sign the record." In addition, N.J.S.A. 12A:12-9(a) provides that "[t]he act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable." Similarly, Rule 7:2-1 defines an electronic signature as "an electronic entry secured by a Personal Identification Number (hereinafter referred to as an electronic signature), which shall be equivalent to and have the same force and effect as an original signature."

To ensure authenticity, the execution of an electronic signature must be secured by a user ID and personal identification number/password that only the signer or designee can perform within the application. This provides the ability to identify, through a system audit or certification process, who signed the document and when the electronic signature was applied.

In addition, once a document has been executed with an electronic signature, any subsequent documents produced, if different, must clearly indicate that the document has been revised or amended. The original data and any changes to that record must be stored separately so that all versions can be reproduced as needed.

Finally, for case-related documents, the typed name or signature image of the electronic signer, as well as the date when the electronic signature was executed, should be included as part of any human readable display or printout so that this information is preserved as part of the record.

Guideline #5:

> **The accessibility to open records and security of confidential records must be considered and planned for at the inception of any new electronic systems or the revision of a legacy system.**

The judiciary has adopted a presumption of open access to court records. As stated in Rule 1:38-1, "[c]ourt records and administrative records as defined by R. 1:38-2 and R. 1:38-4 respectively and within the custody and control of the judiciary are open for public inspection and copying except as otherwise provided in this rule." Several categories of records are considered confidential under Rule 1:38, and systems should be designed to safeguard those records. Conversely, other records are considered open and accessible, and electronic access, where available, should be granted accordingly to the public through kiosks in a court's lobby or via the Internet to the court's website. Security concerns and relevant business policies must be considered in every project plan.

Whenever possible, personal identifiers as defined by Rule 1:38 should not be gathered by the judiciary. Where personal identifiers are present in judiciary records, either by necessity or by error, systems should be designed to allow for the redaction or removal of such record(s) if ordered to do so by the court. Moreover, an outline detailing plans to provide access to open records while restricting access to confidential, sealed or expunged records should be set forth in every project.

Guideline #6:

The judiciary must have systems in place to track, audit and certify the capture of an electronic record.

Maintaining the trustworthiness of electronic records is accomplished through internally established controls that document and report the ongoing functionality of the system, its integrity, and the management and resolution of system and risk incidents, according to established procedure, policies and standards. The records management industry *Standard for Information and Documentation – Records Management, Part 1: General (ISO 15489-1),* developed by the International Organization for Standardization (ISO), specifies that a record's trustworthiness is comprised of four characteristics:

1. **Authenticity** – An accurate account of an activity, transaction, or decision.
2. **Reliability** – Content can be trusted to be a full and accurate representation.
3. **Integrity** – Assurance that the information has not been subsequently changed.
4. **Usability** – The fact that the information can be located, retrieved, presented and interpreted.

The judiciary must develop and maintain adequate and up-to-date technical and descriptive documentation for each electronic recordkeeping system to specify characteristics necessary for reading or processing the records. Documentation for electronic records systems shall be maintained in electronic or printed form as necessary to ensure access to the records.

Guideline #7:

The minimum scanning resolution level must ensure that images are legible and readable compared to the source document.

Scanning resolution is measured in dots-per-inch (dpi). A higher resolution is generally necessary for those records intended for optical character recognition processing, or to produce a relatively legible text file. More detailed documents, such as maps or drawings may also require a higher resolution. The appropriate resolution level should be determined through testing so as to ensure that the results are compatible with the specific business needs of the particular judiciary application.

Guideline #8:

File formats must support long-term archiving and ensure the ability to migrate to future technologies.

The file format utilized in judiciary applications must ensure the ability to migrate to future technologies. The most common file formats currently used in digital imaging systems are tagged image file format (TIFF), portable document format (PDF), and joint photographic experts group (JPEG). The recommended format is PDF/A, which is the standard for long-term preservation of electronic documents adopted by ANSI (American National Standard for Information and Image Management) CGATS/AIIM/ISO (International Organization for Standardization 19005-1-2005) in autumn 2005. The PDF/A standard aims to enable the creation of PDF documents whose visual appearance will remain the same over the course of time. PDF/A files are software-independent and unrestricted by the systems used to create, store, and reproduce them.

Guideline #9:

Compression methods must support long-term archiving and ensure the ability to migrate to future technologies.

Image files are larger than text files and may need to be compressed for storage. Compressed image files must be decompressed for viewing and/or printing. Compression methods may be used to reduce the amount of data needed to store or transmit a representation of a specific image, and the selection of a compression scheme may be application specific. All images, however, must continually be displayed as was originally intended, with no change to format or content. All images must also be maintained and migrated for future use throughout the retention period.

Guideline #10:

The indexing method must adequately address all characteristics of the stored images, the requirements of the storage system, and end-user retrieval requirements.

The ability to retrieve an electronic record is entirely dependent on the index used to catalogue the records maintained in the system. The index is the directory that will be used to find the images once stored to the electronic system.

Indexes may take many forms, including databases, spreadsheets, full-text OCR, and file-naming conventions that help locate and present an image or series of images. The index for each application will depend on the metadata available, the characteristics of the record, the system requirements, and end-user retrieval requirements. Since electronic records must be retained and accessed over a number of years, the index must be developed and documented with future users in mind.

Information in the form of metadata is collected and used in the index to perform several key functions, such as the identification, management, access, use, and preservation of the digital resource. There are two thresholds for the information that must be captured in an index - one for electronically filed/captured records and a second for records scanned by judiciary staff or a contract vendor.

At a minimum, the following information must be captured for electronically filed/captured records:

(a) The case information, including docket number and any other additional identifiers required to be collected at the point of submission.
(b) The filer, creator, or author.
(c) The date and time the document or image was e-filed. This audit trail will provide greater authenticity and transparency.
(d) A standard coding system for different document types, if applicable.
(e) Whether it is an open, confidential, expunged, or sealed record and whether special access is needed to view the information.
(f) The data type (e.g., written document, photograph).

At a minimum, the following information must be captured for records scanned by judiciary staff or a vendor contracted to produce a scanned image:

(a) The case information, including docket number and any other additional identifiers required to be collected at the point of submission.
(b) The creator (vendor or operator who scanned it).
(c) The date and time the document or image was e-filed. This audit trail will provide greater authenticity and transparency.
(d) A standard coding system for different document types, if applicable.
(e) Whether it is an open, confidential, expunged or sealed record and whether special access is needed to view the information.
(f) The data type (e.g., written document, photograph).

Operating procedures should be developed to include an index check for accuracy at the time the index is created. Index entries shall be verified to ensure that records are accurately retrieved prior to destruction of any corresponding paper originals.

Guideline #11:

Records must be migrated to ensure accessibility and usability throughout the records retention period.

Electronic and digital storage media are subject to rapidly changing technologies and are often obsolete within a few years. For this reason, electronic and digital storage media

cannot satisfy long-term storage or preservation requirements unless a conversion and migration strategy for retaining and retrieving stored information is adopted.

Migration is the process of transferring digital information from one generation of hardware and software to the next. Currently, migration is the best practical means for retaining and retrieving electronic records over time. Migrations must be carefully planned, executed sequentially, and audited to ensure against data loss. In addition, the judiciary Information Technology Office must ensure that any new equipment or software replacing that used in an existing system is backward compatible and that the system will convert all data, images and indices to the new system so that access to existing electronic records is not interrupted or impeded.

Guideline #12:

> **Security, storage, and backup policies and procedures must be planned for at the inception of any new electronic system or the revision of a legacy system, and adhered to on a continuous basis.**

Full and regularly scheduled backup of electronic records and indexes is a critical operating procedure to ensure the protection of judiciary data as well as the credibility of the court's record. Backup storage should be off-site in a secure, environmentally controlled facility. In the case of a disaster, maintaining off-site copies of electronic records may be the only answer for recovering data.

Electronic Records Management must be a part of the Judiciary's comprehensive disaster management plan. The plan includes standard backup and recovery procedures as well as quality control and storage procedures such as those mentioned previously. The guidelines for the security controls and for the recovery of data are and must continue to be reviewed on a regular basis. Data recovery exercises must continue to be conducted on a periodic basis.