



Effective and Efficient Records and Information Management in the Digital Age

Karen Anne Perry
Department of the Treasury
Division of Revenue and Enterprise Services
Records Management Services
2025

Disclaimer: The content of this presentation is designed for educational and informational purposes only.

In the ever-evolving world of Digital, Cyber, Cloud, and AI Technologies, safe and effective Records and Information Management has become an uphill challenge, to say the least...

While these technologies provide rapid advancement in the tools available for Data Collection, Compilation, Distribution and Retention, Migration, Longevity and Access, they concurrently present threats ranging from Operational Discontinuity to Data Diffidence, Inaccessibility and/or Interoperability, Technological Obsolescence and the risk of Cyberattack.

Furthermore, the ongoing management of the implementation, maintenance, and optimization of **Minutes**, **Vital Records**, and **Electronic Health Record Systems** - ensuring data collection and compilation, accuracy and completeness, storage and access, and security.

With the objective being to safeguard your most valuable asset: **Information**.

Constituency

Federal, State, County/Municipal, Boards, Authorities, Schools, Colleges, etc.

The International, Global Arena – Government, Private Agencies, Citizenry, etc.

Unions, Associations, Lobby & Additional Groups

Legal Counsel

Healthcare - Facilities & Professionals

Financial Institutions & Auditors

Private Sector & Vendors

The Media – Print, TV/Cable, Radio, etc.

Internet & Social Media

Parents, Legal Guardians & Adult Pupils

Local Residents - Taxpayers

The General Public at Large



A Public Agency's Responsibilities to its Constituency

Promote Transparent, Seamless & Efficient Operations

Foster Positive Trust & Reputation

Verify the Data Fabric

Accurate Data Capture, Collection, Processing, Storage, Management, Retrieval & Delivery

Monitor Data Security

Enhanced Concerns - International, National & Local Levels of Government

Ensure Compliance

International, Federal, State, County & Municipal

Why should **We** be concerned?

It's The Law

- NJ Public Records Law
- Open Public Records Act (OPRA)
- Data Privacy, Compliance and Security Laws
- Litigation and e-Discovery Support
- Globalism: International, Federal and State
 - **European Union's *General Data Protection Regulation (GDPR)* & Regulation (EU) 2016/679** - Privacy and protection for processing of personal data;
 - ***Health Information Technology for Economic and Clinical Health Act (HITECH)*** - Health Information Technology and Electronic Health Records (EHR);
 - ***Health Insurance Portability and Accountability Act (HIPAA)*** - Personal medical information
 - **Family Education Rights and Privacy Act (FERPA)**
 - **Section 504 of the Rehabilitation Act of 1973** - Prohibits discrimination against students with disabilities
 - **Individuals with Disabilities Education Improvement Act (IDEIA)** – Ensures the right to a free appropriate public education (FAPE)
 - **NJAC 6A:22-3.3** – Student enrollment in a NJ Public School regardless of immigration status

It's The Law continued.

- **McKinney-Vento Act** – Protect the rights of children who are homeless
- **Plyer v. Doe US 202 (1982)** – Protect the rights of children to a public education whether residing legally or not
- **Title VI, Civil Rights Act (1964)** – Prohibits discrimination based on race, color or national origin
- **The Immigrant Trust Directive NJ Directive No. 2018-6** – NJ Law Enforcement may not stop, detain, question search or arrest an individual solely on suspected citizenship or immigration status
- **Children's Online Privacy Protection Act (COPPA)**
- **NJ Law Against Discrimination** – Prohibits discrimination and bias-based harassment which includes in a public school
- **NJ Data Privacy Law (NJDPL), PL 2023. c.266** - Personal data & its collection and processing

Personal Data

- Home address
- Driver's license
- Passport information, etc.

Consumer Rights

- Correct inaccuracies in their personal data
- Delete their personal data

Compliance

- Program Review
- Information Governance: Data Access & Migration
- Coding and Classification: medical diagnosis and procedure, billing & treatment
- Data Analytics: Identify trends, improve care, and foster research
- Audit: Financial & Programmatic - Relevance with Regulations & Standards
- Seamless & Efficient Government
- Positive Trust & Reputation
- Verify the Data Fabric
- Data Capture, Processing, Management & Delivery
- Monitor Data Security
- Enhanced Concerns on the International, Federal, State, County & Municipal

Cost Effective

- Minimize costs and promotes savings, efficiency and productivity.

Legacy Information

- Irreplaceable loss of intellectual rights, legacy records, etc.

Valuable Asset

- Establish Policies and Procedures - Health Data Governance with ongoing training.
- Data Quality and Accuracy - Ensuring the completeness, consistency, and accuracy of medical records to avoid compromised decision-making.
- Collaborative, seamless information exchange between the different systems, other departments, clinicians, administration and stakeholders.
- Loss, theft or damage can cause personal loss, financial loss, disrupt business operations, damage an agency's reputation resulting in loss of public confidence and trust.

NJ Data Privacy Law (NJDPL), PL 2023, c. 266

Effective Date: January 15, 2025

New Jersey Data Privacy Law (NJDPL)

Guarantees New Jersey Residents' rights in regard to their Personal Data and Sensitive Data and how it is being collected and processed by controllers.

Personal Data Identified

Home address, driver's license number, passport information, financial account number

Processing Personal Data

Concerns collecting, using, storing, disclosing, analyzing, deleting, or modifying.

Sensitive Data

Racial or ethnic origin; religious beliefs; health condition; financial information; sexual activity or sexual orientation; immigration or citizenship status; status as transgender or non-binary; genetic or biometric data; or precise geolocation data.

Processing Sensitive Data

Prior permission must be obtained to process Sensitive Data.

Rights

- Confirm whether a controller processes their data
- Correct inaccuracies in their personal data
- Delete their personal data

Records

PII vs. PHI

Personal Identifiable Information (PII) vs. Protected Health Information (PHI)

EMRs are typically utilized in a single practice or healthcare facility; whereas EHRs are to be shared among different healthcare providers and facilities as an electronic database of a Patient's Health History.

PII

Name, Date of Birth (DOB), Social Security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number, or credit card number, personal address information, email and personal telephone numbers

PHI

As denoted in HIPAA, Name, Geographics (street, city, or ZIP code), phone and fax numbers, Email addresses, Social Security Numbers, Medical record and health plan beneficiary numbers, Account numbers, Certificate/license numbers, Device identifiers and serial numbers, Web URLs and IP addresses, Biometric identifiers (fingerprints, voiceprints, etc.), Full-face photographs and any other unique code or identifier

Records

EMR vs. EHR

Electronic Medical Record (EMR) vs. Electronic Health Record (EHR)

EMRs are typically utilized in a single practice or healthcare facility; whereas EHRs are to be shared among different healthcare providers and facilities as an electronic database of a Patient's Health History.

EMR

Digital patient medical records that typically include but not limited to: chart clinical information collected during visits such as diagnoses, medications, lab test results, past medical history, visit summaries, demographic, insurance information, etc.

EHR

Database system of a comprehensive and standardized medical record from multiple sources, creating a comprehensive and accessible view of a patient(s) that can be shared across different healthcare settings, such as: hospitals, specialists and labs to foster the interoperability of information sharing, coordination of care, communication, research and trending public health reporting.

Encryption

PII, PHI, EMR, EHR

When collecting, maintaining and distributing information including PII, PHI, EMR and EHR, “end-to-end” in a database encryption should be utilized for the IT system and Business and Personal Data - especially due to the interoperability of the EHR.

IT

- Biometric Identifiers – Fingerprint, Iris Scan, Face/Voice
- Recognition
- Device Identifiers
- IP Addresses
- Facility Identification

Personal

- Home Address
- Email Address
- Financial Information
- Health Insurance Information
- Medical Record Numbers
- Names
- Passwords
- Phone Number(s)
- Social Security Numbers

Personal Identifiable Information - PII
Protected Health Information - PHI
Electronic Medical Record - EMR
Electronic Health Record - EHR

Something we never want to be accused of ...

Spoliation: The destruction of or failure to preserve evidence relevant to litigation or investigation.

Litigation Hold Order

As Public Servants, we have an obligation to preserve the Public Records in our custody – regardless of their medium. In the event of an OPRA Request or potential Litigation, a *Litigation Hold Order* must be issued and all **relevant Hardcopy, Digital and Electronic Information** should be immediately segregated and stored.

[NOTE: Attention must be given to e-mail, because their automated processes may have a function that routinely deletes e-mail if no action is taken. To avoid this, relevant e-mails should be placed in a separate folder.]

- A ***Notice of Acknowledgement*** should be distributed to the specific agencies indicating that they have been notified of the ***Litigation Hold Order***.
- The *Acknowledgement of Receipt* is to be signed and returned to the sender within five (5) days and **immediate** action should be taken in accordance with the **directives to segregate the associated records**.

Litigation Hold Order

For Discussion Purposes Only
Consult With Legal Advisors When Dealing With Litigation Hold Orders

SAMPLE

<date>

TO: <individual and/or custodian>

FROM: <issuing office>

SUBJECT: <subject or nature of the matter>

Please be advised that you are required to immediately preserve all documents and electronic data related to the above-noted matter. Your failure to do so could result in significant penalties.

<Agency> has received the above-captioned complaint and a copy is attached. We have identified you as a <custodian or individual> who may have potentially relevant paper records (e. g. memoranda, letters, pictures) or electronically stored information (e. g. e-mails, other electronic communications such as word processing documents, spreadsheets, databases, calendars, telephone logs, Internet usage files and network access information) or authority over such records.

You must immediately take every reasonable step to preserve this information until further notice.

Your failure to do so could result in significant penalties against us.

Acknowledgement of Receipt

For Discussion Purposes Only
Consult With Legal Advisors When Dealing With Litigation Hold Orders

RE: <subject or matter>

I, <individual or custodian>, acknowledge that I have received the <date of notice> notice regarding the above-captioned matter from <representative> advising me of my obligation to conduct a reasonable search for any documents, whether stored in hard copy or electronically, that may be relevant to the matter and to take reasonable steps to ensure the preservation of those documents.

I understand the instructions contained in the memorandum.

Signature

Name

Date

Note: If you do not understand the instructions, prior to completing this acknowledgement, you should contact <representative> at <___>-<___-___> with any questions you may have regarding either 1) what documents might be relevant to the above matter or 2) what actions you are reasonably expected to take in order to conduct a reasonable search for and preserve any documents, whether stored in hard copy or electronically, that may be relevant to the above matter.



AUDIT

FINANCIAL & PROGRAMMATIC STRATEGIES

Audit

Objective: Transparency in Good Records Governance

Penalties: The unlawful and deliberate alteration, destruction or falsifying of records

Retention: Electronic, Digital, Hardcopy and Cloud Storage Records

IT Security:

- **Prevent Data Breaches**
- **Access** - Physical & Electronic controls to prevent unauthorized access.
- **Data Backup & Migration** - Protect sensitive data onsite and offsite.
- **Change Management** – Document new employee access, hardware, software, database updates; and infrastructure changes; etc.

The Value of NJ Public Records

Value of Public Records

Public records are evidence of taxes paid, services rendered and obligations met. These records are crucial to the organization of our society and essential to the daily operation of government.

- The value of some records endure beyond their active use, because they provide unique evidence of significant actions and transactions that have affected the public.

Legal Framework

Public records are public property and are held in trust for citizens. Accordingly, public officials must ensure that records are protected from unauthorized alteration, defacement, transfer, destruction, being seized or cyberattacked.

- This is accomplished through compliance with New Jersey's Public Records Law (N.J.S.A. 47), the State's Records Management Statute (N.J.S.A 47:3-15 et seq.) and Administrative Rules (under N.J.A.C. Title 15:3 et seq.) which enact the standards and procedures mandated by the Law. Agency-specific Statutes and Administrative Rules have impact upon a public agency's records management responsibilities.

Destruction of Public Records Act

PL 1953, c. 410

What is a Public Record?

Destruction of Public Records Act (PL 1953, c. 410): Defines a Public Record as “Information, regardless of its medium (hardcopy, microform, digital, electronic & Internet-based) that is created, received, maintained and distributed by a public agency receiving taxpayer dollars and serves as Evidence of the Transactions of its Normal Course of Business.”

Title 47 , N.J.S.A. 47:1A-1.1., OPRA: Defines a Government Record as “All records that are made, maintained, kept on file, or received in the course of official business.”

In New Jersey, "Public" Can Have Two (2) Meanings

Ownership

As previously stated, a record is Public when it is evidence of the normal course of business of a Public Agency which receives a substantial contribution of tax dollars to conduct its activities.

Access

The *Open Public Records Act (OPRA)*/PL 2001, c. 404, PL 2024, c. 16, NJSA 47:1A *et seq.*, provides that public records must be accessible. However, because of issues of Privacy, Confidentiality & Security, an agency may restrict access to records:

In New Jersey, "Public" Can Have Two (2) Meanings continued...

Records Access

- OPRA Requests
- Common Law Requests
- Discovery Requests
- Administrative Requests
- Informal Requests
- Subpoenas, Court Orders, etc.

Records Inventory



In the event of an OPRA Request, Litigation, Audit or e-Discovery, a records inventory can be invaluable - documenting paper, digital, web-based and micro-formed records.

The inventory lists record type, volume, record storage location, classification, retention periods, disposition and applicable Federal and State Laws.

Records Inventory continued.

Format –

Paper Records that are also Microfilmed, Imaged, Electronic, Digital, etc.

Electronic Records - indices, input/output, data, etc. should also be identified.

Key to identify the records to safeguard in the event of OPRA, Audit, Litigation, and notably Cyberattack.



Records Retention & Disposition

PL 1953, c. 410/NJSA 47

Records Management Services (RMS)

As per NJSA 47, the Government Agency statutorily-entrusted with the creation of Records Retention Schedules and authorizing Request and Authorization for Records Disposals for EXPIRED* Public Records.

Records Retention Schedules: In accordance with the New Jersey Public Records Laws PL 1953, c. 410 & NJSA 47, Records Retention Schedules must be created for the records maintained by a public agency, noting the MINIMUM Legal and Fiscal time periods the records must be retained.

*Unless in Litigation, e-Discovery, Audit or OPRA, then the retention period is not applicable until after final settlement or resolution.

Records Retention

Records Retention Schedules creation and maintenance for all New Jersey Public

Agencies was mandated in accordance with:

- ❖ New Jersey Public Records Laws PL 1953, c. 410
- ❖ NJ Statutes Annotated Title 47 et. seq.

Records Retention Schedules address the following areas:

- Vital
- Legal, Fiscal & Administrative
- Historical
- Confidential
- Retention Period
- Final Disposition

Records Retention and Disposition Schedule		Agency: S821110	Schedule: 002	Page #:1 of 4
Department:	Treasury - Supplemental Annuity Collective Trust (SACT)	Agency Representative:		
Division:		Title:		
Bureau:		Phone #:		

SCHEDULE APPROVAL: Unless in litigation, the records covered by this schedule, upon expiration of their retention periods, will be deemed to have no continuing value to the State of New Jersey and will be disposed of as indicated in accordance with the law and regulations of the State Records Committee. This schedule will become effective on the date approved by the State Records Committee.

Status	Last Updated Date/Time	Approved Date	Effective Date
Published	3/18/2015 3:56 PM		

Record Series #	Record Title and Description	Audit	Alternate Media	Archival Review	Vital Record	Confidential	Retention Policy		Disposition	Citation
							Total Retention Period	Minimum Period in Agency		
0001-0000	Authorization of Disbursement --- Form authorizes the disbursement of checks from the SACT section.						7 Years	7 Years	Destroy	
0002-0000	Bank Record File --- Contains: acknowledgements, deposit slips, reconciliations, and bank statements.						7 Years	7 Years	Destroy	
0003-0000	Cash Disbursements Journal - Manual Input --- Contains: payment totals, check dates, and reason for refunds.						7 Years	7 Years	Destroy	
0004-0000	Cash Disbursement List --- List of cash disbursements for various programs types (i.e., retirements, withdrawals, deaths). Serves as a cross-reference of terminations for supplemental annuity cases.						7 Years	7 Years	Destroy	
0005-0000	Cash Receipt File --- Contains cash receipts documents and a listing of contributions from the various pension funds, utilized for monthly journal entries.						7 Years	7 Years	Destroy	

Records Disposition

Public Agencies must submit

A Public Agency must submit, through **Artemis**, a “*Request and Authorization for Records Disposal*” to obtain **prior** authorization from DORES-RMS, to legally dispose of the **expired** Public Records in their custody.

Upon receiving authorization

The associated records should be disposed as they are **Discoverable** as long as they are in an Agency’s **Physical Custody** regardless of receipt of a disposal authorization from DORES-RMS.

Request and Authorization for Records Disposal

Are **Permanently** retained in Artemis for immediate access in the event of:

- OPRA
- Litigation
- Audit



NOTE: It is imperative that all HARDCOPY 4-Part “*Request and Authorization for Records Disposal*” forms (Ex., “Agency ‘PINK’ Copy”) issued prior to Artemis, be kept PERMANENTLY.

Artemis-Generated

“Request and Authorization for Records Disposal”

Department of the Treasury, Division of Revenue and Enterprise Services, Records Management Services

REQUEST AND AUTHORIZATION FOR RECORDS DISPOSAL		Instructions: This request must be submitted prior to the disposition of any public records. Items 1. through 14 must be completed in full and Items 15.A and 15.B signed for fiscal records. NOTE: In the event of an unexpected scanning failure, until the problem is resolved, the form may be sent to: DISPOSAL REQUESTS, Department of the Treasury, Division of Revenue and Enterprise Services, Records Management Services, P.O. Box 661, Trenton, N.J. 08625-0661. Questions, call 609.530.7404.		1. Requesting Agency Name and Address Treasury - Pensions & Benefits 50 West State Street PO Box 295 Trenton NJ 08625			
2. Request Id/Date 34274 3/8/2016		3. Requested By (Electronically Signed by)		4. Request Approved By (Electronically Signed by)			
5. Records Manager		1.A Agency Retention Schedule Number S821112 - 002					
6. Archival Review Not Required		7. Early Records Disposal (Due to Document Conversion or Damage) Microfilm Digital Image Damaged Records Certificate		8. Comments - Document Conversion or Damage			
Authorization is hereby requested for the disposal of the following public records in accordance with New Jersey P.L. 1953, c. 410 as amended. It is further certified that the record series listed herein have exceeded their respective retention periods and are not involved in any action, such as a pending OPRA request, litigation, or anticipated litigation as per the Federal Rules of Civil Procedure, December 2006; and are not required for a present or a future audit.							
#	9. Record Series #	10. Record Series Title	11. Retention Period	12. Inclusive Dates		13. Dispose After	14. Volume (in Cubic Feet)
				From (MM/YYYY)	To (MM/YYYY)		
1	0001-0000	Annual Statement Workpapers	10 Years	01/2004	12/2005		1.00

For Records Management Services Use Only :			Total Volume :		1.00
15. Audit Verification		16. Authorization		17. Disposition	
15.A Auditor (Electronically Signed by) 		16.A Authorization Date		16.B Authorization Number	
15.B Date		16.C Authorizing Signature, Records Management Services 		17.A Verification Signature	
				17.B Date	

Image Processing System Certification


 State of New Jersey
Division of Revenue and Enterprise Services (DORES)
Records Management Services - RMS

IMAGE PROCESSING SYSTEM REGISTRATION APPLICATION
(N.J.A.C. 15:3-Set seq.) BEFORE completing this application, please read the [Instructions](#).

AGENCY NAME: _____

This is an application for:

- ☐ In-house Imaging System
- ☐ Service Bureau Imaging
- ☐ Special Document Imaging Services (DORES services)

APPLICATION PACKAGE CHECKLIST (PLEASE INCLUDE ALL THAT APPLY IN YOUR PACKAGE)

<input type="checkbox"/> Review Form	<input type="checkbox"/> Imaged Records Series List
<input type="checkbox"/> Feasibility Study and or RFP/RFI/RFB (if applicable)	<input type="checkbox"/> Microfilm Inspection Report (if applicable)
<input type="checkbox"/> Data Migration Report (replacement systems)	<input type="checkbox"/> Data Migration Statement (all applications)

Registration No. «Certification_»

STATE OF NEW JERSEY
STATE RECORDS COMMITTEE

PUBLIC RECORDS IMAGE PROCESSING SYSTEM
CERTIFICATE OF REGISTRATION



Assistant Director
Division of Revenue and Enterprise Services-RMS

«Certification_Date»

Image Processing System Registration Application and Annual Renewal

As per *PL 1994, c. 140*, the State of New Jersey allows for the replacement of hardcopy public records with digital and microform images (e.g., Optical Disk, CD, DVD, Magnetic Tape & Microfilm).

The State Records Committee and Records Management Services issues Initial and Annual Imaging System Certifications to an Agency for an in-house or outsourced, **Non-Proprietary** imaging application. Documents required for obtaining an Initial and Annual Imaging Certification from the State Records Committee and Records Management Services include:

➤ **Image Processing System Initial Registration Application**

- Scanning Policy and Procedures
- Disaster Prevention and Recovery
- Data Migration Path
- Feasibility Study
- RFP/RFI/RFB
- Vendor Detail
- Imaged Records Series List
- Proof of Public Notice

NOTE 1: PDF/A is the only acceptable format.

NOTE 2: When certifying multiple offices, set up the Imaging System as an **“Enterprise-wide System”** for present and future expansion.

The form is titled "IMAGE PROCESSING SYSTEM REGISTRATION APPLICATION" and is issued by the State of New Jersey, Division of Revenue and Enterprise Services (DORES), Records Management Services - RMS. It includes the state seal and a reference to N.J.A.C. 15:3-5et seq. The form contains a section for "AGENCY NAME:" followed by a blank line. Below this is a section for "This is an application for:" with three checkboxes: "In-house Imaging System", "Service Bureau Imaging", and "Special Document Imaging Services (DORES services)". The form also includes an "APPLICATION PACKAGE CHECKLIST (PLEASE INCLUDE ALL THAT APPLY IN YOUR PACKAGE)" with two columns of checkboxes. The first column includes "Review Form", "Feasibility Study and or RFP/RFI/RFB (if applicable)", and "Data Migration Report (replacement systems)". The second column includes "Imaged Records Series List", "Microfilm Inspection Report (if applicable)", and "Data Migration Statement (all applications)".

State of New Jersey
Division of Revenue and Enterprise Services (DORES)
Records Management Services - RMS

IMAGE PROCESSING SYSTEM REGISTRATION APPLICATION
(N.J.A.C. 15:3-5et seq.) BEFORE completing this application, please read the [Instructions](#).

AGENCY NAME: _____

This is an application for: ☐ In-house Imaging System
☐ Service Bureau Imaging
☐ Special Document Imaging Services (DORES services)

APPLICATION PACKAGE CHECKLIST (PLEASE INCLUDE ALL THAT APPLY IN YOUR PACKAGE)

<input type="checkbox"/> Review Form	<input type="checkbox"/> Imaged Records Series List
<input type="checkbox"/> Feasibility Study and or RFP/RFI/RFB (if applicable)	<input type="checkbox"/> Microfilm Inspection Report (if applicable)
<input type="checkbox"/> Data Migration Report (replacement systems)	<input type="checkbox"/> Data Migration Statement (all applications)

Image Processing System Certificate of Registration

Registration No. 22110901-MP

STATE OF NEW JERSEY
STATE RECORDS COMMITTEE
PUBLIC RECORDS IMAGE PROCESSING SYSTEM
CERTIFICATE OF REGISTRATION

This certifies that Records
Management Services
has determined that the public records image processing system
submitted pursuant to P.L.1994, c.140 by the

Township of _____

is in compliance with all specifications and standards as set forth in
N.J.A.C. 15:3-4, Image Processing of Public Records
and has met the requirements for registration set forth in
N.J.A.C. 15:3-5, Registration of Image Processing Systems
and has therefore authorized the issuance of this
Registration of Compliance.

This registration has a migration path component,
Therefore it is understood that the aforementioned agency
may destroy all short term, long term and non-historical permanent
original records after image processing.

Division of Revenue and Enterprise Services-RMS

09 November 2022

Image Processing System Certification Letter



State of New Jersey

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
P. O. BOX 661
TRENTON, NEW JERSEY 08625-0661

PHILIP D. MURPHY
Governor

SHEILA Y. OLIVER
Lt. Governor

ELIZABETH MAHER ~~MURPHY~~
State Treasurer

JAMES J. FRUSCIONE
Director

9 November 2022

Clerk
City of Brigantine
1417 West Brigantine Avenue
Brigantine, New Jersey 08203

Dear

This is to verify that the public records image processing system for the City of Brigantine was registered by the Records Management Services (RMS) on 09 November 2022, Registration Number 22110905-MP and is in compliance with the standards, procedures and guidelines adopted under N.J.A.C. 15:3-4, *Image Processing for Public Records*. This registration should be retained permanently by your agency, and a copy of it should accompany any future disposal requests for destruction of original records maintained on this system, pursuant to N.J.S.A. 47:3-17. Your agency must submit appropriate documentation to request destruction of the imaged records at such time as the record's lifecycle has expired.

Your system will be due for an annual review and renewal of registration per N.J.A.C. 15:3-5.6 on 1 October 2023.

Sincerely,

Division of Revenue and Enterprise Services-RMS

c: file

Image Processing System Annual Renewal/Amendment

Imaging Registration Annual Review/Amendment Form

Mailing: PO Box 661, Trenton, NJ 08625-0661
Location: 33 W. State St. 5th Floor Trenton, NJ 08625
609-292-8711

ANNUAL REVIEW ☐ AMENDMENT ☐ ANNUAL REVIEW AND AMENDMENT ☐

AGENCY NAME :
CERTIFICATE #:

Primary Contact Name:
Address:

Phone / fax / email:

Custodian of Records Name:
Address:

Phone / fax / email:

Preferred Annual Review Date (choose 1):

☐ January 1 ☐ April 1 ☐ July 1 ☐ October 1

Do you want to make this the annual review date for all certified systems in your agency?

☐ Yes ☐ No

If yes, please list other certified systems:

1. Has your agency added additional records series or inclusive years to your Imaging system?

☐ Yes ☐ No

All Agencies must submit the Imaged Records Series List for each retention schedule/office whose records are scanned into this system

☐ Imaged Records Series List(s) attached

2. Has your agency added to or upgraded the hardware and/or software for your Image processing system?

☐ Yes ☐ No (If yes, attach appropriate documentation.)

3. Has your agency updated your Disaster Prevention/Recovery Plan?

☐ Yes ☐ No (If yes, attach appropriate documentation.)

4. Microfilm Inspection ☐ Microfilm Inspection Report attached

- a. ☐ Our agency has not produced any microfilm since our last annual review
b. ☐ Our agency has its microfilm produced or processed by DORES
c. ☐ Our agency produces its own microfilm or has its microfilm produced by a vendor.

If you checked c. you must submit a reel of microfilm for each size produced for inspection BEFORE submitting an Annual Review/Amendment. This reel should be an original silver halide production copy, NOT a sample. Microfilm must be accompanied by a completed Microfilm Submission Form. Microfilm will be returned to the agency. A passing Microfilm inspection must accompany this Annual Review/Amendment Form.

5. Has your agency changed vendors? This includes vendors for: Imaging services, micrographics, hardware or software, maintenance.

☐ Yes ☐ No (If yes, attach appropriate documentation, including the names of the old and new vendors and contact information)

6. Does your agency want to implement a migration path for long term records if you have not already?

☐ Yes ☐ No (If yes, attach appropriate documentation.)

AGENCY VERIFICATION :

I hereby certify that the documentation listed on and/or attached to this **Image Processing System Annual Review/Amendment Form** is a true and an accurate reflection of the agency's image processing system upon this date and is submitted in compliance with N.J.A.C.15:3-5.6.

Legal Custodian: Print Name

Signature:

Date

For questions or further assistance, contact your agency Records Analyst.

Submit by Email

Attach Documentation

DORES revised 10/2013

Image Processing System Certification Letter of Annual Renewal



State of New Jersey

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND
ENTERPRISE SERVICES
RECORDS MANAGEMENT SERVICES
P.O. BOX 661
TRENTON, NJ 08625-0661

PHILIP D. MURPHY
Governor
SHEILA Y. OLIVER
Lt. Governor

ELIZABETH MAHER MUOIO
State Treasurer
JAMES A. FRUSCIONE
Director

21 June 2022

[Name] _____
NJ Department of Transportation
1305 Parkway Avenue
Ewing NJ 08625

Dear [Name] _____

This is to verify that the annual renewal/amendment for the registered Public Records Image Processing System (#01092001) for public records of NJ Department of Transportation has been determined by the staff of the Department of Treasury Division of Revenue and Enterprise Services, Records Management Services to be in compliance with the standards, procedures and guidelines adopted under N.J.A.C. 15:3-4, *Image Processing for Public Records*.

The destruction of original records must adhere to the procedures mandated by State Statutes per N.J.S.A. 47:3-15 to 30, including the submission of a "Request and Authorization for Records Disposal" form accompanied by a copy of the "Certificate of Registration."

Regulations allow an agency to choose their annual review date from the following dates, January 1, April 1, July 1 and October 1. We have temporally assigned you a new date. *Your next annual review will be due, July 1, 2023.* If you would rather have one of the other dates, please let us know as soon as possible.

Respectfully,

Liz Hartmann

Liz Hartmann

Image Processing System Guidelines

When Contracting a Vendor

1. Ensure it is understood that hardcopy & imaged records are **Public Records** and **belong to the Public Agency**.
 2. Ensure that the stored records are classified in accordance with their records retention schedules.
 3. Require security controls to prevent unauthorized records access, manipulation, defacement or destruction.
 4. Be aware of storage and backup locations restrictions.
 5. Prohibit the Vendor from destroying any Imaged records unless the agency specifically directs the action.
 6. Require the Vendor to document changes in their format/programming that may affect records access.
 7. Specify records transfer requirements for contract-exit processes.
 8. Ensure records are **retrievable and accessible** in response to OPRA Requests, Audits, Subpoenas, Investigations, e-Discovery, Litigation Holds and Litigation.
-

The Cloud

Due to the nature of virtual cloud storage, precautions must be taken when dealing with Database Data, Metadata, Portable Data, Text Messages, Email and Electronic Communications.

Records & Health Professionals should work across disciplinary lines to protect these records with the same considerations that were always given for hardcopy records:

- Auditors
- Procurement Professionals
- Legal Advisors
- Health Information Technology Staff
- Health Information/Internal Security Staff
- Agency Managers
- Records Management Liaisons
- Risk Management Professionals

Cloud Storage Guidelines

When Contracting With a Vendor

1. Ensure it is understood that hardcopy & imaged records are **Public Records** that **belong to you**.
2. Ensure that the stored records are classified in accordance with their records retention schedules.
3. Require security controls to prevent unauthorized records access, manipulation, defacement or destruction.
4. Be aware of storage and backup locations restrictions.
5. Monitor the life-cycle of records stored in the Cloud – creation, storage, access, storage or legal destruction.
6. Prohibit the Vendor from destroying or image records unless the Agency specifically directs the action.
7. Require the Vendor to document changes in their format/programming that may affect records access.
8. Specify records transfer requirements for contract-exit processes.
9. **Ensure records are retrievable and accessible in response to Audits, Subpoenas, Investigations, e-Discovery, Litigation Holds and Litigation.**

Email & Electronic Communication



Email & Electronic Communication

Including content, metadata and attachments, are Public Records with the same Records Retention, Disposition, Access, Intellectual Property, Legal Rules of Evidence and e-Discovery concerns as hardcopy or microform records. This includes: Email, Blogs, Wikis, Pod Casts, Social Media, Posts, Text, Chats, etc.

Email & Electronic Communication Management Guidelines

Email and Electronic Communications System should have:

- **Security Controls** that guard against **unauthorized** access, use, modification, dissemination, disclosure and/or destruction as Email is often a phishing target.
- **Provisions** for the administration of “Litigation Holds” and Compliance Audits.
- **Back-up and Disaster Recovery** for the restoration of Email.
- ***Authorized* Agency IT Staff** should control the tracking, indexing archiving, access, retention and disposition of Email records in the Email Central Storage/Management System.

Consult the General Schedule - General Retention:

Retentions for Email and Electronic Communication - in general, a **seven (7) year retention period** is regarded for the Retention and Disposition of Email.

Adopt

Polices for Email, Social Media and Internet usage with ongoing Agency-wide training.

Implement

Security Controls that guard against unauthorized access, use, modification, dissemination, disclosure and/or destruction as Email is often a phishing target.

Establish

Provisions for “Litigation Holds” and Compliance Audits.

Institute

Back-up and Recovery methods for the restoration of Email.

Authorized Agency IT Staff

Only authorized IT staff should control the tracking, indexing archiving, access, retention and disposition of Email records.

Email Safeguards

- Strong passwords and multi-factor authentication (MFA)
- Email encryption
- Email sender identity authentication protocols
- Data Loss Prevention (DLP) to detect & block sensitive data from being sent
- Routine backups and software updates

Email Threats

- Phishing - Emails aimed at stealing information
- Malware & Ransomware - Malicious software delivered via email
- Business Email Compromise (BEC) - Criminals impersonate executives, vendors, or business partners to initiate wire transfers or divulge confidential information
- Data Loss - Accidental or Deliberate leak of data through email
- Email Spoofing - Emails that appear to originate from legitimate sources to deceive recipients
- Weak Passwords - Increase the risk of unauthorized access and account compromise





Remember...

Email and Electronic Communication are

- **Public Records**
- **May Not be Destroyed Without Prior Authorization from DORES-RMS**
- **Accessed under OPRA**
- **Accessed under an Audit**
- **Discoverable**
 - May be Disclosed in a Court of Law
 - May be Disclosed through e-Discovery

Social Media

Interactive communication, web-based & mobile technology, **not the same as Digitally-borne or Website records**. On a website, you can print hardcopy and control and protect it; whereas Social Media, you **cannot** control it and it **can** be altered and or removed.

Social Media

Global, immediate and very accessible!

Public

Records Retention & Disposition directives should be established regarding content, language, subject matter, which includes: blogs, Wikis, Pod casts, Metadata, TEAMS, OneDrive, SharePoint and Email regarding – Operational Records, Meetings, Events, Chats & Recordings

Disclaimer

Should accompany the data being placed on a Social Media site and hardcopy should be printed as an audit trail in the event of e-Discovery, Litigation, etc.

Security

Social Media can be altered and used as a portal for Cyberattack, which presents a real concern for an agency's ability to operate effectively and release vital public information.

Passwords

Use different passwords for every social network used a single password enables a hacker to get access to everything.

Be careful of your mailbox

Direct messages are a form of phishing to get access.

Internet

Due to ever-changing content & structure, an agency's website should be routinely maintained and its hardware, software, metadata and content should reflect the following areas of concern:

Enterprise-wide Records & Information Management Policy

Records Access Perspective

Public and Private Access

Security Perspective

Implemented & Monitored Data Security/Encryption

Health IT Perspective

Website Creation, Maintenance, Growth & Security

Intellectual Property & Historical Perspective

Digitally-born documents if not printed, may be lost

Legal Perspective

Litigation, Rules of Evidence & e-Discovery

Financial Perspective

Federal, State or Local Audit

Blockchain

A transparent, decentralized “distributed digital ledger” of data blocks recording transactions chronologically across a cryptographic network linked chronologically in a "chain" that in theory, cannot be altered – however blockchain can be hacked.

Audit Trail

- Financial and Programmatic Audits - data “chained” together that is irreversible and cannot be altered, such as cryptocurrency, contracts, records, etc.

Data Management

- Secure Data Storage – Decentralized and Distributed - harder to attack
- Control over Records Access and Processing – every transaction is recorded and can be accounted

Supply Chain Management

- Authenticity Verification
- Transparent
- Cost & Time Saving

Expedite Claim Processing & Contract Management

- “Plays well” well with online, automated claims and contracts processing and transactions

Four (4) Types of Blockchain

- **Public blockchain** – anonymous, open network
- **Private blockchain** – permission, closed network
- **Hybrid blockchain** – combination of public and private network
- **Consortium/Federated blockchain** – combination of public and private where members collaborate in a decentralized network



VITAL RECORDS: LIFE RELATED

Life event-related records maintained by State, County, Municipal Agencies - Birth, Death, Marriage, Adoption, Divorce, Domestic Partnership, Civil Union, Custody, Separation, Drivers License, Disability ID, and SSN and Religious Institutions - Sacramental Records*.

- **Public Health**

Data collection, statistics, research, monitoring trends, tracking disease and developing public health programs.

- **Legal**

Legal procedures, proving identity and residence, applying for benefits and obtaining citizenship.

- **Genealogical Research**

***Religious Sacramental Records have been used as proof of residency.**



VITAL RECORDS: MEDICAL

Records and data imperative to maintain life, such as:

- **Prescriptions**
- **Medication(s)**
- **Living Will**
- **Medical Diagnosis**
- **HIPAA**
- **Power of Attorney**



VITAL RECORDS: OPERATIONAL



Records, regardless of their medium, that are deemed **Essential** in case of Litigation, Prove Legal Ownership, Emergency, Disaster, and Cyber Breach – they typically comprise **10%** of an Agency's records.



However, the best laid plans...

Disaster Prevention & Recovery/Business Continuity of Operations (COOP) Plan

Objective

To **identify the major operational records** (Hardcopy, Electronic, Digital, etc.) and institute measures for their protection in the event of a Disaster (Cyberattacked or Destroyed) and mitigate data loss; ensure data integrity and access and resume operations and services quickly, efficiently and effectively to lessen the amount of damage and associated costs relating to:

- **Data & Information**
- **Lost Revenue**
- **Wages**
- **Labor**
- **Employee Morale**
- **Customer Goodwill**
- **Marketing Opportunities**
- **Incurred Bank Fees**
- **Incurred Legal Penalties &**
- **Bad Publicity**



Disaster Prevention & Recovery

Business Continuity of Operations (COOP) Plan

Used in conjunction with: Security Standards, Guidelines, Policy and Procedures, Client Network Installation and De-installation Plans, Hardware and Software supporting documentation.

ESTABLISH

- Disaster Prevention & Recovery and Business Continuity of Operations (COOP) Plan
- Identify Physical and Cyber Vendors for: Disaster Recovery Services and Supplies, System Hardware and Software and Information and Electronic Disaster Recovery Services
- Establish Disaster Recovery & COOP Team – Management, Records Management, Key IT Staff, Custodian of Public Record and Local Law Enforcement
- Create an Agency Chain of Command
- Designate Data Center Hot & Cold Site(s) & Alternate Operations Site for Staff, IT and Records

IDENTIFY

- Hardware and Software (manufacturer, models and versions)
- Identify the Agency's Vital Records – Legal, Fiscal, Personnel, Contracts, Plans, etc.
- Potential Recovery Costs associated with Hardware, Software, Supplies, Technology Supplies, etc.

RETAIN

- Retain *hardcopy* of the *Disaster Prevention & Recovery and Continuity of Operations Plan* in various safe and accessible in *offsite locations* and with every Disaster Recovery & COOP Team Member.

REVISE

- Create the Plan! Test The Plan! Revise The Plan! Re-Test The Plan!

If a Records Disaster should strike...

Check

Your **Insurance Policy!**

Implement

Disaster Prevention & Recovery Plan!

Assemble Disaster Prevention & Recovery Team - Management, Records Management, Custodian of Public Record, State Cybersecurity and Law Enforcement Agencies

Conduct an Assessment

To ascertain if the Damaged Records and Information may have had backups such as, Hardcopy, Optical Disk or Microform that may be salvaged.

Submit to DORES-RMS

Damaged Records Report for presentation before the **State Records Committee (SRC)**.

TECHNOLOGY A DOUBLE-EDGED SWORD?

Information Technology fosters Operational Efficiencies but it can also create Internal and External Operational Single & Multiple Threat Groups that can:



Cause Physical Harm

Affect Employee Morale

Disrupt and/or Shutdown Operations

Alter, Corrupt and/or Destroy Information

Exploit to Ruin an Agency's Credibility & Reputation

Inflict Legal, Intellectual, Political & Financial Ramifications

Cyber Security

Cyber Security

Safeguarding devices, hardware, software, networks, data and information from cybercriminal attacks including but not limited to: phishing, ransomware, identity theft, data breaches, espionage and nation-state attacks.

Data and Information Targets

Personal & Sensitive Data, Protected Health Information (PHI), Personally Identifiable Information (PII), Electronic Medical Record (EMR), Electronic Health Record (EHR), Personal and Sensitive Data, Intellectual Property, Personal Information, Financial, Educational, Government and Business Information Systems.

Cyber Security Key Elements:

- Disaster Prevention and Recovery**

- Business Continuity**

- Cloud Security**

- Email, Internet & Social Media Security**

- Identity Management**

- Data Security**

- Mobile Security**

- Network Security**

- Vital Records**

COMMON TYPES OF CYBERATTACK



Malware attacks



Password attacks



Ransomware



Man-in-the-middle (MitM) attacks



Phishing



URL interpretation/
URL poisoning



SQL injection attacks



Cross-site scripting (XSS)



DDoS



DNS spoofing



Botnets



Watering hole attacks



Insider threats

CYBER ATTACK TYPES

Cyber Attacks may be a single or group attack, a one-time or a repeated attack for: Financial Gain, Espionage, Sabotage, Fraud, Influence, Notoriety, etc.

- **Phishing, Spearphishing, Smishing, Typosquatting, Vishing, Whaling**
- **Ransomware/Scareware**
- **Malware & Wiper Malware Families**
- **Exploit & Prior Compromise**
- **Cyber-Physical Attack**
- **Man-in-the-Middle Attack (MITM)**
- **SQL injection**
- **Identity Theft, Medical Information & Stolen Devices/Credentials/IDs**
- **AI-generated Voices in Video & Robocalls**
- **Stalkerware/Spyware**
- **Denial of Service (DoS)**
- **SIM Swap Attacks/SIM Swap Scam/Port-out Scam/SIM Splitting/ Smishing / Simjacking /SIM Swapping) Account Takeover (ATO)**

Third-Party Contractor or Vendor Risks

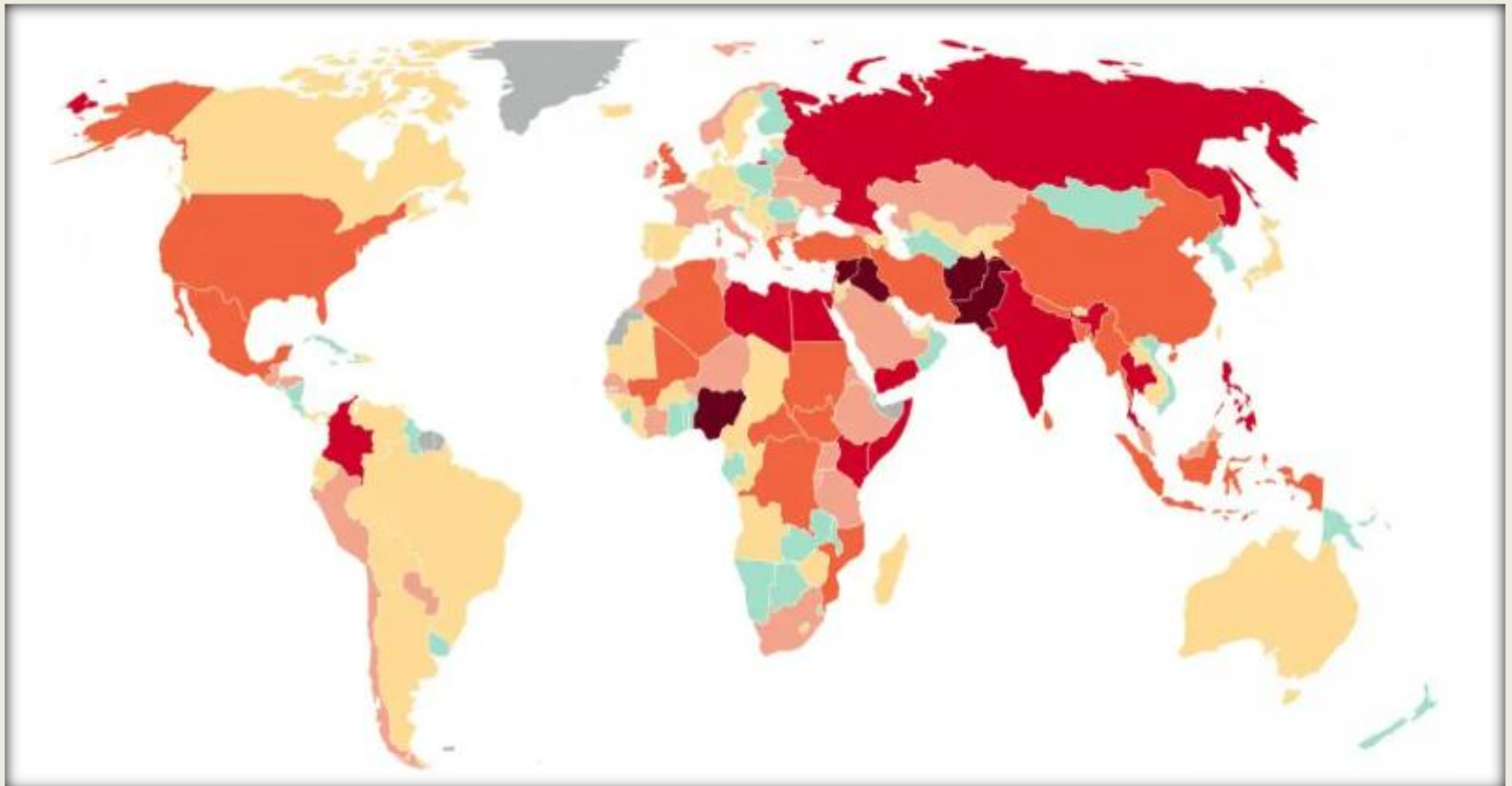
Direct access to people, facilities, networks and/or systems could unknowingly pose a risk to an agency. In addition, they could pose a threat through their network databases and systems if their security became compromised.



Noted Regions of Nation State-Sponsored Cyberterrorism, Cyber Security Wars & Attacks

Americas - North & South ● Asia-Pacific (APAC) ● Europe-Middle East-Africa (EMA)

Cyber Attacks may be a single/group attack(s), a one-time/repeated attack(s) for Financial Gain, Espionage, Fraud, Sabotage, Influence, Notoriety, etc.



THREE (3) CYBER ATTACK STRATEGIES



ZERO TRUST POLICY



What is **Zero Trust**?

Answer:

A User or Device is *never* trusted and access is denied until Identity *and* Authorization have been thoroughly verified.

CIA STRATEGY

CIA

Confidentiality

Only Authorized Individuals can access information.

Integrity

Only Authorized Individuals can alter, add or remove sensitive information.

Availability

Systems, Functions and Data must be accessible on-demand.



ETHICAL HACKING



Ethical Hacking

An *agency-authorized* deliberate attempt to gain unauthorized access to its System, Applications and/or Data through duplicating the strategies and actions of a Hacker to identify system security vulnerabilities and resolve them **before** a real cyber attack occurs.

Cybersecurity Incident Response Plan

Components

Much like the Vital Records Plan, a Cybersecurity Incident Response Plan, identifies essential personnel, vendors, equipment and alternate space which are imperative to resume offsite daily operations and safely mitigate the consequences of such an event:

Before a Cyberattack

ESTABLISH

- Vendors Lists: Disaster Recovery Services/Supplies, System Hardware/Software Information and Electronic Disaster Recovery Services
- Cyber Security Team: Management, Records Management, IT, Custodian of Public Record, State Cyber Security Agencies & Local Law Enforcement
- Create an Agency Chain of Command
- Designate Data Center Hot & Cold Site(s) and establish an Alternate Operations Site for Staff, IT and Records
- MVR Monitoring: Continuous (24/7/365) automated Monitoring, Verification and Reporting – “End-to-End”

Cybersecurity Incident Response Plan

ESTABLISH cont.

- Physical Security: Enterprise-wide Policies and Procedures
- Data Encryption: Storage/transit/network-wide
- Firewalls & Filters: Prevent illicit network traffic
- Software/Antivirus/Antimalware: Routine update and patching, detect & prevent unauthorized access and/or intrusion and minimize Dwell Time
- Back-up: Data and Records
- Computer: Configuration Management
- Security Event: Management and Reporting
- Data Security: Policies and Procedures

Cybersecurity Incident Response Plan

ASSEMBLE

- Activation Authority Procedures
- Specific Task(s) List
- Disaster Recovery Team List
- Response Team List
- Vital Records Protection Methods/Equipment Already Employed
- Cyber Security Response Procedures Distribution List
- Cyber Security Monitoring Procedures
- Communications and Media Sources
- Backup and Hot/Cold Site Locations
- Federal Agency & State Agency Cyber Security Resource Lists
- Cyber Security & Firewall Software Vendor Lists
- Hardware and Software Lists

RETAIN

- Retain hardcopy of the Disaster Prevention & Recovery and Continuity of Operations Plan in various safe and accessible offsite locations and with every Disaster Recovery & COOP Team Member.

Cybersecurity Incident Response Plan

In the event of a cyberattack...

IDENTIFY

- Assemble Cybersecurity TEAM
- Identify and Target attacked areas as best as possible
- Isolate them from further attack, quickly as possible
- Check your Insurance Policy
- **Reach out immediately to the NJ Office of Homeland Security for assistance 1-866-4-SAFE-NJ**
- Resume operations safely & efficiently as possible
- Reassure staff, clients, constituents
- Ensure the normal flow of business as quickly as possible – seconds count!
- Submit - DORES-RMS Cyber Attack Records Report for presentation before the State Records Committee (SRC).

Artificial Intelligence (AI) Defined

Artificial Intelligence (AI) - Computers that perform reasoning, decision making, problem solving and learning on a level that exceeds human intelligence through processing large quantities of data and identifying patterns and relationships utilizing Computer Science, Data Analytics, Statistics, Hardware & Software Engineering, Linguistics, Neuroscience, Philosophy and Psychology.

Machine Learning (ML) - A subset of AI that use data and algorithms to replicate how a human learns and quantitatively improve its accuracy.

Deep Learning (DL) - A subset of ML that uses multilayered neural networks (Deep Neural Network [DNN]) to simulate the complex decision-making function of the human brain.

Generative Artificial Intelligence (GAI) - A subset of AI that can analyze code, syntax, functions, words, grammar, semantics and context to constantly refine, rebuild and perfect itself.

Natural Language Processing (NLP) - The process of Speech Recognition and Synthesis, Question Answering, Information Retrieval in a human language format.

AI Applications & Strategies: Positive

Medical: *DaVinci Robot* Enhanced Surgical Procedures

Interaction via Human Speech: Siri and Alexa

Human-Machine: Interaction techniques

Robotics: Productivity enhancements

Government: Enhance processing times

Educational: Intelligent tutoring and adaptive learning tools

Generative & Creative Tools: ChatGPT,* CoPilot, Gemini, Claude

Cyber Incursions & Defense: Applications for Detection and Elimination

Climate Change: Advanced Strategies & Techniques

*ChatGPT, a chatbot application using Generative Pre-trained Transformer (GPT) technology.

AI Applications & Strategies: Negative

Medical: Bad AI Data resulting in Mis-Diagnosis & Incorrect Procedure/Treatment;

Taking Wrong Medication or Taking Incorrect Dosage of Medication

Human Visual & Speech: Perfect Impersonation

Human-Machine Interaction Techniques: Replace Human involvement

Government: Warfare, Espionage, Control, Fake Data & Fake Information

Education: Replace Human Student-Teacher Classroom Learning Experience

Übermensch, Super-man, Superhuman: “Terminator”?

War-gaming: Advanced Warfare Techniques and Strategies

Workforce: Replace White Collar & Blue Collar Jobs

Global Control & Interaction: Distribute False Information

Decrease Human Contact/Interaction/Relationships: Loneliness and Isolation

AI can make mistakes, so double-check responses

AI & Ethics

The NEED for Government Regulations and Control to Prevent Misuse

Moral Compass for Emerging Technology & Innovation

Legal & Financial Ramifications

Maintaining Confidentiality

AI Threats & Ethical Risks

Fake Data & Information Distribution

AI Threat of Replacing Humans Jobs

An Overall Threat

Emotional Attachment to AI - Distorted Human Social
Expectations/Relations

Social Isolation - Atrophy of Human Empathy

Replace Human-to-Human Relationships

AI & the Human Touch

AI Needs a real flesh & blood Human Being

Be part of the loop

Perform Decision Management

Human introduction & oversight of standards, procedures, etc.

Foster Effective Negotiations between individuals or groups

Ensure that no Bad Data is getting into the process, the IT adage still applies:

“Garbage in, Garbage out”  “Bad AI in, Bad AI out”



GLOBAL AREAS OF AI PROCESSING EFFICIENCY OR AI TAKE OVER?

Agencies & Institutions

- Healthcare
- Government
- Financial Institutions
- Education
- Higher Education
- Nonprofit Organizations
- Religious Institutions
- Business
- Military

Operations & Services

- High Tech
- Telecommunications
- Entertainment & Media
- Construction & Engineering
- Transportation & Logistics
- Energy & Utilities
- Retail
- Manufacturing
- Hospitality



Records & Information Management, OPRA and AI

A thorough and efficient Records and Information Management Program should be the foundation before implementing an AI Application.

Public Agencies must continue safeguarding their Public Records and conducting ongoing due diligence on the part of the “Human Component” - Records Manager, IT, Legal, etc. pertaining to: Data Retention, Disposition, Conversion, Preservation, Migration, and Protection of the AI process.



Records & Information Management, OPRA and AI

Enhanced Knowledge Capture and Analysis for Information and Services - AI and Generative AI can search, retrieve, process and provide information at rapid speed and create reports, audio & video –

Customer Service Process - Enhancing customer response turnaround for information processing and delivery.

High Speed Data Search & Retrieval - Search and Retrieval Systems are able to understand queries and extract relevant information from structured and unstructured data sources quickly and accurately ex., OPRA Request Processing.

Data Governance - Data Analysis repositories and can identify PII, PHI and Confidential information providing guidelines for ethical use of information.

Data Compliance - Regulatory Compliance monitor and detect abnormalities, visual security, authentication which has the potential to reduce risk of data breaches.



Department of the Treasury
Division of Revenue and
Enterprise Services
Records Management
Services

PO Box 661

Trenton, NJ 08625

609-292-8711

[https://www.nj.gov/treasury/
revenue/rms/index.shtml](https://www.nj.gov/treasury/revenue/rms/index.shtml)

Records Management Services Staff Contact

The screenshot shows the 'Records Management Services' website. In the top navigation bar, the 'RMS Consultation' link is circled in red. A red arrow points from this link to a dropdown menu that contains 'Directions' and 'Contact'. Below the navigation bar, the 'Records Management Services' section displays the contact information for Liz Hartmann (609-777-1020). To the right, a table lists staff contacts for various categories.

Category	Staff Name	Contact Number
County: A - C	Terricka Page	609-292-8708
County: E - H	John Berry	609-292-8683
County: M - W	Marcella Campbell	609-292-8689
Municipalities: A - E	Terricka Page	609-292-8708
Municipalities: F - L	John Berry	609-292-8683
Municipalities: M - R	Marcella Campbell	609-292-8689
Municipalities: S - Z	Robert Herrick Virma Guzman-Reyes	609-292-8698 609-292-8711
Schools	Karen Perry	609-292-8697
County and Municipal Prosecutors	Terricka Page	609-292-8708
County Community Colleges/County Vo-Tech Schools	Karen Perry	609-292-8697
County Detention Centers - Adult and Juvenile	Robert Herrick Alternate Virma Guzam-Reyes	609-292-8698 609-292-8711

Records Management Services Staff Consultation

Records Management Services

RMS Records Imaging New Jersey Records Manual Contact RMS **RMS Consultation**

[Home](#) / [RMS Contact Information](#) [Records Retention and Disposition](#)

Records Management Services Contact Information Records Retention and Disposition

Division Management
State Records Center
2300 Stuyvesant Avenue,
PO Box 661,
Trenton, NJ 08625-0661

Imaging Services Group
Microfilm Client Relations and Billing
Sue Crammer
[609-777-0902](tel:609-777-0902)

Records Storage - Unit Supervision
Lisa Montano
[609-292-8689](tel:609-292-8689)
James Jenkins

Records Management

Agency Type

County: A - C

County: E - H

County: M - W

Contact Us - Records Management Consultations

[Home](#) / [Contact Us - Records Management Consultations](#)

For business records please visit the [Business Records Service portal](#).

The Division of Revenue and Enterprise Services, Records Management Service Unit, is pleased to offer online, real-time consultations to public agencies throughout New Jersey. If your agency is experiencing problems with managing its public records or needs guidance on a particular records management topic or practice, use this service to obtain help.

Fill out and send the following service request to us. We will assemble a team of experts who will respond to your request or problem and then schedule a live video conference with you and your team. We look forward to serving you.

Service Request

Prefix: First Name: Middle I: Last Name:

Address Line 1:

Marcella Campbell [609-292-8689](tel:609-292-8689)

Thank You.