Guidelines for Developing Retention and Disposition Policies for Artificial Intelligence/Machine Learning Systems

Background and Action Steps

Published by:

New Jersey Division of Revenue and Enterprise Services
James J. Fruscione, Director
February 2025

TABLE OF CONTENTS

Introduction

These guidelines include suggested action steps for creating retention and disposition policies for public records associated with or created by systems using artificial intelligence/machine learning (AI/ML).[1]

AI/ML offers government agencies opportunities to innovate and greatly improve their services and productive capacities. In this connection, the potential applications for AI/ML touch upon a broad range of institutional activities and can give shape to initiatives that influence our social, economic, political, cultural, health, academic, scientific and environmental sectors. Accordingly, as government agencies work to implement and leverage the technology, the development of pathways to effective governance of AI/ML, including the institution of retention and disposition policies, is in order.

Applicability of Public Records Law

As with all public records management publications, the foundation for this document is the legal imperative expressed in New Jersey's public records law (N.J.S.A. 47:3 et seq.). That is, irrespective of medium, all records that are generated and received during governmental operations are public records and subject to the State's records management and archival requirements. Records associated with or created by governmental systems using AI/ML are therefore subject to the State's public records law.

Audience

These guidelines are primarily for professionals who work in records and information management capacities and who have some familiarity with the State's records management program as described in the New Jersey State Records Manual (New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit, 2024c). In addition, generalist managers, administrative support staff, technologists, cybersecurity exerts, procurement officials, auditors, human resources officers, legal advisors and ethics liaisons may find the guidelines useful.

Background

While AI/ML itself is not new, the recent emphasis on expanded experimentation with and use of the technology, including new governmental initiatives and applications, represents an important trend.

The background discussion that follows helps set the general context in which the guidelines may be applied. The assumption here is that use of AI/ML is a relatively new concept for many State and local records managers and public officials, so the discussion goes into greater depth

[1] ML is a subset of AI technology. For purposes of this presentation, the acronyms AI and AI/ML are used interchangeably.

than is typical for records management guidelines. Notwithstanding, this is not intended to be an exhaustive or authoritative treatment of the technological dimensions of AI/ML systems.

Definition and Uses

The Organization of Economic Cooperation and Development (OECD) defines an Artificial Intelligence system as:

> "…a machine-based system that can, for a given set of human defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments (OECD, 2019, p.1)."

Thus defined, use cases for AI/ML technology may encompass a variety purposes. For example, in the public sector, AI/ML may be used to augment or directly execute informational searches and text retrieval. Similarly, it may summarize meetings and text from a collection of works or be used to personalize a citizen's on-line interactions with public agencies based on prior patterns of on-line behavior and/or demographical data. It may be used to predict outcomes or render diagnoses/decisions in topical spaces like computer security, health care, finances, benefits eligibility, environmental controls and public safety/defense. Moreover, it can recognize objects and biological traits, generate media presentations, handle language translations, drive robotic operations and more. (Glasscock, 2019; State of New Jersey, 2023; OECD, 2024)

Predictive forms of AI activity center on ML and revolve around pre-defined rules and data sets. More advanced applications focus on the generative capabilities of AI, or GenAI. GenAI goes beyond the predictive thrust of ML. It uses massive computing power to derive relationships, patterns and inferences from data sources to create <u>new</u> outputs or contents.

Such generative outputs can be new written works, formulas for planning or problem resolution, fully automated decisions, computer code/controls, graphics/pictures, cyber/physical security controls, audio/visual works, etc. Increasingly, AI/ML systems leverage aligned technologies such as natural language processing and customer-centered interfaces like chatbots to facilitate end-user interactions (Lawton, 2024).

Typical Components AI/ML Systems

Industry observers (Fleming, 2024; Lawton, 2024; Run:ai, 2024) note that AI/ML systems operate within infrastructures that feature data, software processing, hardware/network architectures and user interface tools.

Data can come from structured data bases, semi-structured data like electronic documents and spread sheets and unstructured data such as images, video and audio compilations. It can be owned by the end user organization and/or be supplied by third parties. Data can be stored within in-house facilities, Cloud-based platforms or hybrid (Cloud/in-house) complexes.

Software processing tools operate on source data to yield desired outputs. These tools can be based on traditional business rules-processing software. However, increasingly, language models, including so-called large language models (LLMs) like OpenAI's GPT-3 and Google's Palm 2, are rising to prominence. Language models leverage technologies and processes such as neural networks and deep learning and operate with natural language processing to yield answers and predictions to end users (Barney and Lutkevich, 2024). Other types of software tools include data transport, cleansing and access programs that supply usable data to the AI/ML system and end-users. Generally, software tools can be owned by the user organization and/or be obtained via licensure from vendors. Use of language models will likely entail licensure of a vendor's product.

Hardware/network architectures provide the resources needed to run AI/ML systems, transport data to/from system nodes and end-users, and train/operate language models. AI/ML systems are likely to require high capacities to handle massive volumes of data and complex, resource-intensive computational work. For the latter consideration, beyond traditional central processing units, AI/ML may require components that are geared to massive and specialized processing operations – for example, GPUs (Graphics Processing Units), TPUs (Tensor Processing Units), FPGAs (Field-Programmable Gate Arrays), etc. (Flipsson, 2024). These systems are also likely to require massive data storage arrays and robust communications networks to move large volumes of data within and across information system platforms. Given the need for specialized hardware/software, it is likely that most organizations will need to procure and/or license significant portions of their AI/ML architectures from third parties.

Finally, user interface tools enable developers, testers and end users to interact with AI/ML systems. Interface tools can be in the form of customized software such as application programming interfaces and increasingly, natural language interfaces connected with chatbots. These tools can be developed in-house by the organization and/or be procured or licensed from a third party.

Potential Benefits of AI/ML

The potential benefits of AI/ML flow logically from the use cases described previously. For example, in its final 2024 report to the Governor, New Jersey's Artificial Intelligence Task Force (2024) highlights that AI (with specific reference to GenAI) could potentially enhance a range of state government functions, from internal administrative operations to external service delivery.

Likewise, the OECD (2024) investigates the benefits that societies (including their governmental institutions) can derive using AI, with a focus on ten such benefits. Paraphrased, these include: enhanced scientific progress; improved economic growth, productivity and living standards; decreased levels of inequality and poverty; better approaches to complex issues like climate change; more effective forecasting, predictions and analysis; broader and more flexible forms of information production, distribution, access and sharing; advanced healthcare and personalized educational services; improved/safer job experiences; increased citizen engagement and empowerment; and increased institutional transparency/accountability.

Concerns about the Use AI/ML

The potential for improving human endeavors through use of AI/ML is truly impressive. However, OECD (2024) also cautions that use of the technology engenders many significant risks and potential harms.

Once again, paraphrased, the organization's top ten prioritized risks and potential harms are: providing foundations for sophisticated cyber-attacks (including unauthorized access, use and/or defacement of sensitive information); spreading misinformation/disinformation, with negative outfalls like increased fraud and election interference; implementing rushed and poorly designed AI systems that are not safe or trustworthy; causing unexpected harms through misalignments between AI systems and stakeholders' desires, needs and values; concentrating power in the hands of a few technology companies and/or countries that underwrite the development of the technology; using flawed outputs that cause critical system failures; infringing on privacy (through stepped-up surveillance) or on copyright protections; operating with inadequate governance programs that fail to keep up with rapid technological advances; using technologies that are opaque (not clearly understood), thereby engendering accountability gaps; and through system bias, worsening inequality and poverty and/or threatening employment.

The New Jersey AI Task Force (2024) identifies risks and potential harms that are like OECD's. Further, to counterbalance these risks/potential harms, in a joint circular letter, the State of New Jersey (Office of Information Technology et al., 2023) exhorts agencies using AI/ML to adhere to principles like empowerment, inclusion, transparency, innovation, and risk management, as well as to take measures to protect sensitive information.

State and Federal Actions in the AI/ML Practice Space

State and federal authorities within the executive and legislative branches are taking actions to address the potential risks and harms of AI/ML. The Future of Privacy Forum (2024) points out that state lawmakers are working to enact legislation that regulates AI used in decisions that have significant impacts on peoples' lives and livelihoods, with an eye toward mitigating discrimination and violations of citizens' rights. Hooshidary, Canada and Clark (2024) also highlight various initiatives at the federal and state levels – directives, executive orders, legislation, etc., aimed at creating rules to govern the application of the technology, with emphases on the ethical use of AI/ML and protecting the legal rights of individual citizens.

In all these efforts, either explicitly or implicitly, government authorities point to the need for governance – policies, procedures, rules and staffed administrative functions that determine how and when the technology is to be employed.

AI/ML governance aims at the creation of systems that are fit-for-purpose, understandable (explainable), accountable, safe/secure and as free from bias as possible (Mooradian, 2019; U.S. Department of Homeland Security, 2024; The White House, 2024).[2]
Per force, such governance (and ultimately, the sustained success of AI/ML technology itself) relies on records that document how AI/ML systems are designed, developed, tested, operated, used and managed throughout their life cycles. Therefore, basic records management practices, including retention and disposition policies, are core parts of AI/ML governance. In fact, at the national level, professionals representing state government technology agencies note that strong governance programs, including controls over the public records that GenAI creates, are needed to address the risks posed by the technology (Glasscock, 2024).

Governance Models and Their Relationships with Records Management Practices

Arguably, as of the writing of these guidelines, the two most complete and mature governance models for AI/ML technology in the U.S. can be found in the Government Accounting Office's (GAO) AI accountability framework (2021) and the National Institute of Standards and Technology's (NIST) risk management framework for AI (2023).

Both frameworks feature controls that span the life cycles of AI/ML systems and in doing so, highlight documentary resources (records) required to manage the systems' risks and ensure the requisite system qualities – safe, secure/resilient, privacy-enhanced, explainable, fair, accountable/transparent, valid and reliable (National Institute of Standards and Technology, 2023). As will be discussed, these documentary resources can be used to develop a tentative AI/ML record series taxonomy that can be translated into a records retention/disposition policy regime.

Summary of NIST Framework

The NIST framework (2023) includes four functions: 1) govern (a cross-cutting function that defines the values, policies, procedures, rules, roles and responsibilities associated with AI/ML systems); 2) map (determining and documenting the legal and operational context of AI/ML systems and associated risks); 3) measure (collecting and assessing data points – qualitative and quantitative, on system operations and impacts); and 4) manage (assigning resources to run/administer AI/ML systems and directing steps required to address issues and opportunities that result from the operation of the systems). Within the NIST framework, there are requirements for involving diverse stakeholders, managing vendors and determining when to decommission systems.

[2] Federal government perspectives on AI/ML may be shifting. As of the writing of these guidelines, it is too early to predict how this development will evolve to influence the uses of AI/ML technology.

Summary of GAO Framework

GAO's framework (2021) also includes four functions: 1) govern; 2) data; 3) performance; and 4) monitoring. To a significant degree, these functions overlap NIST's. However, as one might expect, GAO has a stronger orientation toward documentary artifacts that facilitate auditing. So, for example, the governing function requires documentation of technical specifications to ensure AI/ML systems are suited for their intended purposes. The data function calls for documentation of sources and attributes of data used by the systems – for instance, reliability measures, documentation of use of synthetic, imputed and/or augmented data, information about data dependencies, measures of bias, security classifications, etc.

Organizational Structure

Both frameworks pre-suppose organizational structures (governing bodies) within which AI/ML governance is developed, applied and administered. In New Jersey's governmental context, these structures will vary based on the level, size and complexity of specific institutional settings. Broadly, however, one could envision governing bodies consisting of diverse groups of people representing wide ranges of disciplines, including system owners/subject matter experts, legal authorities, procurement officials, records management professionals, information technologists, cyber security authorities, human resources specialists, ethics officers and external/internal stakeholders.

Despite the organizational diversity that exists among governmental agencies in New Jersey, there is a common legal structure through which AI/ML retention and disposition programs can be implemented – approval of retention schedules and disposition actions through the State's Records Management Services Unit and State Records Committee (New Jersey Division of Revenue and Enterprise Management, Records Management Services Unit, 2024c, pp. 10-13). Thus, as will be shown, no matter how agencies constitute their AI/ML governance functions, those functions can be linked with this common legal structure, seamlessly and to good effect, for records management purposes.

Guidelines

With a basic understanding of AI/ML technology, its potential benefits/risks and the governance structures needed to ensure sound and accountable AL/ML system operations, New Jersey governmental officials can develop policies for AI/ML records retention and disposition. Given the rapidly expanding and diversified uses of the technology, such policies <u>must be considered provisional</u>. Nonetheless, it would be best for agencies to plan for retention and disposition controls before implementing AI/ML technology. Organizations that fail to take proactive postures may ultimately find themselves unable to account for their uses of AI/ML in a responsive, legally defensible manner.

In connection with the points above, even if their approaches to records retention/disposition are provisional, proactive agencies will gain better understandings of AI/ML records by taking the actions outlined below. Improved understandings of these records will foster greater intellectual control over the components of AI/ML systems. Through this, agencies will improve their capacity to develop more understandable, fair, secure, reliable, valid and effective systems over the course of time.

Key Contacts

The contact for the records management topics covered in the guidelines is the New Jersey Division of Revenue and Enterprise Services' Records Management Services Unit (DORES/RMS): 609-777-1020 or 609-292-8711. Guidance on records with permanent and historical value can be obtained from the State Archives: 609-633-8304 or 609-292-6260.

Action Steps

Following are the action steps that agencies can take to create AI/ML records retention and disposition policies. The action steps mirror those reflected in earlier guidelines issued by DORES/RMS (New Jersey Division of Revenue and Enterprise Management, Records Management Services Unit, 2024a, 2024b).

Because many governmental agencies are just beginning to explore and use the technology, the guidelines include the formation of an AI/ML governing board, which can interact with DORES/RMS and the State Records Committee when formulating and administering the agency's AI/ML retention and disposition policies.

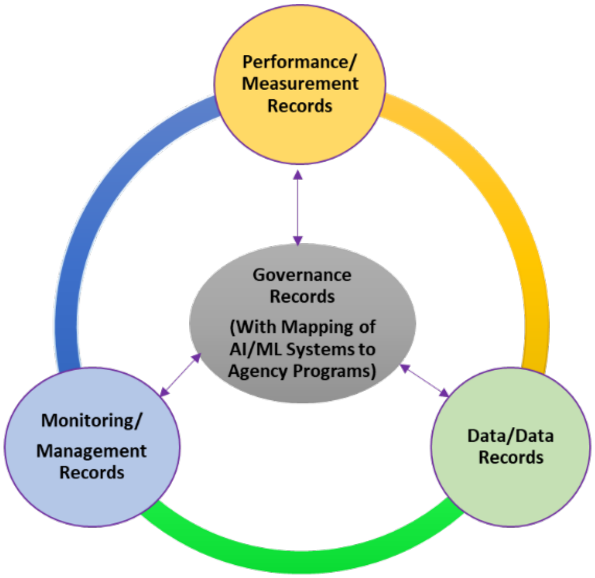
1. ***Form an AI/ML Governing Board.*** Given the potential benefits and risks of AI/ML technology, it would be wise to form an AI/ML governing board with a mandate to assess, charter and monitor the agency's use of AI/ML systems. This would be especially important if the agency intends to use the technology in settings involving significant societal concerns such as benefits eligibility, health care coverage, education, environmental protection or public safety.

As noted previously, one could envision representatives from a wide range of disciplines and endeavors participating on an AI/ML board – for example, system owners/subject matter experts, legal authorities, records management professionals, information technologists, cyber security experts, procurement officials, human resources authorities, ethics officers, and external/internal stakeholders. Records management professionals would likely be the best candidates to coordinate and lead projects aimed at establishing Ai/ML retention and disposition policies.

Finally, the best practice would be for the governing body to review and approve action steps 2-6 below.

2. ***Inventory/Create Categories for Records***. For new systems, agencies may create records categories (series), or for existing systems, conduct inventories of existing series. In both cases, using a scheme such as the example taxonomy depicted below may prove helpful. Note that the example record series in the taxonomy align with functions like those found in the GAO and NIST frameworks discussed previously. Ultimately, building formal records series taxonomies is central to developing intellectual control over the contents and functions of AI/ML system.

Figure 1. Tentative AI/ML Records Series Taxonomy


Performance/ Measurement Records
Governance Records (With Mapping of AI/ML Systems to Agency Programs)
Monitoring/ Management Records
Data/Data Records

a. Governance Records. These records pertain to the core organizational, financial/fiscal and technical aspects of the system. They inform, and in turn are informed by, the system as it operates throughout its life cycle. Examples of records in this category may include:
   - Documented goals and objectives of the system
   - Technical specifications and resources – records covering all the technical components of the system, including documentation of system architecture/system design, development, AI model training, testing, implementation, etc.
   - Project management documentation such as plans and status reporting associated with system development and major system upgrades
   - Budget and expenditure records
   - Laws, policies, procedures, rules and regulations that shape and limit system operations, including official records retention and disposition policies
   - Assigned roles and responsibilities (mappings to responsible agency programs and staff) for system design, development, implementation, operation, administration, audit, etc. (See U.S. Department of Homeland Security (2024) for a discussion of AI/ML-related roles.)
   - Communications plans involving stakeholders
   - Risk assessments and recommendations

- Staff training plans
- Cybersecurity controls
  *Note: In New Jersey, the Office of Homeland Security and Preparedness' Statewide Information Security Manual (2024) sets forth cybersecurity policies, standards, processes and guidance for the State's information programs.
- Decisions to migrate a system to another platform or to decommission a system
- Contractual terms and conditions, including service level agreements, which govern relationships with vendors who provide system platforms, software, services, etc.

b. Data/Data-Records. These records include documentation of the data identified by the governance function, which are used to create, train, test, operate and manage the AI/ML system, **as well as the actual data compilations that serve as the content for the systems**. Data records also include meta-data associated with AI/ML data compilations – for example, names and functional descriptions (purposes for which the data is used), authorship, dates created/updated, dependencies, transformations/augmentations such as changes used to combine or anonymize data elements, create proxy values for data, etc. Examples of data/data records include:
   - System data -- databases, data sets and other compilations, which can be structured (for example, table-oriented databases), semi-structured (for instance, delineated text files, documents, spreadsheets) and unstructured (such as pictures, graphics, chats, audio and video files)
   - Meta-data as described above
   - Web sites and social media link (AI/ML software can crawl and *learn* sites by navigating a set of links)
   - Log files – files reflecting system events including end user interactions, security alerts, performance issues, etc.
   - Prompts (inputs that trigger queries and requests processed by AI/ML systems) and responses/outputs generated by the systems

     *Note: Agencies will need to consider whether it is feasible to store prompts and outputs produced during normal system operations for fixed time periods. The logistics and costs for doing so may prove prohibitive for large-scale systems, particularly those used by government agencies to serve the public. Alternately, for low impact systems, prompts may generate non-sensitive, ephemeral outputs and so may not warrant coverage in the system retention schedule. If the agency decides it cannot accommodate storage of these entities or believes that they are ephemeral, it would still be wise to document how prompts and outputs are produced/used and the reasons for not storing them.

- Classifications that indicate whether the records/data used by the system are public, confidential, private, etc. (Data classifications will inform cyber security controls enacted via governance directives.)

  *Note: AI/ML systems may employ combinations of internal and third-party data resources and combinations of in-house and Cloud-based storage. For Cloud-based storage of agency-owned data, use of the State's suggested controls for Cloud storage would be a best practice (New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit, 2019). The guidelines make it clear that decisions about retention and disposition of agency-owned data fall under the exclusive purview of the agency. Handling data provided by third parties is a more complicated consideration, which will likely connect with negotiated contractual provisions established by the governance function.

c. Performance/Measurement Records. Agencies will generate these records as they test, operate and use an AI/ML system in accordance with the goals and objectives set forth by the governance function. Examples of performance/measurement records include:
   - Reports and metrics that plot actual system performance against desired operational capacities and outcomes defined by the governance function (for example, end-user satisfaction ratings, assessments of citizen engagement with the system, transactions handled within a specific timeframe, internal and/or third-party reviews of accuracy, completeness, observed bias(es) and/or usability, evaluations of efficiency measures/cost savings associated with task automation, etc.
   - Readings of a system's transparency and understandability via ad-hoc and/or structured stakeholder feedback, subject matter expert assessments, industry and/or cross agency benchmarks, etc.
   - Quality control and test records that reflect processes used to ensure the accuracy, reliability, validity and integrity of data used by the system
   - Results of cyber security and operational audits
   - Reports of broader consequences for humans (for example, job losses or shifts in responsibilities due to automation, complaints regarding privacy violations stemming from stepped up surveillance, increased denials of benefits due to automated decision-making, etc.)

d. Monitoring/Management Records. In this category, records document the decisions and actions the agency takes to implement, control, adjust, secure, and ultimately, decommission a system in accordance with directives emanating from the governance function and information drawn from performance/measurement records. Examples include records reflecting:

- Corrective action plans designed to adjust data sources, language models, business rules and related system resources to address issues and/or improvement opportunities surfaced in audits or other evaluations
- Responses to specific incidents involving breaches or harms caused by the operation of an AI/ML system
- Configuration control records showing significant adjustments to the system architecture and/or functions
- Changes to contractual terms and conditions due to evolving circumstances that affect system design or performance
- Changes (deletion, addition, substitution) of data sources
- Changes to language models, user interfaces and/or data transmission/transformation software
- Changes to storage platform(s) (for instance, moving from in-house to Cloud, switching Cloud vendors or adopting a hybrid arrangement)
- Significant reengineering of prompts (inputs used to interact with language models)
- Correcting for identified bias(es)
- Adjustments made for new or modified stakeholders
- Records disposition actions based on approved retention schedules and disposition requests per these guidelines; these actions will be documented in the State's authorized disposition action database, ARTEMIS (See Step 6.).

3. *Conduct a Value Assessment(s).* Based on the taxonomy, assign values to the AI/ML records. While traditional values -- for example, administrative, fiscal, audit, legal and historical, could apply to AI/ML records, it may be best to emphasize the level of human impact in this space – that is, to emphasize a risk management perspective. This is appropriate because, to a higher degree than previous technologies, AI/ML augments or drives the automatic generation of information that can have direct effects on the well-being of citizens, businesses and society. Indeed, it is for this reason that states and the federal government seek to place restrictions on the technology's use (Hooshidary, Canada and Clark, 2024; The White House, 2024).

As public agencies in New Jersey become more experienced in the use of AI/ML, broader methods of value assessment, including methods that blend traditional and sensitivity values, may surface. Ultimately, some systems may produce outputs of enduring, historical value such as meeting minutes, executive summaries of technical reports used for decision-making and other reports scheduled as permanent. For this reason, agencies should consult with the State Archives both prior to implementing AI/ML systems and before any final decisions to decommission them.

Following are value dimensions that agencies can consider. The value dimensions are tied to a simple sensitivity range that parallels information system categorizations found in cybersecurity/risk management regimes (New Jersey Office of Homeland Security and Preparedness, 2024, pp. 51-52):

a. Low -- System generates/stores records that have limited or no impact on individual citizens, businesses or broader society; examples may include records associated with a system that supports agency employees in answering routine questions about or locating information on agency forms, procedures and policies, summarizing routine meeting dialogues, drafting routine correspondence that employees must review/approve before sending, etc.

b. Moderate -- System generates/stores records that affect individuals and businesses such that inaccurate or misleading outputs may inconvenience end-users or frustration them, but that will entail no- or low-risk of any lasting harm and/or broader societal impacts; examples may include outward facing (public) chatbots regarding routine agency forms, services, procedures and policies, informational guides on general licensing requirements, summaries of public meeting minutes, etc.

c. High -- System generates/stores records that affect individuals, businesses and/or society in substantial, consequential ways; examples may include records associated with a system that generates decisions on citizens' applications for social or medical benefits coverage, produces recommendation for job eligibility, serves as a self-regulating mechanism for critical infrastructure, etc.

> *Note: As with many types of governmental records, AI/ML system records may bridge or overlap the value dimensions above. That is, different system records may have varying sensitivity levels -- from *low to moderate*, *moderate to high*, *low to high*. A common approach to assessment in cases involving overlapping values is to assign the highest level to the system as a whole – for example, if the overlapping range is *low to high*, assign the *high* value to all system records. If this approach is not feasible or desirable, then the agency can opt for a more granular approach and assign values to the involved records on a series-by-series basis. The discussion in Step 4 below covers both of these approaches.

4. *Assign Retention and Disposition Policies*. Based on the value assessments conducted in Action Step 3, assign retention and disposition polices to the AI/ML records. For the steps involved in creating official retention and disposition polices (schedules) in conjunction with DORES/RMS and the State Records Committee, consult the State Records Manual (New Jersey Division of Revenue and Enterprise Services, 2024c, pp. 10-13).

Before proceeding, be aware that there may be use cases that do not require the creation of new AI/ML record series. Specifically, if the agency uses the technology to produce only low sensitivity outputs and all those outputs must be reviewed and approved by designated, responsible employees, then the agency may be able to focus on scheduling those outputs alone and not the entire system. An example use case would be a system that produces routine correspondence, operational meeting summaries or statistics used in an agency's monthly report, all of which are reviewed by designated, responsible employees. Here, general schedule items such as external correspondence, electronic resource files and monthly reports may be used for AI/ML records retention scheduling. Review available general retention schedules for these routine types of records online at the DORES/RMS web site and also review the New Jersey State Records Manual (New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit, 2024c). RMS will assist agencies in using existing records series for AI/ML records.

a. Following is an example AI/ML record series taxonomy, along with example retention and disposition policies for each series. Agency retention/disposition scheduling efforts may result in record series like those shown below **or** be different based on the agency's circumstances and the characteristics of its system(s). Work with RMS to settle upon a records retention/disposition scheme.

   The tables show two possible approaches to AI/ML records retention and disposition scheduling: Table 1, system-wide scheduling with a single policy assigned to all records series (easiest to promulgate and administer, but may foster over-retention and/or pre-mature disposition actions); and Table 2, granular scheduling series-by-series (may be cumbersome to administer and maintain, but provides the greatest degree of control).

   *Note: The application of any AI/ML retention/disposition regime pre-supposes that the agency has taken steps to ensure either:

   - The underlying system infrastructure upon which records generation, receipt and storage depends remains active for the length of the longest records retention period involved; or
   - There is an actionable plan to migrate records to a successor system that addresses retention/disposition requirements.

   Because the use of AI/ML likely entails substantial reliance on third-party system infrastructures and potentially, third-party data resources, agencies will need to **align contractual terms to assure system availability for the duration of all retention periods**.

Table 1. Example of System-wide Retention Scheduling

Example Record Series	**Retention/Disposition Policy by Sensitivity Level**		
	Low	**Moderate**	**Low**
• Governance Records • Data/Data Records • Performance/Management Records • Monitoring/Management Records	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy

Table 2. Series-by-Series Scheduling

Example Record Series	**Retention/Disposition Policy by Sensitivity Level**		
Governance Records	**Low**	**Moderate**	**High**
Organizational (charter) documentation including: feasibility studies; directives to implement system; stake-holder rosters/communications; goals/objectives of system; citations to governing laws and regulations; system policies/procedures; assigned roles/responsibilities; communications plans; status reports; decisions to migrate to another platform or to decommission; and project management files	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Technical specifications including: design/development documentation; bias assessments/reports; test plans/results; and system configuration information	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Budget and expenditure records (Assumes these are copies, with original records kept by budget/fiscal officers)	3 Years/Destroy	3 Years/Destroy	3 Years/Destroy
Risk management records including assessments and recommendations	As updated/Destroy	3 years/Destroy	7 years/Destroy
Staff training plans	As updated/Destroy	As updated/Destroy	As updated/Destroy
Contractual terms and conditions	7 years following termination of contract/Destroy	7 years following termination of contract/Destroy	7 years following termination of contract/Destroy

Example Record Series (Series-by-Series Continued)	**Retention/Disposition Policy by Sensitivity Level**		
Data/Data Records	**Low**	**Moderate**	**High**
Source data and associated meta-data (databases, data sets and other compilations), web sites and social media records used by the system	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Records/data classifications	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Prompts and responses/outputs generated by the systems (As noted previously, it may not be feasible or necessary to retain these records, but to the extent that they are retained, retention/disposition policies are in order.)	Retain until business use ceases/Destroy	1 year/Destroy	7 years/Destroy
Log files – files reflecting system events including end user accesses, tracked changes to databases, security alerts, performance issues, etc.	As updated/Destroy	Maintain until no-longer needed for operational and/or management control purposes/Destroy	Maintain until no-longer needed for operational and/or management control purposes/Destroy

Example Record Series (Series-by-Series Continued)	**Retention/Disposition Policy by Sensitivity Level**		
Performance/Measurement Records	**Low**	**Moderate**	**High**
Reports and metrics that plot actual system performance against desired outcomes defined by the governance function; readings of a system’s transparency and understandability; and quality control and test records	As updated/Destroy	Maintain until no-longer needed for operational and/or management control purposes/Destroy	Maintain until no-longer needed for operational and/or management control purposes/Destroy
Cybersecurity and operational audit reports/evaluations	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Reports of consequences for humans (for example, job losses or shifts in responsibilities due to automation, complaints regarding privacy violations stemming from stepped up surveillance, increased denials of benefits due to automated decision-making, etc.)	N/A	N/A	7 years following decommissioning or migration to replacement platform/Destroy

Example Record Series (continued)	**Retention/Disposition Policy by Sensitivity Level**		
Monitoring/Management Records	**Low**	**Moderate**	**High**
Corrective action plans (to address audit findings) and status reports	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Responses to specific incidents involving breaches or harms caused by the operation of an AI/ML system or process	7 years following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Change files documenting adjusts and corrections to the system, including: contractual terms and conditions; deletion, addition or substitution of data sources; language models, user interfaces and/or data transmission/transformation software; storage platform(s); reengineering of prompts (inputs used to interact with language models); and identified bias(es)	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Configuration control records showing significant adjustments to the system architecture and/or functions	Retain until business use ceases/Destroy	1 year following decommissioning or migration to replacement platform/Destroy	7 years following decommissioning or migration to replacement platform/Destroy
Cyber security controls including plans and configurations settings	As updated/Destroy	3 years following update/Destroy	7 years following update/Destroy
Records disposition actions based on approved retention schedules and disposition requests per these guidelines Note: The State's automated records disposition system, ARTEMIS, houses these records. (See Action Step 6.)	Permanent	Permanent	Permanent

5. ***Choose Modes of Records/Data Storage***. As can be seen from the record series taxonomy, AI/ML systems involve both document-based records like feasibility studies, reports and corrective action plans, and data-oriented compilations that serve as the foundational resources for language models and system software. Also, as noted, agencies will likely use third party contractors, including Cloud service providers, for AI/ML, either exclusively or in tandem with in-house storage platforms. With these factors in mind, consider the following for agency AI/ML storage environments:

a. Adopt a digital-only records policy for AI/ML systems so that both documents and data records can be managed in computer-based form.

b. To the extent possible, use a single platform for all AI/ML records, thereby avoiding fragmented, application-by-application approaches to storage. Realistically though, for the foreseeable future, agencies may be faced with the need to manage data across multiple storage platforms – for example, an office software suite including electronic mail (in-house or Cloud-based) for documentary forms of records and a combination of in-house and Cloud-based storage for data.

c. Ensure that the storage platform(s) incorporates features that enable the agency to implement basic records management functions like policy-based retention and disposition, as well as general principles, practices and standards that support these functions. Doing this will not only bolster the agency's posture relative to records management, but also relative to risk management, cybersecurity and overall accountability and transparency. Accordingly, agencies may wish to review the following to develop records management requirements for their AI/ML systems specifications and contracts:

- Through its Federal Electronic Records Modernization Initiative, the National Archives and Records Administration (2024) provides a model that covers the basic functions that federal agencies must implement to support their records management programs. These requirements, which broadly apply to New Jersey's government sector as well, cover the life cycle of records: capture (including creating/declaring a record); maintenance and use; disposal; transfer; metadata; and reporting. While not all of the requirements here relate to AI/ML, the overall model does touch upon key functions that undergird records retention scheduling and disposition in all settings, as well overall records system integrity, accountability and transparency.

- Looking to the professional non-profit sector, the Association of Records Managers and Administrators International's Generally Accepted Recordkeeping Principles © (2017) highlights the foundations for information governance, including accountability, transparency, integrity, protection, compliance, availability, retention and disposition. Agencies building AI/ML systems would do well to consult and incorporate these principles in their system specifications. Likewise, The Association for Intelligent Information Management (AIIM) (2024) provides useful guidance on structuring AI/ML systems. The organization stresses the institution of policies and protocols in the areas of access control, data encryption, searching, private data identification, automated data classification and user/intent /context analysis.

- The IT industry offers tools and platforms the agency can employ to manage records used by AI/ML systems, and that facilitate the implementation of retention and disposition policies. The elements included in these tools/platforms may involve: encryption of data in transit and at rest; the ability to identify and inventory AI applications used by the agency; electronic discovery (for legal proceedings); security regime compliance reports (for instance, HIPAA, Criminal Justice Information System (CJIS), Safeguards, etc.); role-based security for data access/manipulation; data loss prevention (via detection, labelling and control of sensitive data); assignment of retention periods to specifically labelled records; centralized review and approval of disposition actions; secure deletion (destruction) of records; and audit trailing of deletion actions.

  By way of illustration and not endorsement, Microsoft (2024) is an example of a firm that offers solutions covering elements such as these, as are firms like Gimmal and Preservica and others. In the same illustrative way, firms such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud, Oracle Cloud, Snowflake and Databricks are examples of third-party Cloud platforms/services that feature security and compliance features, including data retention management.

- At a minimum, if the agency is dealing with a third party for data storage, ensure the contractual agreement includes controls such as those suggested in the State's records management guidelines for Cloud storage (New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit, 2029).

d. When it comes to tracking retention and disposition of AI/ML records, it is important to keep an important distinction in mind. Documentary records like reports and electronic mail can be managed at the item or entity level. That is, it is feasible to manage individual instances of documentary records as discrete entities from the beginning to the end of their respective retention periods. It may also be possible to do this with semi-structured and unstructured records. From a practical perspective, however, it will likely be infeasible to accomplish this with respect to individual entries (fields) in databases. In most cases, retention periods will apply to a database in its entirety. Thus, retention periods will relate to the data base as a whole or possibly to dated versions (snap shots or copies) of the database taken at pre-defined time intervals.

6. *Implement and Monitor/Evaluate the Program*. After completing the five preceding steps, work with DORES/RMS to implement and monitor/evaluate the retention and disposition program. In this connection, agencies may use one or two formats for disposition actions following the expiration of AI/ML records retention periods: *single-action* and *phased* disposition. Single-action disposition requests relate to AI/ML records that can be managed at the item or entity level such as reports and electronic mail. For single-action requests, the agency periodically identifies specific records that have met or exceeded their approved retention periods and submits individual requests for each. In contrast, phased disposition is most useful for frequently updated databases and other bulk data compilations. For these requests, the agency obtains authority to dispose of AI/ML records on an on-going basis for renewable time periods (6 months or year) without having to submit requests for individual disposition actions.

Referring to the example retention schedules under Action 4, if the agency adopts for a system-wide approach (single retention/disposition policy assigned to all records series in the system), only the single-action disposition format will be feasible. Agencies that opt for the record series-by-record series format may use both disposition formats. For example, again referring to the example retention schedules under Action 4, use phased disposition for source databases, metadata, log files and prompts/outputs, and use the single action format for the balance of AI/ML records.

> *Note: Agencies will obtain authorizations for and maintain records of their disposition actions through use of the online system known as ARTEMIS. Use of ARTEMIS requires the agency to register staff authorized to request and approve disposition actions. Once registered, the agency will be able to submit disposition requests to RMS via ARTEMIS, including the entry of approved schedule/record series numbers, and then receive online authorizations to proceed with disposition actions. ARTEMIS includes automated workflow features that guide the agency through the steps in the authorization process. Using ARTEMIS provides for legally defensible disposition actions.

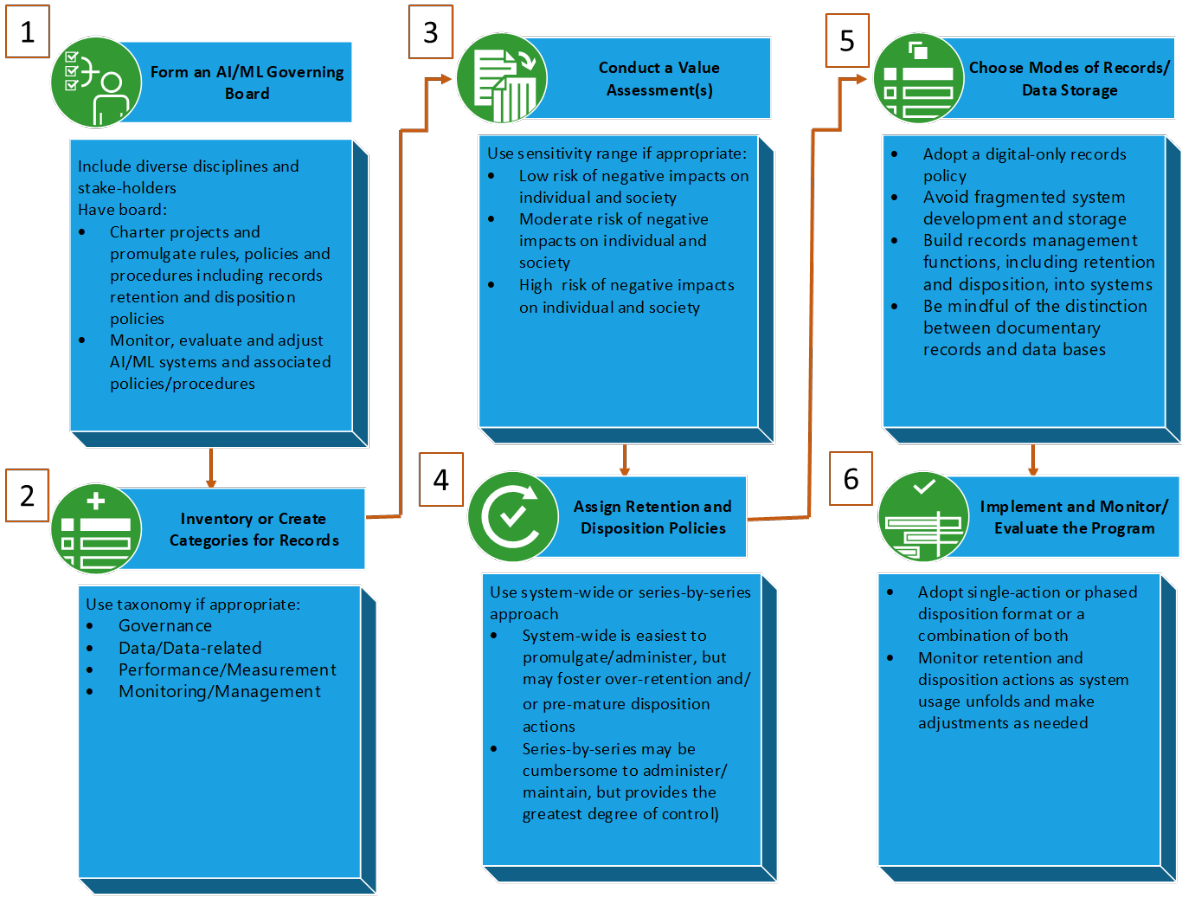
Monitor and evaluate retention and disposition actions as system usage unfolds and make adjustments as required. While the need for monitoring, evaluation and adjustment is implicit in any business system or program, agencies should give these functions particular emphasis given the rapidly evolving and potentially expansive impacts of AI/ML technology.

Conclusion

This presentation provided background on AI/ML technology, its potential use cases and the possible benefits and drawbacks associated with those uses. As summarized in Figure 2 below, it then provided guidelines on how to address AI/ML records retention and disposition within a governance framework based on risk/sensitivity levels. The levels align with the potentially transforming and yet still-uncertain effects of the technology.

The hope is that these guidelines will help New Jersey's governmental officials gain intellectual control over the contents and outcomes of their AI/ML systems and through this, the ability to institute accountable and legally-defensible records retention/disposition policies. From a broader perspective, by implementing governance measures and achieving intellectual control over AI/ML, our public agencies will be better-positioned to realize the transformative potential of the technology.

Figure 2. Summary of Action Steps for Establishing AI/ML retention and Disposition Policies



1

Form an AI/ML Governing Board

Include diverse disciplines and stake-holders
Have board:

- Charter projects and promulgate rules, policies and procedures including records retention and disposition policies
- Monitor, evaluate and adjust AI/ML systems and associated policies/procedures

2

Inventory or Create Categories for Records

Use taxonomy if appropriate:

- Governance
- Data/Data-related
- Performance/Measurement
- Monitoring/Management

3

Conduct a Value Assessment(s)

Use sensitivity range if appropriate:

- Low risk of negative impacts on individual and society
- Moderate risk of negative impacts on individual and society
- High risk of negative impacts on individual and society

4

Assign Retention and Disposition Policies

Use system-wide or series-by-series approach

- System-wide is easiest to promulgate/administer, but may foster over-retention and/ or pre-mature disposition actions
- Series-by-series may be cumbersome to administer/ maintain, but provides the greatest degree of control)

5

Choose Modes of Records/ Data Storage

- Adopt a digital-only records policy
- Avoid fragmented system development and storage
- Build records management functions, including retention and disposition, into systems
- Be mindful of the distinction between documentary records and data bases

6

Implement and Monitor/ Evaluate the Program

- Adopt single-action or phased disposition format or a combination of both
- Monitor retention and disposition actions as system usage unfolds and make adjustments as needed

References

Association for Intelligent Information Management. (2024). “Safeguarding Your Organization’s Data in the Age of AI”, AIIM, Silver Spring Md.

Association of Records Manager and Administrators. (2017). Generally Accepted Recordkeeping Principles. © ARMA International, www.arma.org/principles.

Barney, N. and Lutkevich, B. (2024, August). “What is Language Modeling?” TechTarget, https://www.techtarget.com/searchenterpriseai/definition/language-modeling

Fleming, G. (2024, August). “The Top 10 Key Components to Artificial Intelligence”, https://www.linkedin.com/pulse/top-10-key-components-artificial-intelligence-gerry-fleming-ri0rc

Filipsson, F. (2024, July). “Artificial Intelligence Hardware – What is Required to run AI?”. Redress Compliance, https://redresscompliance.com/artificial-intelligence-hardware-what-is-required-to-run-ai/

Future of Privacy Forum. (2024). *U.S. State AI Legislation, How U.S. Policymakers Are Approaching Artificial Intelligence Regulation*, https://fpf.org/wp-content/uploads/2024/09/FINAL-State-AI-Legislation-Report-webpage.pdf

Glasscock, A. (2024). “Generating Opportunity: The Risks and Rewards of Generative AI in State Government”. National Association of State Chief Information Officers, https://www.nascio.org/resource-center/resources/generating-opportunity-the-risks-and-rewards-of-generative-ai-in-state-government/

Government Accounting Office. (2021). *Artificial Intelligence, an Accountability Framework for Federal Agencies and Other Entities,* https://www.gao.gov/assets/gao-21-519sp.pdf

Hooshidary, S., Canada, C., Clark, W. (2024). “Artificial Intelligence in Government: The Federal and State Landscape”. National Conference of State Legislatures, https://www.ncsl.org/technology-and-communication/artificial-intelligence-in-government-the-federal-and-state-landscape#:~:text=This%20legislation%20is%20designed%20to,AI%20practices%20across%20government%20agencies

Lawton, G. (2024). “What is GenAI? Everything You Need to Know”. TechTarget, https://www.techtarget.com/searchenterpriseai/definition/generative-AI

Microsoft (2024). Microsoft Purview data security and compliance protections for generative AI apps. Microsoft, https://learn.microsoft.com/en-us/purview/ai-microsoft-purview

Mooradian, N. (2019). “AI, Records, and Accountability”. ARMA International, https://magazine.arma.org/2019/11/ai-records-and-accountability/

National Archives and Records Service. (2024, September). “Federal Electronic Records Modernization Initiative (FERMI)”. NARA, https://www.archives.gov/records-mgmt/policy/fermi

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0),* https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

New Jersey AI Task Force. (2024). *Final Report to the Governor*, https://www.nj.gov/governor/docs/Final-2024-NJ-AI-Task-force-Report-to-Governor.pdf

New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit. (2019). Records Management Guidelines for Cloud-based Records Storage, https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforRecordsManagementintheCloud.pdf

New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit. (2024a). *Guidelines on Retention Scheduling Public Records Stored on Electronic Messaging Platforms,* https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforSchedulingElectronicMessagingRecordsforRetentionandDisposition.pdf

New Jersey Division of Revenue and Enterprise Services, Records Management Services Unit. (2024b). *Guidelines on Retention Scheduling Public Records Stored on Social Media Platforms*. https://www.nj.gov/treasury/revenue/rms/pdf/GuidelinesforSchedulingSocialMediaRecordsforRetentionandDisposition.pdf

New Jersey Division of Revenue and Enterprise Services. (2024c). New Jersey Records Manual, https://www.nj.gov/treasury/revenue/rms/manual/RMSManual.pdf

New Jersey Office of Homeland Security and Preparedness. (2024). Statewide Information Security Manual, https://www.cyber.nj.gov/home/showpublisheddocument/36/638568130115330000

Office of Information Technology, Office of Homeland Security and Preparedness and NJ Cybersecurity & Communications Integration Cell. (2023). *AI Acceptable Use Joint Circular*, https://www.nj.gov/circulars/23-oit-007.pdf

Organization of Economic Cooperation and Development. (2019). *Artificial Intelligence & Responsible Business Conduct*, https://mneguidelines.oecd.org/RBC-and-artificial-intelligence.pdf

Organization of Economic Cooperation and Development. (2024). *Assessing Potential Future Artificial Intelligence Risks, Benefits and Policy Imperatives,* OECD Artificial Intelligence Papers, No. 27, OECD Publishing, Paris, https://doi.org/10.1787/3f4e3dfb-en

Run:ai. (2024). *AI Infrastructure, 5 Key Components to Building Your AI Stack*, https://www.run.ai/guides/machine-learning-engineering/ai-infrastructure

U.S. Department of Homeland Security. (2024). *Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure*,https://www.dhs.gov/sites/default/files/2024-11/24_1114_dhs_ai-roles-and-responsibilities-framework-508.pdf

The White House. (2024). *Framework to Advance AI Governance and Risk Management in National Security*, https://home.treasury.gov/system/files/216/Framework-to-Advance-AI-Governance-and-Risk-Management-in-National-Security.pdf