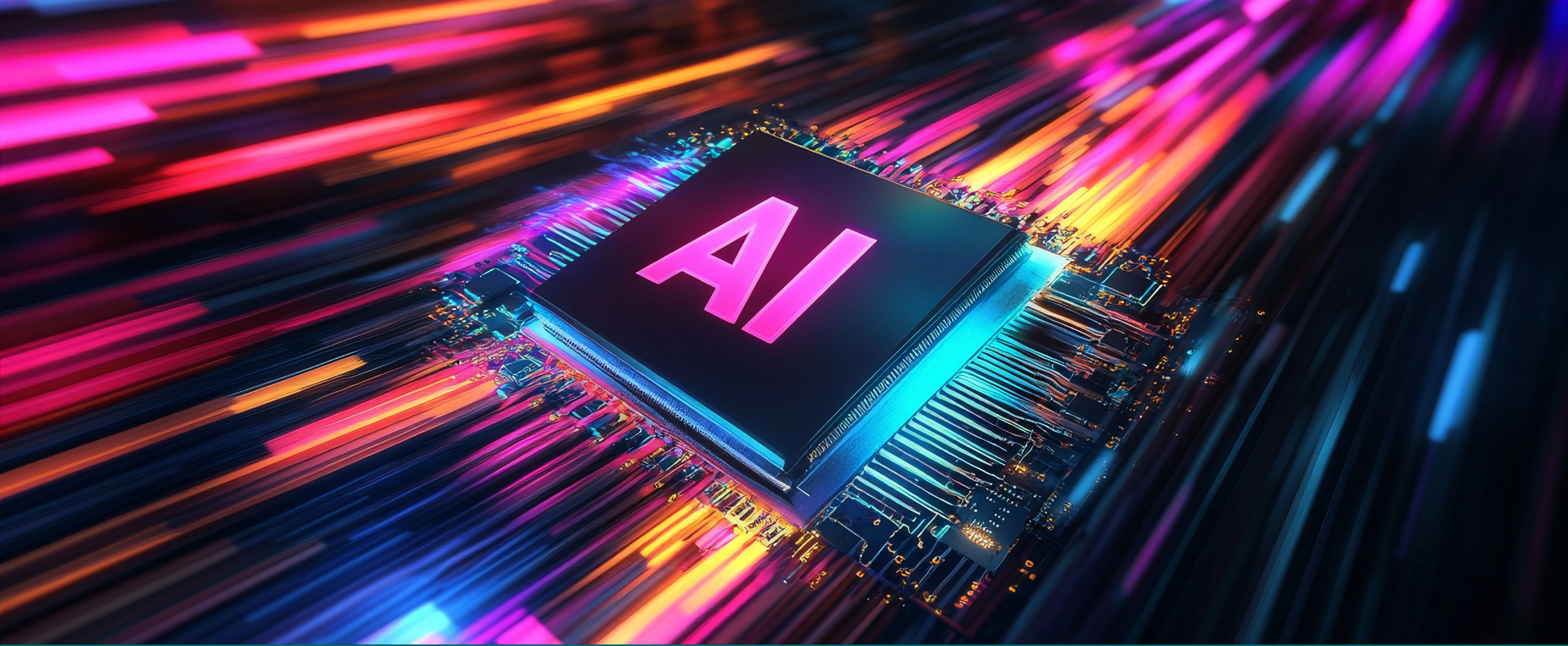


RECORDS COORDINATOR ALL-HANDS

APRIL 25, 2025

NORTH Dakota | Information Technology

Be Legendary.

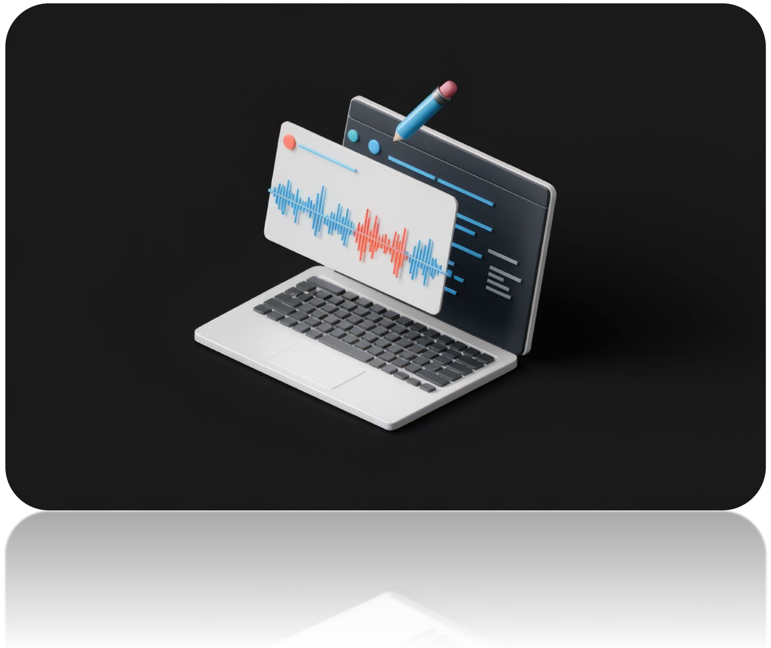
Agenda

- Getting Ready for AI
    - Introduction
    - Best Practices for AI Records
    - Key Takeaways
- News from Records Management

Overview

- **Introduction:**

  AI productivity tools (such as Copilot) do not inherently create "records" in the traditional sense (contracts, policies, or legal documents), but it generates new AI-powered content that may be considered records based on the definition in North Dakota Century Code 54-46-02.4 and may be subject to open records laws in North Dakota Century Code 44-04-18.



Getting Ready for AI – Know Your Data

- Understand what types of records and information you have
  - Where is it stored?
  - Who has access? How is access managed? How often is it reviewed?

- Know where you have sensitive data
  - SharePoint, Teams, Email (Exchange), One Drive, repositories outside M365…

Getting Ready for AI – Eliminate ROT

ROT: Redundant, Obsolete, Trivial

- Redundant: Information that is duplicated or has multiple versions without unique value.
- Obsolete: Outdated records no longer needed or relevant.
- Trivial: Records with little business value (e.g., old drafts or non-work-related content).

Note: Make sure you are adhering to your retention schedules– old doesn't always mean eligible!

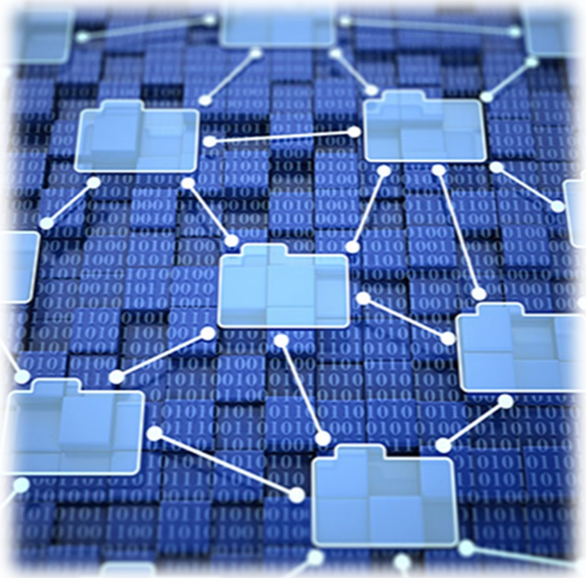
Getting Ready for AI – Data Cleanup

- AI tools have access to everything you have access to and can locate and make use of old and outdated information.
  - Clean up:
    - Emails
    - Unused drafts or older versions of documents
    - Duplicate copies stored in different places
    - Teams files that have not been accessed recently
    - Anything else that would result in incorrect or outdated information being located, referenced, or aggregated by generative AI.

Getting Ready for AI – Data Cleanup

Other Places You May Have Records & Data:

- **Local Storage**: Desktop, Documents Folder, Downloads Folder, Temporary Files and Caches
- **Shared Network Drives**: Company File Servers, Department-Specific Shared Folders, Network Storage
- **In the Cloud:** Google Drive, OneDrive, Dropbox, iCloud, MS SharePoint, ECMs
- **Email and Messaging Platforms:** Email inboxes and archives, attachments stored in emails or drafts, messaging apps
- **Business Applications and Databases:** ERP, CRM or related software (Salesforce, QuickBooks), project management tools (such as Trello)
- **External Storage Devices:** USB drives, external hard drives, SD cards, CDs/DVDs
- **Web Browsers & Temporary Internet Files:** Browser downloads folder, auto-saved forms and credentials, bookmarks



Getting Ready for AI – Retention Schedule

- Ensure your retention schedule is up-to-date and includes all record types in your environment
- If default retentions are set, ensure they match the requirements on your schedule, or an alternate process is in place
- Make sure records are being disposed of according to the schedule to avoid AI tools pulling expired records
- Work with your Records Coordinator to make changes

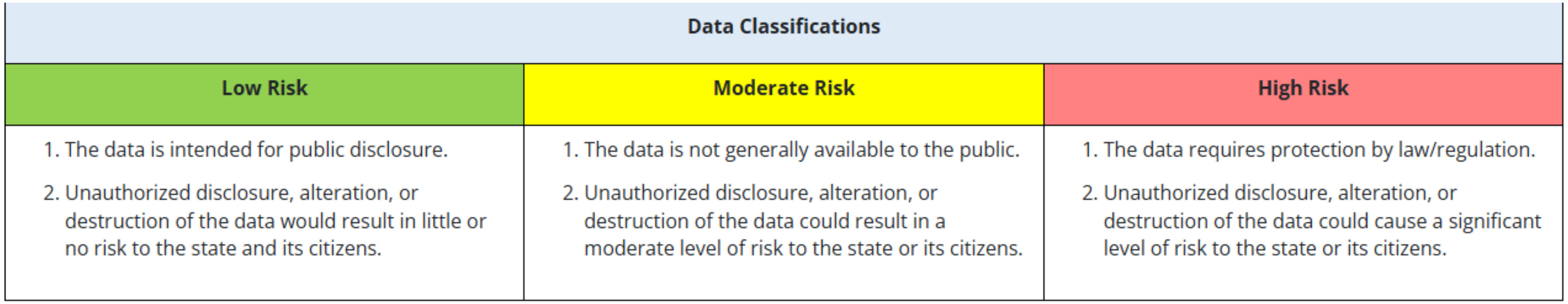
Public link: ND Records Retention Schedules

Getting Ready for AI – Classifying Data

Classification

Identify the classification of the data contained in AI-generated content using the guidelines in the Data Classification Policy.

- Aids in decisions to restrict access by AI tools
- Helps prevent misuse of sensitive information
- Sets up environment for future data governance success



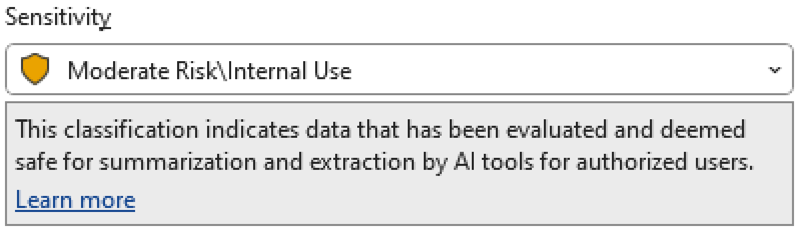
Data Classifications		
Low Risk	**Moderate Risk**	**High Risk**
1. The data is intended for public disclosure. 2. Unauthorized disclosure, alteration, or destruction of the data would result in little or no risk to the state and its citizens.	1. The data is not generally available to the public. 2. Unauthorized disclosure, alteration, or destruction of the data could result in a moderate level of risk to the state or its citizens.	1. The data requires protection by law/regulation. 2. Unauthorized disclosure, alteration, or destruction of the data could cause a significant level of risk to the state or its citizens.

Getting Ready for AI – Data Tagging

Tagging/Labeling

Once data is classified, technical controls can be applied to help protect high-risk data

- In M365, sensitivity labels can help control:
  - Access: Copilot can't access, can't extract
  - Behavior: User can't copy to clipboard, can't print, can't send externally
  - Retention: Can be used in conjunction with retention labels to meet regulatory requirements

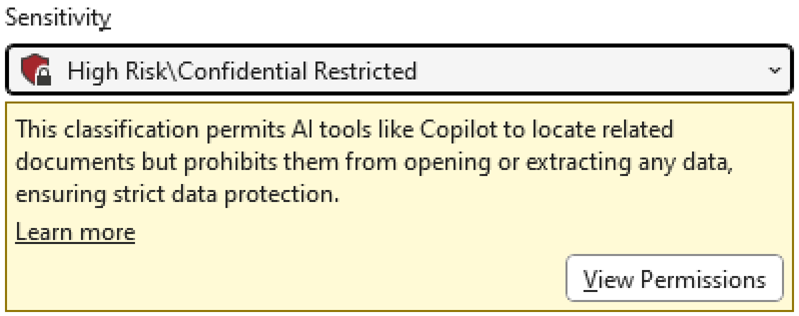


Sensitivity

Moderate Risk\Internal Use

This classification indicates data that has been evaluated and deemed safe for summarization and extraction by AI tools for authorized users.

Learn more

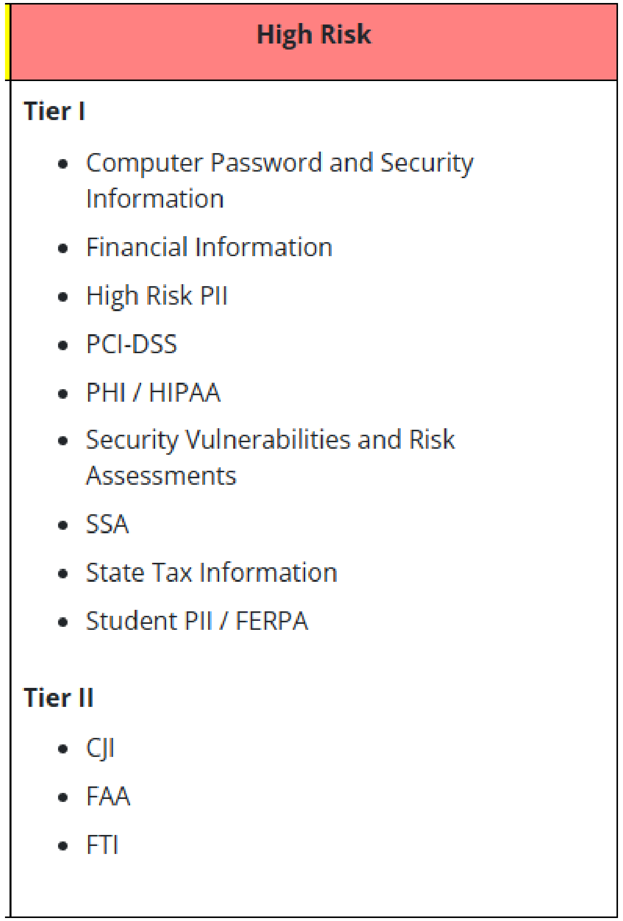


Sensitivity

High Risk\Confidential Restricted

This classification permits AI tools like Copilot to locate related documents but prohibits them from opening or extracting any data, ensuring strict data protection.

Learn more



High Risk

Tier I

- Computer Password and Security Information
- Financial Information
- High Risk PII
- PCI-DSS
- PHI / HIPAA
- Security Vulnerabilities and Risk Assessments
- SSA
- State Tax Information
- Student PII / FERPA

Tier II

- CJI
- FAA
- FTI

Getting Ready for AI – User Access Reviews

Permission and Access Control Validation: Use Data Classification

- **Copilot:**
  - Complete Initial Review of M365 user access – Managers/Site Owners
  - Low/Moderate Risk Data: Review annually at minimum
  - High-Risk Data: Review quarterly, or more frequently if needed to meet regulatory requirements
- **Other AI tools:**
  - If using web capabilities, access low-risk data only
  - Refer to Artificial Intelligence Policy

Best Practices – Identification and Awareness

Identification and Awareness

- Identify AI-generated or AI-Assisted content that qualifies as a record
- Manage most content similarly to other Microsoft Office suite items
- Be aware of Copilot usage in meetings, chats, or workflows and what records are being created due to this usage.

New Record Types

- AI-Generated Drafts & Summaries
  - Meeting Summaries
  - Email Summaries
  - Document or Presentation Drafts
- AI-Generated Code & Workflows
  - Power Automate/Power App usage
- AI-Assisted Business Insights & Reports
  - Excel Data Analysis
  - Forecasts
- Adaptive AI-Chat Logs
  - AI-generated responses and logging in Teams chats & meetings

Best Practices – Review and Validation

Review and Validation

- Always review AI-Generated content for accuracy and completeness
- Use human oversight and validation before using AI-Generated records for decision-making.
- Open records exemptions, review and redaction

Best Practices – Retention, Compliance and Disposal

Retention, Compliance, Disposal

- Ensure AI-generated records are easily found through eDiscovery and meet legal hold requirements
- Ensure changed file names meet standard naming conventions
- Ensure AI-generated records' retentions do not conflict with existing retention policies
- Dispose of records according to established (or default) retentions
- Discard working copies, drafts, or reference materials as soon as possible and retain only final versions of records
- Ensure that AI-Generated or AI-Assisted records meet regulatory standards and guidelines. Some industries have strict compliance requirements for recordkeeping

Best Practices – Retention, Compliance and Disposal

Retention Defaults for Copilot:

- Chat Interactions (prompts and responses): 1 year
- Meeting Recordings, Transcriptions, Summaries: 60 days

- ✓ Subject to change
- ✓ Users need to manage if not compliant
- ✓ Other AI tools may not manage retention

Best Practices – Recording, Transcription, Summary

Recording, Transcription, Meeting Summaries

- Determine if Meeting Should be Recorded
  - If yes, manage the AI-generated or assisted records as you would those being created today
  - If no, consider the appropriateness and necessity of recording
    - Will recording have repercussions?
    - Could sensitive information be included in the transcription or summary?

- Follow Best Practices (meetings and email)
  - Avoid unnecessary recording/transcribing/summarizing
  - Ensure accuracy and context, protect sensitive information
  - Align with retention and open records
  - Adhere to agency guidance

Takeaways

- Get your information environment ready for AI by eliminating ROT, cleaning up data, classifying and tagging so technical controls and access restrictions can be applied
- Educate yourself and your staff on the capabilities, business use cases, risks, and considerations prior to onboarding Copilot or using other AI tools
- Identify records created or assisted by AI
- Ensure you are managing retention on these items (update retention schedules if needed)
- Ensure you understand eDiscovery practices and open records legal obligations
- Ensure you are protecting sensitive information and controlling access to it
- Be aware of your settings/options and don’t create any unnecessary records
- Keep informed as this technology changes
- Consult your legal counsel where needed

TIME FOR ...
QUESTIONS

News From Records Management

- ND ARMA Spring Seminar – last day to register is 4/28
- ND GRS Updates:

  Change to 011201 – ASSET MANAGEMENT RECORDS 4/23/25

  Removed 440101 – FORMS MASTERS 3/11/25
- RC Survey:
  - Getting started for new RCs, what training is available
  - Tracking disposals
- Next meeting June 2025, will have guest speaker TBA

Sharon Freeman is retiring June 1 after 34 years of service to the State of ND!

Contact NDIT Records Management:

Aimee Bader
State Records Administrator
Compliance & Records Team Lead
aimee.bader@nd.gov

Dawn Cote
Records Analyst
dcote@nd.gov

Sharon Freeman
Records Analyst
sfreeman@nd.gov

Visit our website: Records Management | North Dakota Information Technology