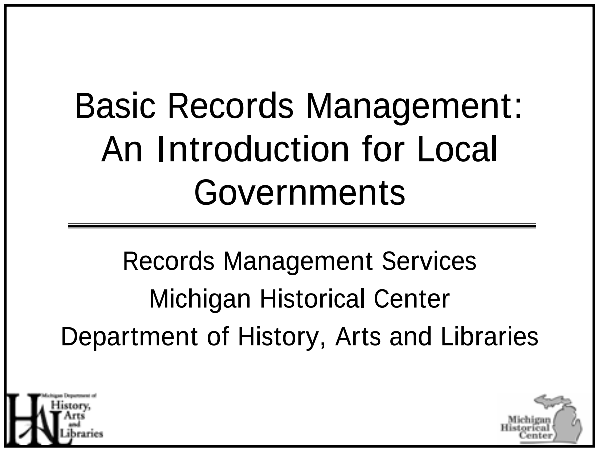
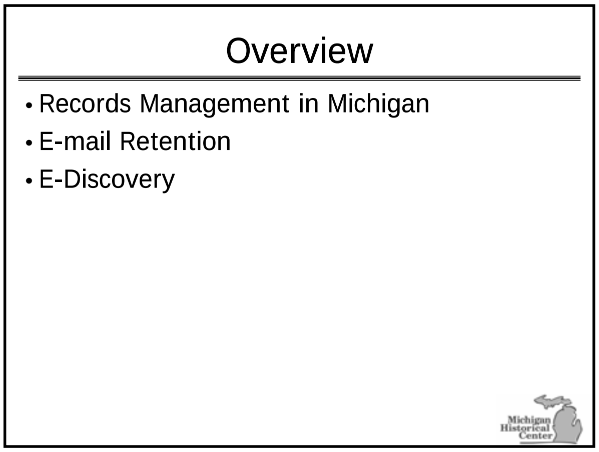


Basic Records Management: An Introduction for Local Governments

Records Management Services
Michigan Historical Center
Department of History, Arts and Libraries

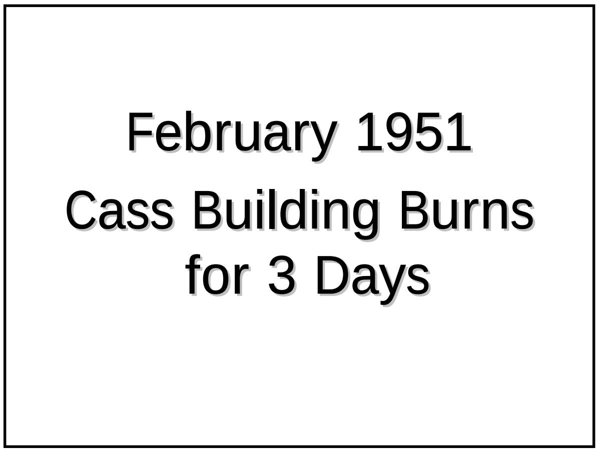


Overview

- Records Management in Michigan
- E-mail Retention
- E-Discovery

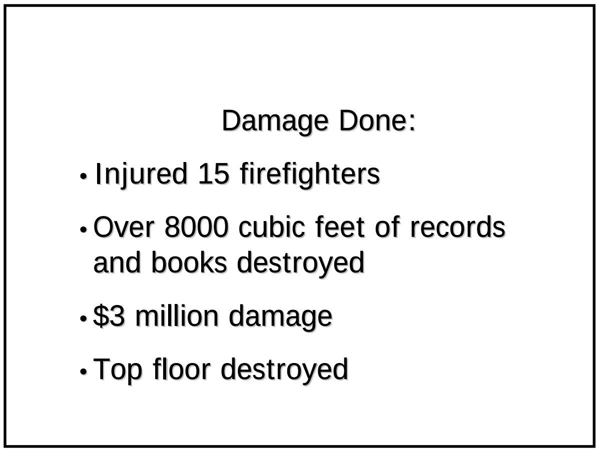
Origins

1913:	Michigan Historical Commission
1950:	Little Hoover Commission
1951:	State Office Building Fire
1952:	Records Management Legislation
1954:	State Records Center Opens
2001:	Department of History, Arts and Libraries (HAL) created
2002:	Executive Order moves RMS from DMB to HAL
2004:	State and local government records management services are merged



February 1951

Cass Building Burns for 3 Days



Damage Done:

- Injured 15 firefighters
- Over 8000 cubic feet of records and books destroyed
- $3 million damage
- Top floor destroyed

Michigan Department of History, Arts and Libraries

- Michigan Historical Center
  - Records Management Services
  - Archives of Michigan
  - Michigan Historical Museums
  - Office of the State Archaeologist
  - *Michigan History* Magazine
  - State Historic Preservation Office
- Library of Michigan
- Michigan Council for the Arts and Cultural Affairs
- Mackinac State Historic Parks

Laws

- M.C.L. 15.231-15.232

Freedom of Information Act, Definitions

- M.C.L. 18.1284-1292

Management and Budget Act, Records Management

- M.C.L. 399.1-10

Historical Commission Act

- M.C.L. 750.491

Penal Code, Public Records

- Note: The Michigan Compiled Laws are available online at http://www.legislature.mi.gov/.

What is Records Management?

- Management of the life cycle of a record
  - Creation
  - Storage
  - Retrieval
  - Retention
  - Protection
  - Disposition
- Ensures that authentic and accurate information can be retrieved quickly, easily and cost-effectively

Records Management Principles

- If the information is recorded it is a record
- Public records are evidence of government activities
- Destruction must be authorized by an approved Retention and Disposal Schedule
- Records supporting the same business process need to be stored together on media that will keep them accessible and usable for the entire retention period

Records Management Services

- Retention and Disposal Schedule development, review and approval
- Recordkeeping system consulting
- Microfilming and digital imaging services
- Education and training
- Disaster prevention and recovery assistance
- Records Center operations (state agencies only)

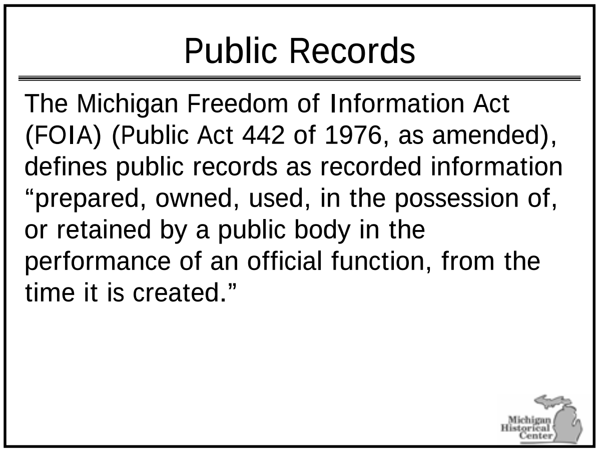
Our Customers

- Executive Branch
- Legislative Branch
- Judicial Branch
- Local Governments

Have you ever contacted the State of Michigan or visited our website to get records management information?

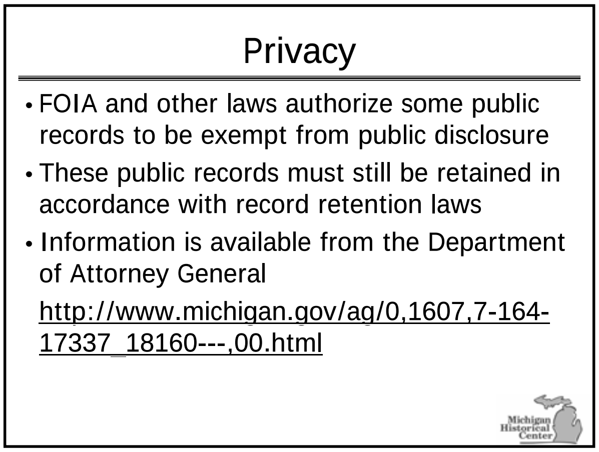
Yes

No



Public Records

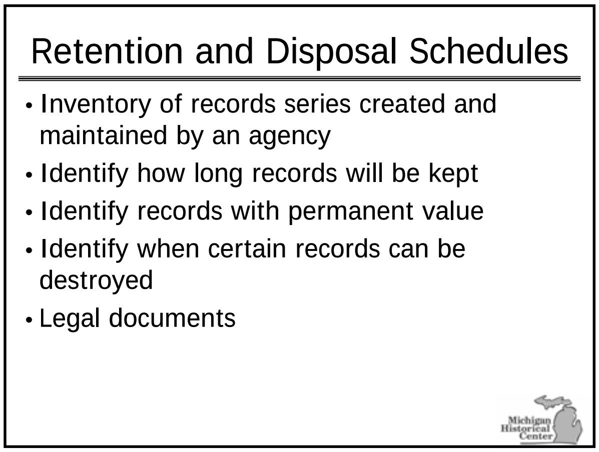
The Michigan Freedom of Information Act (FOIA) (Public Act 442 of 1976, as amended), defines public records as recorded information "prepared, owned, used, in the possession of, or retained by a public body in the performance of an official function, from the time it is created."



Privacy

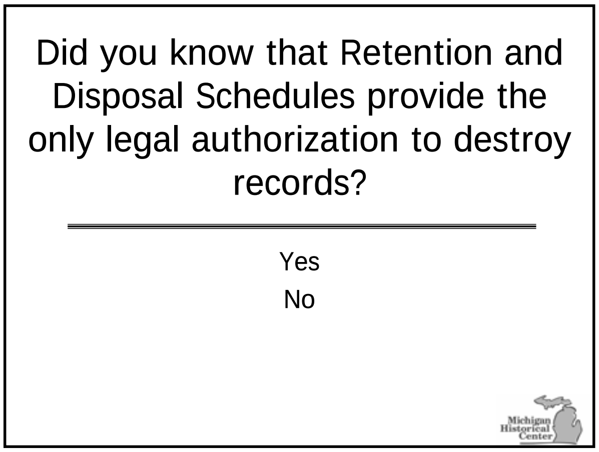
- FOIA and other laws authorize some public records to be exempt from public disclosure
- These public records must still be retained in accordance with record retention laws
- Information is available from the Department of Attorney General

  http://www.michigan.gov/ag/0,1607,7-164-17337_18160---,00.html



Retention and Disposal Schedules

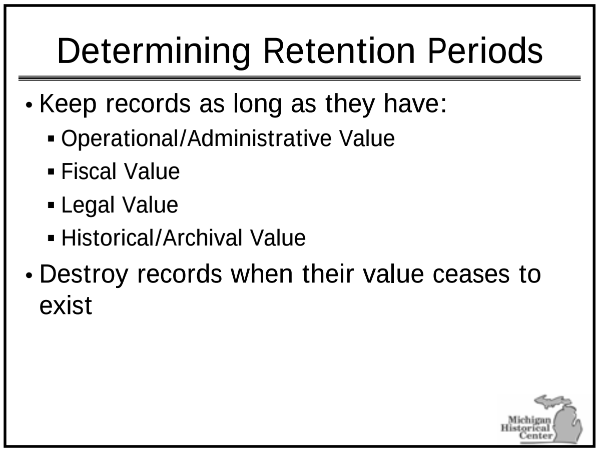
- Inventory of records series created and maintained by an agency
- Identify how long records will be kept
- Identify records with permanent value
- Identify when certain records can be destroyed
- Legal documents



Did you know that Retention and Disposal Schedules provide the only legal authorization to destroy records?

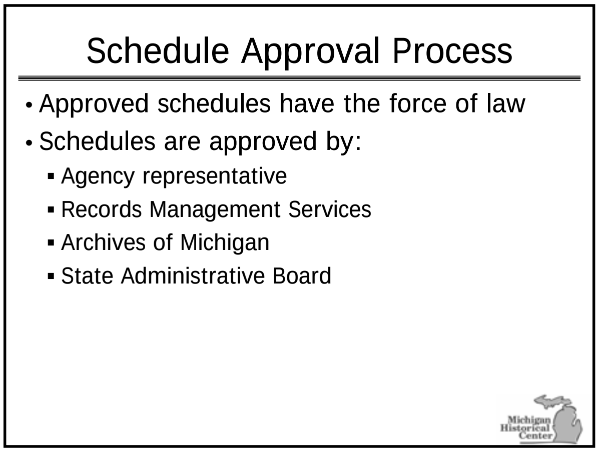
Yes

No



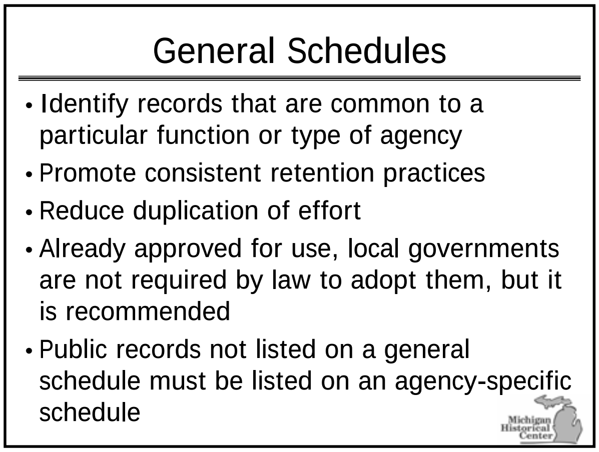
Determining Retention Periods

- Keep records as long as they have:
  - Operational/Administrative Value
  - Fiscal Value
  - Legal Value
  - Historical/Archival Value
- Destroy records when their value ceases to exist



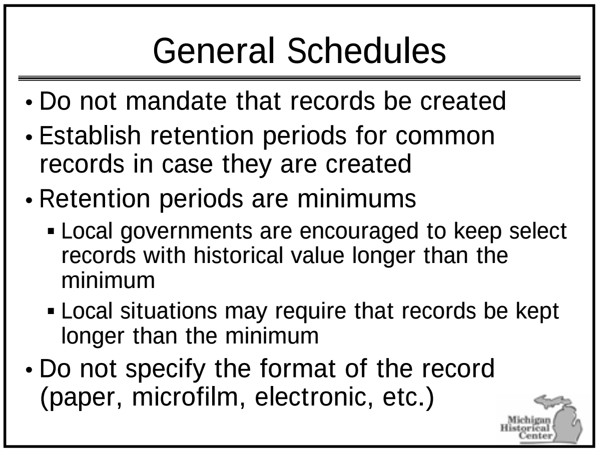
Schedule Approval Process

- Approved schedules have the force of law
- Schedules are approved by:
  - Agency representative
  - Records Management Services
  - Archives of Michigan
  - State Administrative Board



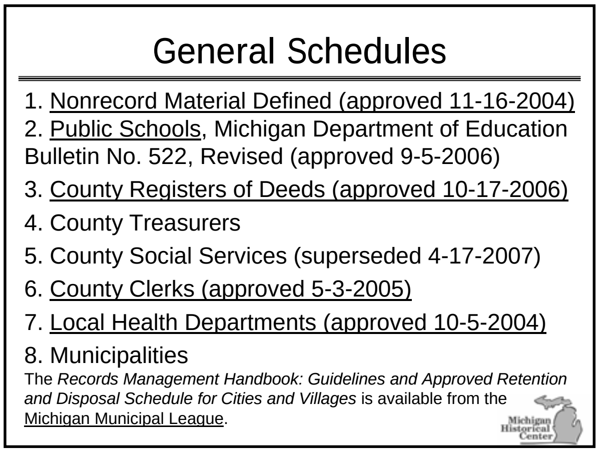
General Schedules

- Identify records that are common to a particular function or type of agency
- Promote consistent retention practices
- Reduce duplication of effort
- Already approved for use, local governments are not required by law to adopt them, but it is recommended
- Public records not listed on a general schedule must be listed on an agency-specific schedule



General Schedules

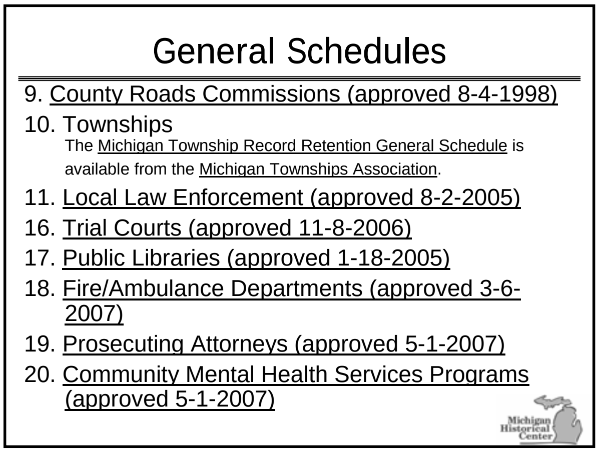
- Do not mandate that records be created
- Establish retention periods for common records in case they are created
- Retention periods are minimums
  - Local governments are encouraged to keep select records with historical value longer than the minimum
  - Local situations may require that records be kept longer than the minimum
- Do not specify the format of the record (paper, microfilm, electronic, etc.)



General Schedules

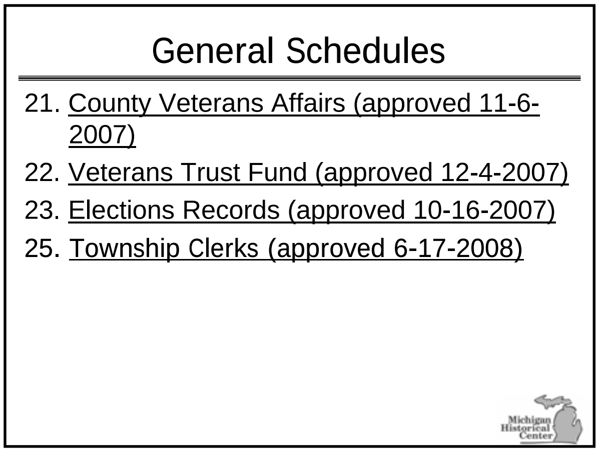
1. Nonrecord Material Defined (approved 11-16-2004)
2. Public Schools, Michigan Department of Education Bulletin No. 522, Revised (approved 9-5-2006)
3. County Registers of Deeds (approved 10-17-2006)
4. County Treasurers
5. County Social Services (superseded 4-17-2007)
6. County Clerks (approved 5-3-2005)
7. Local Health Departments (approved 10-5-2004)
8. Municipalities

The *Records Management Handbook: Guidelines and Approved Retention and Disposal Schedule for Cities and Villages* is available from the Michigan Municipal League.



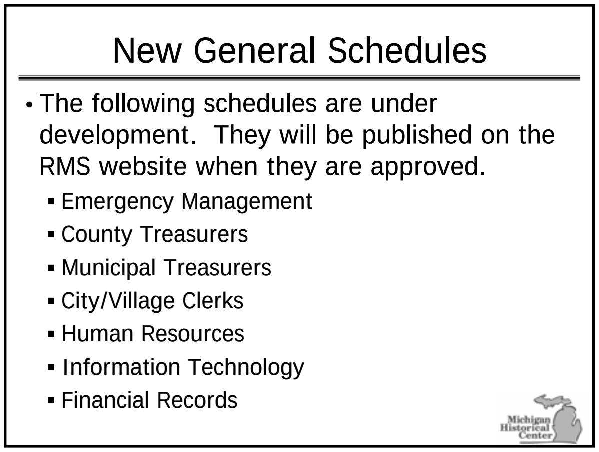
General Schedules

9. County Roads Commissions (approved 8-4-1998)
10. Townships
    The Michigan Township Record Retention General Schedule is available from the Michigan Townships Association.
11. Local Law Enforcement (approved 8-2-2005)
16. Trial Courts (approved 11-8-2006)
17. Public Libraries (approved 1-18-2005)
18. Fire/Ambulance Departments (approved 3-6-2007)
19. Prosecuting Attorneys (approved 5-1-2007)
20. Community Mental Health Services Programs (approved 5-1-2007)



General Schedules

21. County Veterans Affairs (approved 11-6-2007)
22. Veterans Trust Fund (approved 12-4-2007)
23. Elections Records (approved 10-16-2007)
25. Township Clerks (approved 6-17-2008)



New General Schedules

- The following schedules are under development. They will be published on the RMS website when they are approved.
  - Emergency Management
  - County Treasurers
  - Municipal Treasurers
  - City/Village Clerks
  - Human Resources
  - Information Technology
  - Financial Records

General Schedule #2—Public Schools

Approved
September 5,2006

Agency-Specific Schedules

- Cover records not listed on general schedules
- Records may be unique to a particular agency
- General schedule may not be available
- Agency must inventory and describe the records
- Agency must submit schedule for approval
- Specific schedules always supersede general schedules

Developing Schedules

- Inventory the records in the office
  - Survey filing systems: paper, microfilm and electronic
  - Use inventory forms to collect information (HAL-507)
- Determine how long records are needed
- Complete the Retention and Disposal Schedule form (MH-43)
  - Describe the records—why are they created, what information do they contain
- Submit the draft schedule to RMS for review and approval
- RMS will route the schedule to the approving agencies
- RMS will return the approved schedule

Nonrecord Material

- Full definition in General Schedule #1.
- Includes drafts, duplicates, convenience copies, publications and other materials that do not document agency activities.
- Can be disposed of when they have served their intended purpose.
- Sometimes multiple offices possess copies of the same record. Only the “office of record” is responsible for following the retention period that is specified. Duplicates do not need to be retained.

Why Follow a Retention Schedule?

- Risks with keeping records too long
  - Wastes space
  - Harder to find records you need
  - Records must be reviewed for FOIA and litigation
- Risks with destroying records too soon
  - Violation of Michigan law
  - Exposes agency to liability if the records are requested via FOIA or litigation
- Avoid random record purging by establishing a routine within the normal course of business

HAL Does Not Audit for Compliance

- Agency is responsible for complying with the records management laws
  - Records Management Services provides the tools and the training
- Agency must weigh risk of non-compliance
  - Inability to produce records that are requested by the public, lawyers, auditors, etc.

Bottom Line

- Agencies need to know how long they are legally required to retain records
- Agencies need a legal authorization to destroy records
- Agencies should purge records that have fulfilled their retention requirements on a regular basis
- Keeping records too long costs money

What is the Role of IT?

- Get an approved Retention and Disposal Schedule for all IT records
- Know what the approved retention period is for all electronic records IT is supporting/maintaining for customers

What is the Role of IT?

- Develop preservation plans for long-term electronic records
  - Remember that records often have to be retained longer than the technology that was used to create them
- Ensure that accurate systems documentation and metadata are maintained to keep data meaningful and usable
  - Version control is very important
- Select file formats and storage media that facilitate accessibility of the data throughout its life cycle

Questions?

E-mail Retention

Yes. E-mail is a record!

36 Years Worth of E-mail

- E-mail was invented in October 1971
  - Technology to support sending electronic messages between computers in different locations
- E-mail use increased steadily over the past 15 years, and the trend will continue
- Today, most employees cannot function effectively at work without e-mail

Quiz: True or False?

Q. My information technology department automatically deletes all e-mail in the system after 90 days, so I am not responsible for keeping e-mail beyond that period of time.

A. FALSE: We don’t keep all paper records for only 90 days. If an e-mail message is related to a contract, we need to keep it as long as all other contract records. If the message is related to a personnel issue, we need to keep it as long as all other personnel records.

Quiz

Q. I am the only person who can see the messages in my government e-mail account. It is private.

A. FALSE: Information technology staff and management may choose to monitor the activity in your e-mail account. In addition, the messages may become the subject of a FOIA request or litigation. If this happens, legal staff may review your e-mail messages to find evidence.

Quiz

Q. If I am one of 50 people who receive a message, and I do not have to fulfill an assignment as a result of that message, then I can destroy it.

A. TRUE: The sender should retain the message, as well as any employees who are assigned a task as a result of the message.

Quiz

Q. I should create a folder called “e-mail” and store all of my e-mail messages in it.

A. FALSE: E-mail messages should be stored in topical folders with other paper or electronic records that document the same business process.

Quiz

Q. It is best to save all e-mail messages that I send and receive, in case I need to prove I did something.

A. FALSE: It is best to destroy e-mail messages that have fulfilled their retention period so they do not waste space on the computer system. Also, these messages could become a liability if a FOIA request or litigation discovery request is received.

E-mail Liabilities

- President Bush sent his last e-mail message prior to his 2001 inauguration. He told family and friends that all correspondence would become public record. He wants to prevent disclosure of “personal stuff.”
- Former U.S. Attorney General Alberto Gonzales was concerned that “perfectly innocent” communications could be “twisted” by administration critics. “I don’t get e-mail and I don’t send e-mail.”

Lessons Learned the Hard Way …

- Oliver North thought incriminating e-mail messages related to Iran-Contra had been safely deleted. “Wow, were we wrong.”
- Oregon’s worker compensation insurer (a state agency) was held in contempt of court and fined $2.5 million for routinely deleting e-mail, including messages that had been requested by the public and the court.

E-mail is Not Private

Do not write something in an e-mail message that you do not want to see published in the newspaper or on television news reports.

E-mail and FOIA

- If a message still exists (in active accounts, on backup tapes, etc.) when a FOIA request is received, it must be evaluated by legal staff for release.
- If messages are destroyed on a regular basis, in accordance with approved Retention and Disposal Schedules, they may no longer exist when a FOIA request is received. Agency will not be penalized for not releasing the record.

E-mail and Litigation

- Immediately cease all destruction of relevant e-mail in active accounts and on backup tapes when litigation is imminent.
- Government agencies do not want to be charged with destroying evidence.
- Amendments to the Federal Rules of Civil Procedure went into effect on December 1, 2006
  - Address the role of electronically stored information as evidence in federal courts

E-mail and the Open Meetings Act

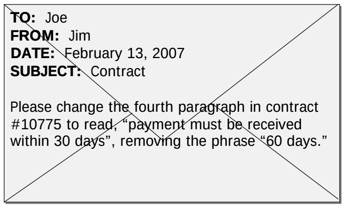
- A quorum of members of public bodies (as defined by FOIA) cannot use e-mail to deliberate issues outside of a public meeting.
- The e-mail of members of public bodies can be eligible for release in accordance with FOIA and can be used as evidence in litigation.

Releasing E-mail

- Finding and releasing e-mail can be time-consuming and costly
- E-mail can be retained in a lot of places, by a lot of people
- Notify all responsible parties to stop destroying relevant messages once a request is received or anticipated
- Keep your records organized
- Know who has what

Four Categories of E-mail

Official Records: recorded information that is prepared, owned, used, in the possession of, or retained by an agency in the performance of an official function.

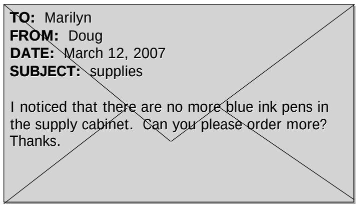


TO: Joe
FROM: Jim
DATE: February 13, 2007
SUBJECT: Contract

Please change the fourth paragraph in contract #10775 to read, "payment must be received within 30 days", removing the phrase "60 days."

Four Categories of E-mail

Transitory Records: records relating to agency activities that have temporary value and do not need to be retained once their intended purpose has been fulfilled.

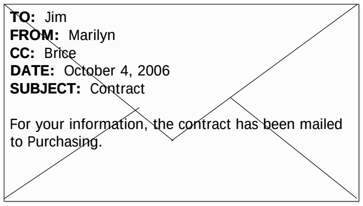


TO: Marilyn
FROM: Doug
DATE: March 12, 2007
SUBJECT: supplies

I noticed that there are no more blue ink pens in the supply cabinet. Can you please order more? Thanks.

Four Categories of E-mail

Non-records: recorded information in the possession of an agency that is not needed to document the performance of an official function.

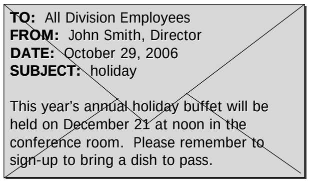


TO: Jim
FROM: Marilyn
CC: Brice
DATE: October 4, 2006
SUBJECT: Contract

For your information, the contract has been mailed to Purchasing.

Four Categories of E-mail

Personal Records: records that document non-government business or activities. Note: agencies may have policies that prohibit the use of personal e-mail with government technology resources.



TO: All Division Employees
FROM: John Smith, Director
DATE: October 29, 2006
SUBJECT: holiday

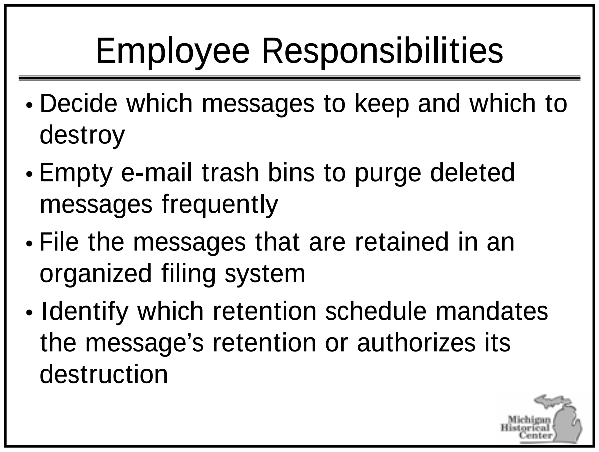
This year's annual holiday buffet will be held on December 21 at noon in the conference room. Please remember to sign-up to bring a dish to pass.

E-mail Retention

- Official Records: Retain according to agency-specific and general schedules
- Transitory Records: Retain for up to 30 days
- Non-records: Destroy ASAP
- Personal Records: Do not use government technology resources

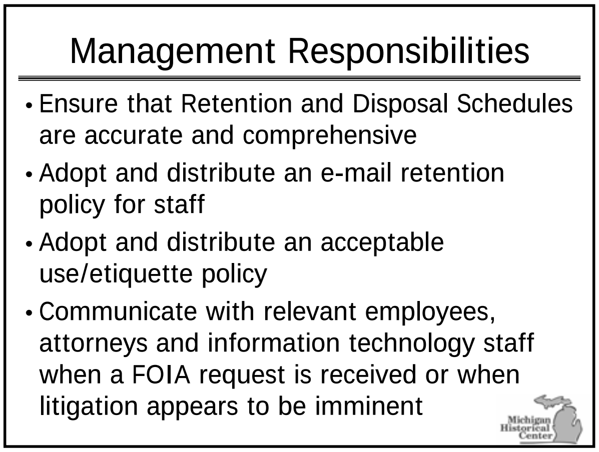
Who is Responsible for Retention?

- Official Records: Senders are the "person of record"
- Official Records: Recipients may need the record to support business functions
- Transitory Records: Retain until task or activity is completed
- Non-records: Informational copies do not need to be retained



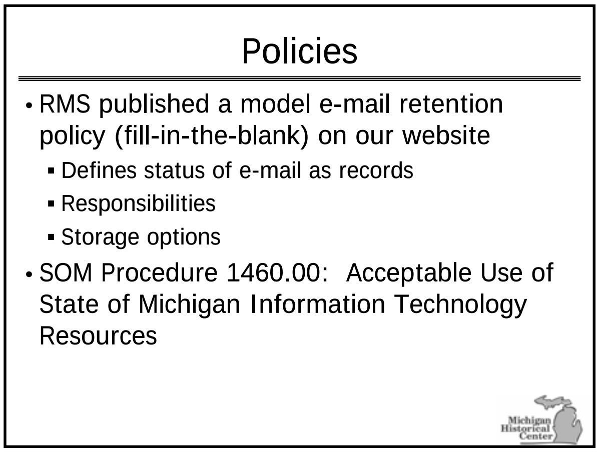
Employee Responsibilities

- Decide which messages to keep and which to destroy
- Empty e-mail trash bins to purge deleted messages frequently
- File the messages that are retained in an organized filing system
- Identify which retention schedule mandates the message’s retention or authorizes its destruction



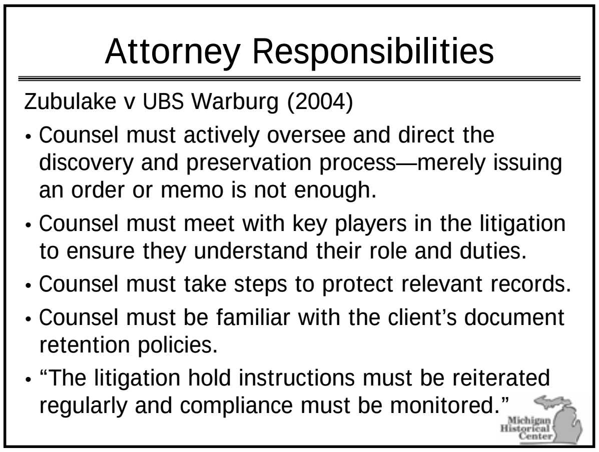
Management Responsibilities

- Ensure that Retention and Disposal Schedules are accurate and comprehensive
- Adopt and distribute an e-mail retention policy for staff
- Adopt and distribute an acceptable use/etiquette policy
- Communicate with relevant employees, attorneys and information technology staff when a FOIA request is received or when litigation appears to be imminent



Policies

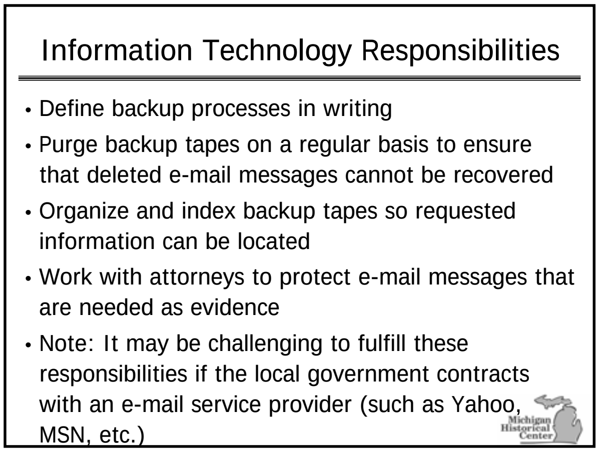
- RMS published a model e-mail retention policy (fill-in-the-blank) on our website
  - Defines status of e-mail as records
  - Responsibilities
  - Storage options
- SOM Procedure 1460.00: Acceptable Use of State of Michigan Information Technology Resources



Attorney Responsibilities

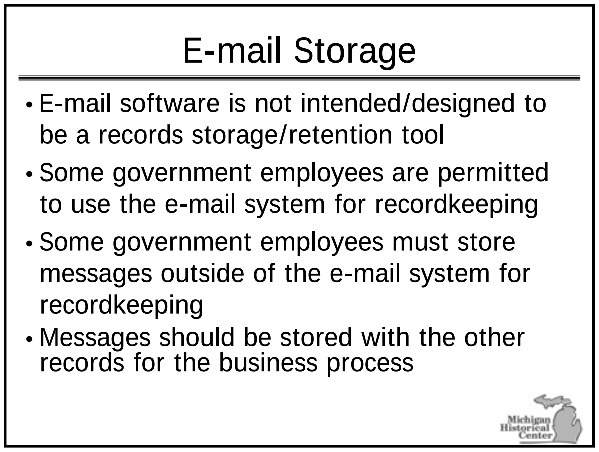
Zubulake v UBS Warburg (2004)

- Counsel must actively oversee and direct the discovery and preservation process—merely issuing an order or memo is not enough.
- Counsel must meet with key players in the litigation to ensure they understand their role and duties.
- Counsel must take steps to protect relevant records.
- Counsel must be familiar with the client’s document retention policies.
- “The litigation hold instructions must be reiterated regularly and compliance must be monitored.”



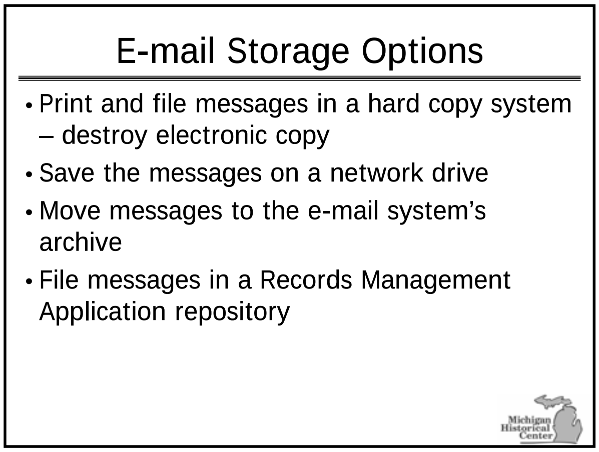
Information Technology Responsibilities

- Define backup processes in writing
- Purge backup tapes on a regular basis to ensure that deleted e-mail messages cannot be recovered
- Organize and index backup tapes so requested information can be located
- Work with attorneys to protect e-mail messages that are needed as evidence
- Note: It may be challenging to fulfill these responsibilities if the local government contracts with an e-mail service provider (such as Yahoo, MSN, etc.)



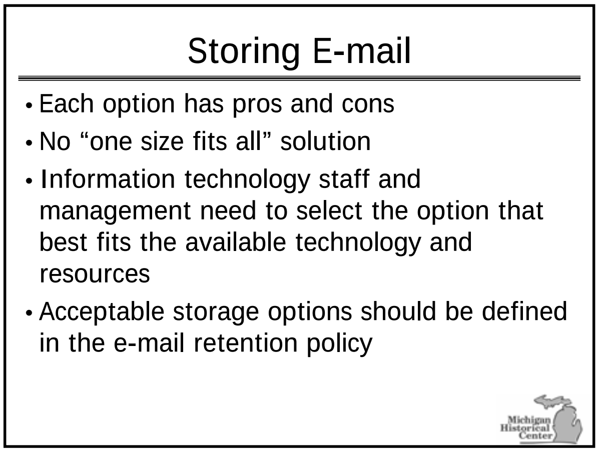
E-mail Storage

- E-mail software is not intended/designed to be a records storage/retention tool
- Some government employees are permitted to use the e-mail system for recordkeeping
- Some government employees must store messages outside of the e-mail system for recordkeeping
- Messages should be stored with the other records for the business process



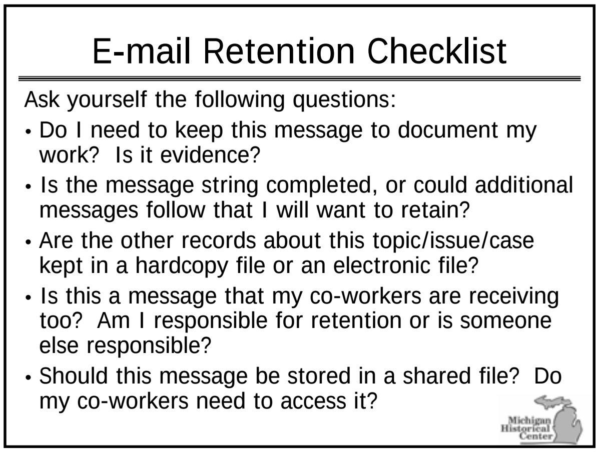
E-mail Storage Options

- Print and file messages in a hard copy system – destroy electronic copy
- Save the messages on a network drive
- Move messages to the e-mail system's archive
- File messages in a Records Management Application repository



Storing E-mail

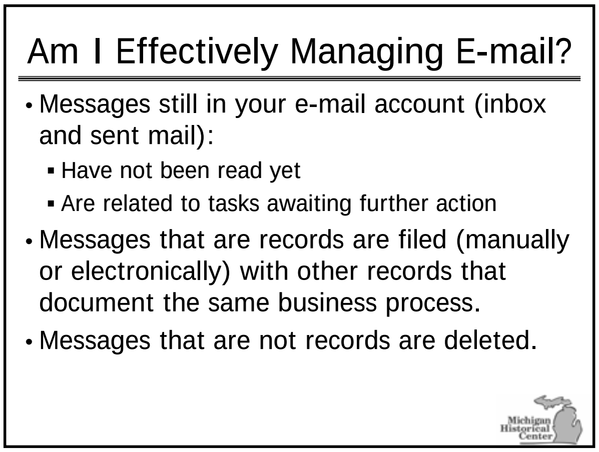
- Each option has pros and cons
- No "one size fits all" solution
- Information technology staff and management need to select the option that best fits the available technology and resources
- Acceptable storage options should be defined in the e-mail retention policy



E-mail Retention Checklist

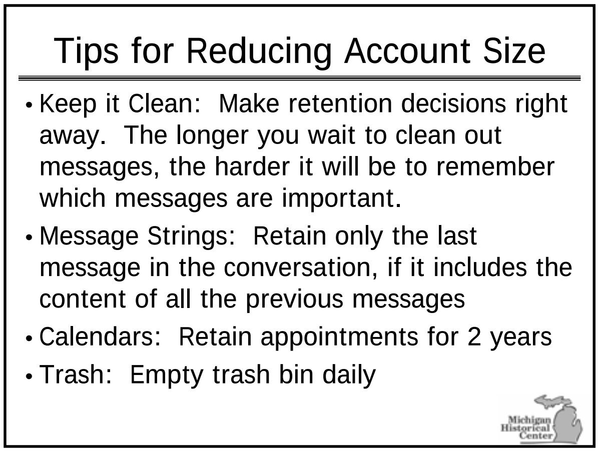
Ask yourself the following questions:

- Do I need to keep this message to document my work? Is it evidence?
- Is the message string completed, or could additional messages follow that I will want to retain?
- Are the other records about this topic/issue/case kept in a hardcopy file or an electronic file?
- Is this a message that my co-workers are receiving too? Am I responsible for retention or is someone else responsible?
- Should this message be stored in a shared file? Do my co-workers need to access it?



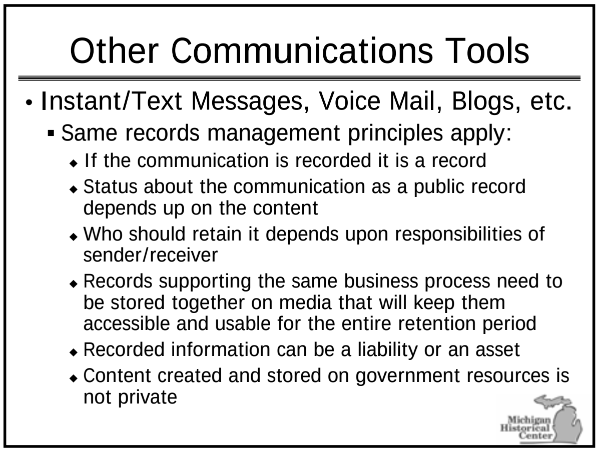
Am I Effectively Managing E-mail?

- Messages still in your e-mail account (inbox and sent mail):
  - Have not been read yet
  - Are related to tasks awaiting further action
- Messages that are records are filed (manually or electronically) with other records that document the same business process.
- Messages that are not records are deleted.



Tips for Reducing Account Size

- Keep it Clean: Make retention decisions right away. The longer you wait to clean out messages, the harder it will be to remember which messages are important.
- Message Strings: Retain only the last message in the conversation, if it includes the content of all the previous messages
- Calendars: Retain appointments for 2 years
- Trash: Empty trash bin daily



Other Communications Tools

- Instant/Text Messages, Voice Mail, Blogs, etc.
  - Same records management principles apply:
    - If the communication is recorded it is a record
    - Status about the communication as a public record depends up on the content
    - Who should retain it depends upon responsibilities of sender/receiver
    - Records supporting the same business process need to be stored together on media that will keep them accessible and usable for the entire retention period
    - Recorded information can be a liability or an asset
    - Content created and stored on government resources is not private

Detroit Mayor’s Text Messages

- Message service saved content and transmission information
- Messages were retrieved through a FOIA request
- Mayor and others charged with felony crimes
- Message services have different policies for saving information

Additional Resources

Materials on the CD and website

- Frequently Asked Questions about E-mail Retention
- E-mail Retention Guidelines
- Model E-mail Retention Policy
- E-mail Storage Options
- File Plan Template

More Training

- E-mail Retention Class
- Free web-based user training
- Course takes 30-45 minutes to complete
- Flyer on CD provides instructions for accessing the class
- Available at:

http://www.quicknowledge.com/qk/hal/email

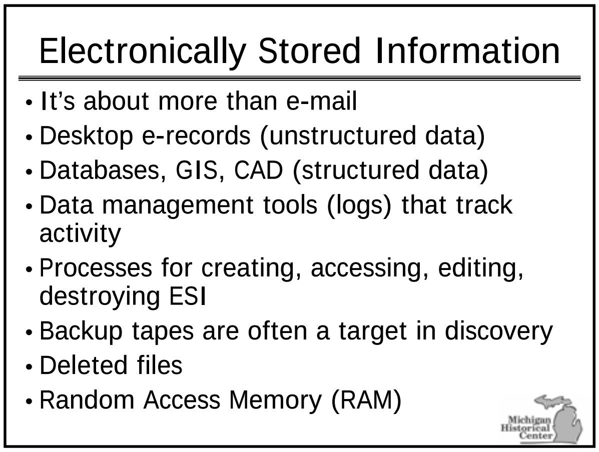
Questions?

Discovery

Protecting Your Government Agency

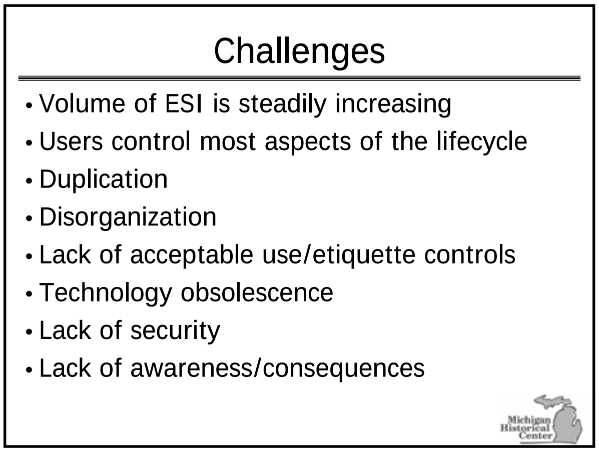
e-Discovery

- E-Discovery is the process in which electronic data is sought, located, secured, and searched, with the intent of using it as evidence in a civil or criminal legal case.
- The medium used to document official government activity is irrelevant.
  - The content of the record determines if it is evidence of an official government transaction, action, or activity.



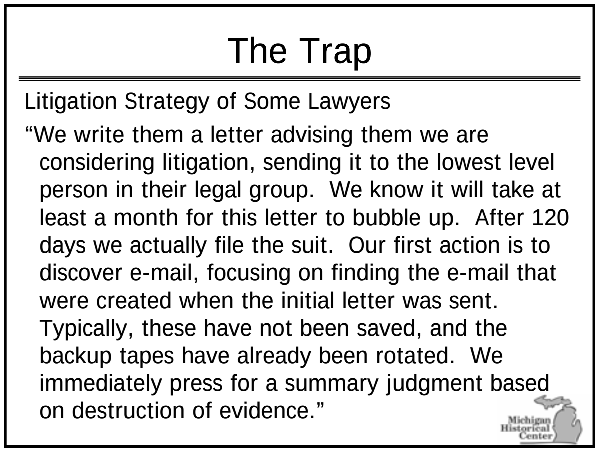
Electronically Stored Information

- It's about more than e-mail
- Desktop e-records (unstructured data)
- Databases, GIS, CAD (structured data)
- Data management tools (logs) that track activity
- Processes for creating, accessing, editing, destroying ESI
- Backup tapes are often a target in discovery
- Deleted files
- Random Access Memory (RAM)



Challenges

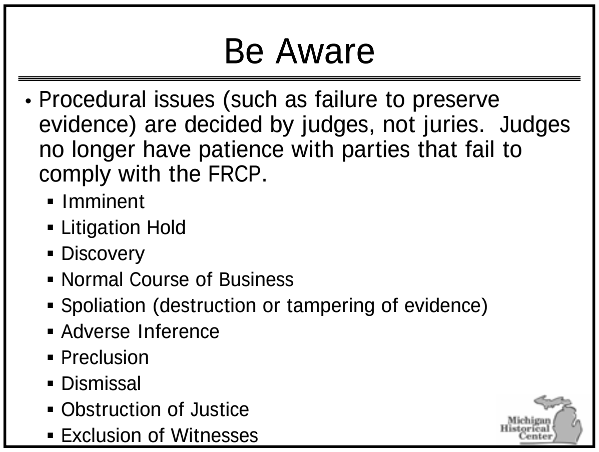
- Volume of ESI is steadily increasing
- Users control most aspects of the lifecycle
- Duplication
- Disorganization
- Lack of acceptable use/etiquette controls
- Technology obsolescence
- Lack of security
- Lack of awareness/consequences



The Trap

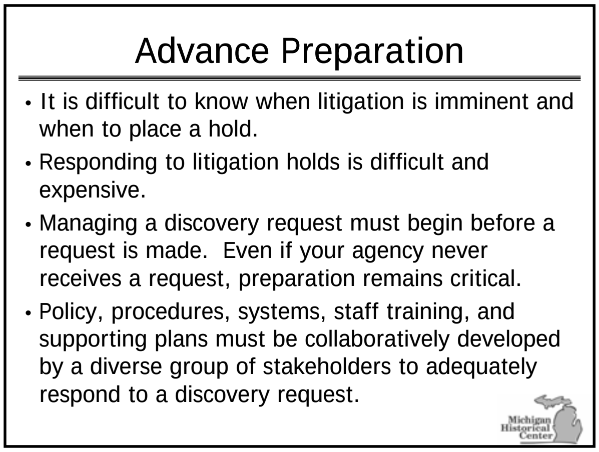
Litigation Strategy of Some Lawyers

"We write them a letter advising them we are considering litigation, sending it to the lowest level person in their legal group. We know it will take at least a month for this letter to bubble up. After 120 days we actually file the suit. Our first action is to discover e-mail, focusing on finding the e-mail that were created when the initial letter was sent. Typically, these have not been saved, and the backup tapes have already been rotated. We immediately press for a summary judgment based on destruction of evidence."



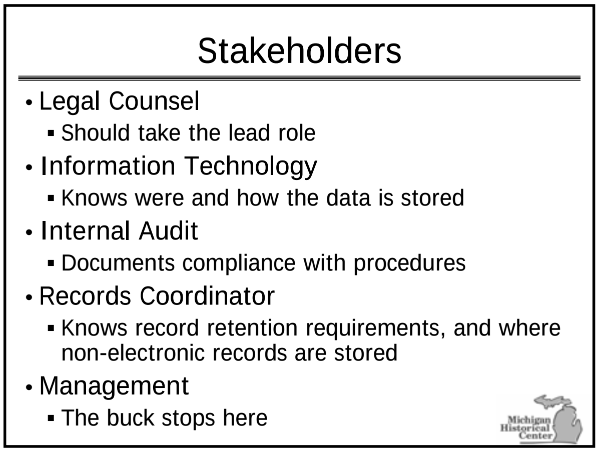
Be Aware

- Procedural issues (such as failure to preserve evidence) are decided by judges, not juries. Judges no longer have patience with parties that fail to comply with the FRCP.
  - Imminent
  - Litigation Hold
  - Discovery
  - Normal Course of Business
  - Spoliation (destruction or tampering of evidence)
  - Adverse Inference
  - Preclusion
  - Dismissal
  - Obstruction of Justice
  - Exclusion of Witnesses



Advance Preparation

- It is difficult to know when litigation is imminent and when to place a hold.
- Responding to litigation holds is difficult and expensive.
- Managing a discovery request must begin before a request is made. Even if your agency never receives a request, preparation remains critical.
- Policy, procedures, systems, staff training, and supporting plans must be collaboratively developed by a diverse group of stakeholders to adequately respond to a discovery request.



Stakeholders

- Legal Counsel
  - Should take the lead role
- Information Technology
  - Knows were and how the data is stored
- Internal Audit
  - Documents compliance with procedures
- Records Coordinator
  - Knows record retention requirements, and where non-electronic records are stored
- Management
  - The buck stops here

Role of Legal Counsel

- Adopt litigation hold procedures
  - Identify who in the legal department should be contacted by employees who believe litigation is imminent
- Identify custodians of evidence that is relevant to litigation (both legal and physical custody)
- Notify record custodians that a litigation hold is in place, including periodic reminders
- Notify record custodians when the litigation hold is lifted

Discovery Procedures

- Identify responsibilities of parties
- Identify sources of evidence
- Identify how to comply with the immediate discovery requests (short term)
- Identify how to support ongoing business processes as the litigation continues without compromising the evidence and operational efficiency (long term)

Role of IT

- Maintain a current and accurate inventory of IT resources
- Maintain documentation about use and access of systems
- Develop and implement standard operating procedures
- Establish and test procedures for holding evidence needed for litigation

Backups: False Assumptions

- Every backup event is successful
- Backup captures every document or piece of data every time
- It is easy to locate and restore documents and data from backup tapes

Backup Systems

- RM Perspective: Backups are duplicate, "nonrecords" covered by GS #1, unless the original record was deleted from the active storage system. IT needs a written data storage policy, and needs to follow it routinely.
- FOIA/Litigation Perspective: If records still exist on backup tapes, and no where else, they must be evaluated for release to the requesting party.
- Compliance Perspective: Ensure that backup and recovery systems capture content and metadata in a synchronized manner to protect linkages.

Inventory Your Technology

- All devices owned by the agency (device type, location)
- Develop a diagram (schematic) of all devices and how they are connected (networked), including backups
- All software used by the agency (manufacturer, program name, version)

Inventory Your Data

- Data Survey and Review
- Data Extraction
  - Automate as much as possible (reduces wasted employee time)
    - Rebuilding backups is expensive
    - Archival data storage permits selective retrieval
  - Organize data for extraction
    - By user
    - By type
    - By date
- Reduce / Eliminate Secondary Data Sources
    - File Sharing
    - Thin Client

Where is ESI evidence stored?

- server/SAN
- PC / laptop
- deleted files (trash, backups, memory until it is overwritten)
- offline, near-line, off-site, redundant data
- voice mail
- cell phones and service provider logs, call detail
- instant and text message devices and service provider logs
- CDs, DVDs, tapes, floppy disks
- e-mail accounts
- phone / VOIP log
- firewall log
- backup tapes – full & incremental
- SPAM filter log
- RAM
- home computers
- thumb/USB drives
- Web browser cache
- cameras
- server logs
- PDA

Who to Notify in IT

- Storage Administrator
- Application Administrator
- E-mail System Administrator
- Network Administrator
- Management Team
- Person who orders supplies
  - Buy additional backup tapes to replace those pulled from the rotation

Don’t Alter the Evidence

- Identify if older data is automatically deleted or overwritten by newer data
- Could the inspection of a record or generation of a discovery copy alter the metadata, such as date stamps?
- Protect proprietary, confidential or sensitive information
- Courts will decide the format that the evidence is shared in (pre-trial conference), native format is the default

Delete Does Not Mean Delete!

- Deleted files can be stored:
  - E-trash bins
  - Backup tapes
  - Memory until it is overwritten
    - Computer forensics tools can recover overwritten memory
  - Duplicate copies
    - Printouts
    - Disks and external drives
  - Surplus property
    - Was memory erased?

Memory is Resilient

- Computer Forensics
  - Can recover data that was overwritten multiple times
- Space Shuttle Challenger
  - Black box tapes were exposed to fire and salt water
  - Data was recovered
- If you have the time, the will and the money it may be discovered
- Some parties settle litigation because it is cheaper than the recovery costs

Policies, Procedures, Plans

- Need to document all activity that could affect the integrity and authenticity of the records
  - System security
  - Storage/backup routines
  - Access rights
- Will you be able to answer questions about your data storage practices in court?
- Will you have evidence to support your actions or identify violations?

Role of Internal Audit

- Performance Audits
  - Audit compliance with Retention and Disposal Schedules
  - Audit security and accuracy of recordkeeping systems (paper and electronic)
  - Audit completeness of and compliance with standard operating procedures

Role of Records Management

- Records Retention and Disposal Schedules document that there is an approved timeline for retaining records, regardless of format
- Schedule identifies each responsible recordkeeper
- If the schedule is followed routinely ("normal course of business"), there will not be suspicion about why some records still exist and others do not
- Litigation hold suspends the schedule

3-Point Test for Spoliation

1. Is the record retention period reasonable? Does it take into consideration relevant laws, regulations, and best practices? Is it sufficient to meet the administrative, fiscal, legal and historical values of the record? Can it be implemented in a practical manner?
2. Was the records retention policy adopted in good faith? Was it reviewed and approved by proper authorities? Has it been implemented on a routine and on-going basis? Has it been effectively communicated to all affected employees?
3. Is there reasonable evidence to suspect that the records will be the subject of future litigation, audit or investigation beyond their retention period, based upon the frequency of past lawsuits, complaints, etc.?

--Sedona Conference

Automatic Purging

"A policy that routinely deletes "old" data (such as e-mail messages) without any other protections can be analogized to destroying boxes in a warehouse based on where they are on the shelf, without any regard to the contents."

--Sedona Conference

Role of Top Management

- Provide adequate funding to implement and support good recordkeeping systems (paper and electronic)
- Adopt policies and procedures
- Provide training to staff
- Ensure staff are fulfilling their responsibilities

Business Process Procedures

- Each business process should have written procedures that will support the integrity and authenticity of the records
- Procedures define who is authorized to:
  - Create records
  - Access records
  - Modify records
  - Destroy records

Who is at fault?

- Employer: did not establish policies, and did not train employees about the policies—employer is at fault
- Employee: received the policies and the training, but failed to follow them—employee is at fault
- Attorney: received notification about litigation, but failed to notify custodians of the evidence—attorney is at fault
- IT: did not inventory assets and establish data maintenance policies—IT is at fault

Sources for More Information

- Sedona Conference
  - http://www.thesedonaconference.org/
  - Publications
    - Commentary on Legal Holds: The Trigger and The Process
    - Best Practice Recommendations and Principles for Addressing Electronic Document Production
    - Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age
    - Commentary on ESI Evidence and Admissibility
    - Best Practices for the Selection of Electronic Discovery Vendors

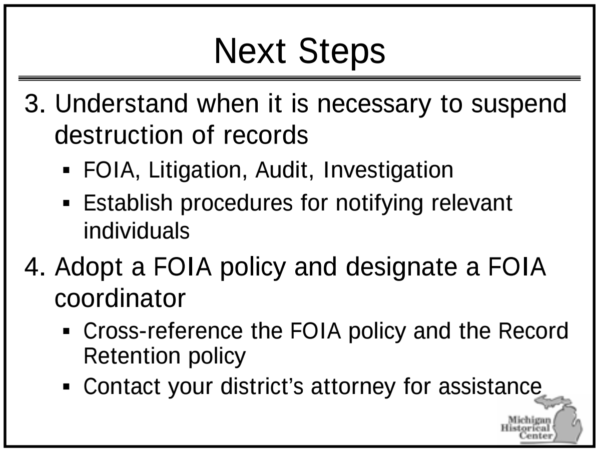
Questions?

Don't Feel Overwhelmed…

Getting Started with Record Retention

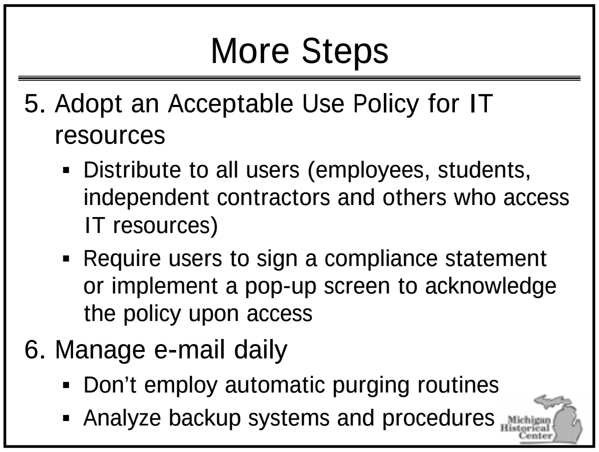
First Steps

1. Distribute the General Schedule for Public Schools to staff
   - Provide a link on the district's intranet site
   - Brief department director's about the importance of following the schedule and expectations
   - Each department should focus on learning their chapter in the schedule, plus the general administrative records
2. Training: ensure all staff have some basic awareness of the record retention policy as it applies to their job



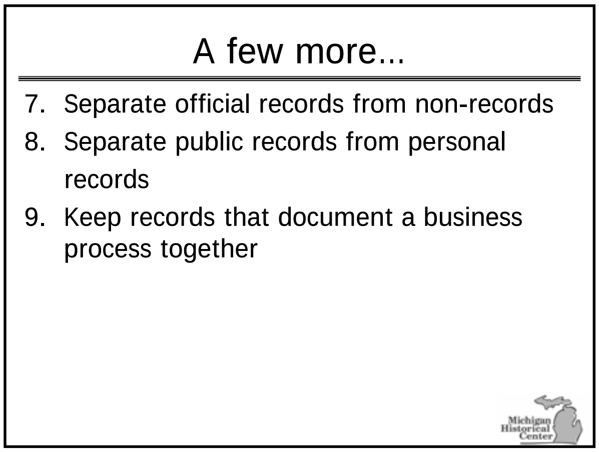
Next Steps

3. Understand when it is necessary to suspend destruction of records
   - FOIA, Litigation, Audit, Investigation
   - Establish procedures for notifying relevant individuals
4. Adopt a FOIA policy and designate a FOIA coordinator
   - Cross-reference the FOIA policy and the Record Retention policy
   - Contact your district's attorney for assistance



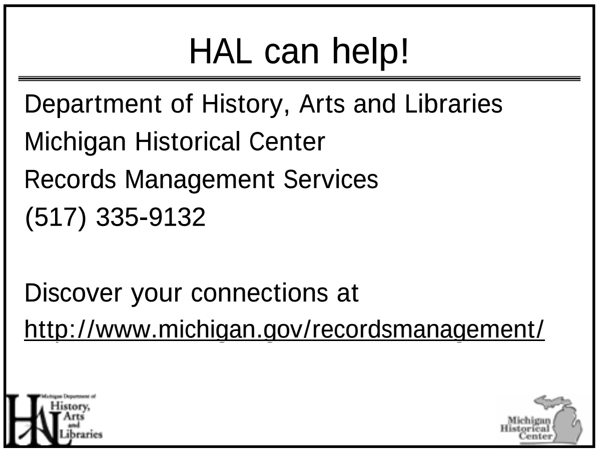
More Steps

5. Adopt an Acceptable Use Policy for IT resources
   - Distribute to all users (employees, students, independent contractors and others who access IT resources)
   - Require users to sign a compliance statement or implement a pop-up screen to acknowledge the policy upon access
6. Manage e-mail daily
   - Don't employ automatic purging routines
   - Analyze backup systems and procedures



A few more…

7. Separate official records from non-records
8. Separate public records from personal records
9. Keep records that document a business process together



HAL can help!

Department of History, Arts and Libraries

Michigan Historical Center

Records Management Services

(517) 335-9132

Discover your connections at

http://www.michigan.gov/recordsmanagement/