INFORMATION TECHNOLOGY GUIDELINES

OFFICE OF THE CIO
UNIVERSITY OF MICHIGAN

Guideline number:	DM-08
Title	**eDiscovery at the University of Michigan**
Date issued:	August 10, 2010
Date last reviewed:	February 13, 2017
Version number:	3.0
Approval authority:	Vice President and General Counsel; Vice President and CIO
Responsible office:	Office of the General Counsel and Information Assurance

I. **Overview**

The identification, preservation, production, and management of electronic information associated with litigation cases are generally referred to as the eDiscovery process. Amendments to the Federal Rules of Civil Procedure (FRCP), effective December 2006, and amendments to the Michigan Court Rules, effective January 2009, specifically address the litigation discovery process for electronically stored information (ESI). To comply with these rules, the University of Michigan is obligated to take good faith efforts to preserve ESI that could be relevant to pending or reasonably anticipated lawsuits and to potentially retrieve and produce this information in the course of the litigation process.

II. **Guideline Purpose**

The purposes of these guidelines are to:

A. Ensure that the university complies with eDiscovery obligations;
B. Ensure that individuals—data holders, their managers, and their IT providers—are aware of their responsibilities to promptly respond to eDiscovery requests;
C. Provide a repeatable, streamlined eDiscovery process for the Office of the General Counsel (OGC) and for others involved in this process; and
D. Protect the privacy of personally identifiable information (PII) that may have been captured during the eDiscovery process in compliance with university policies.

The guidelines are specifically intended for data holders, IT providers, department managers and department administrators who are requested by OGC to hold, preserve and produce electronic (and other) information associated with a given dispute. The guidelines also serve as general awareness information for IT providers and others across the university.

III. **Guidelines**

These guidelines apply to all campuses including Flint and Dearborn and are generally consistent with the process used in Michigan Medicine . The guidelines do not cover disputes involving HIPAA-related information that are handled by OGC and the Michigan Medicine Compliance Office.

In general, electronically stored information (ESI) relevant to a dispute must be preserved. This includes information that is centrally stored (in email and other file servers), information that is locally stored on desktops, laptops, home computers, PDAs, CDs, flash drives, smart phones, etc., and also information that is outsourced or stored in the cloud, to the extent that the data holder has the ability to ensure such information is preserved. While the focus of these guidelines is on electronically stored information, paper and other media containing information relevant to a given case should also be preserved and are addressed by these guidelines.

There may be some cases where relevant information does not need to be stored, for example, multiple generations of backup storage do not need to be preserved if a master copy is preserved. In other cases, the difficulty of preserving/producing certain information may be deemed unreasonable. Any such exclusion must be specified and approved by OGC.

These guidelines do not include detailed instructions for how to preserve, search, or produce ESI in a specific technical environment. Such instructions vary and need to be provided by the appropriate IT support staff.

IV. Responsibilities

While individuals have particular responsibilities concerning eDiscovery, it is essential that the eDiscovery process is collaborative and all lines of communication remain open. For example, in order to ascertain the scope of potential eDiscovery, OGC will require reliable information from Data Holders and User Advocates concerning the underlying facts of the dispute and the location of relevant ESI. Similarly, Data Holders and User Advocates may have questions for OGC that arise throughout the process.

A. **Office of General Counsel (OGC)**: OGC is the owner of the eDiscovery process and has overall responsibility for initiating the eDiscovery process, notifying individuals of their responsibilities, and monitoring and managing the process. Specific responsibilities include:

1. Determining the need to issue a preservation/litigation hold;
2. Involving the IT User Advocate in the eDiscovery process as appropriate;
3. Determining the scope of the hold and, in conjunction with IT providers and/or the User Advocate, identifying the types of systems and media that need to be searched, the searching criteria, and the appropriate collection methods;
4. Issuing preservation/litigation holds;
5. Collecting and reviewing relevant ESI and non-electronic information;
6. Ensuring the confidentiality and integrity of private personal information or other sensitive information that may have been captured as a part of a litigation hold;
7. Issuing instructions to release a litigation hold;
8. Monitoring, managing, and working to further improve the overall litigation process.

B. **IT User Advocate (UA)**: The User Advocate (UA) function is part of Information and Infrastructure Assurance, and is generally responsible for investigating potential violations of information policies and for ensuring that the privacy of individuals is protected when information assets containing private personal information are accessed. In the context of eDiscovery, the User Advocate assists OGC, in particular in cases where individual data holders are not available or when OGC determines that it is not appropriate to engage data holders.

Specific responsibilities include:

1. In conjunction with OGC, identifying relevant computing environments and searching/preservation approaches;
2. Ensuring the confidentiality and integrity of private personal information or other sensitive information that may have been captured as a part of a litigation hold;
3. Conducting searches and preservation when data holders are not available and in other cases as instructed by OGC;
4. Assisting departmental IT staff in complying with OGC requirements relative to a litigation/preservation hold;
    a. Providing consulting and support in conducting search, preservation, and production and in protecting sensitive information;
    b. Providing guidance and templates for departmental eDiscovery instructions;
    c. Packaging ESI from multiple sources, if appropriate, and providing it to OGC.

C. **Data Holders**: Data holders are faculty, staff, or students who may hold information relevant to a given case in their records and are requested by OGC to preserve these records. Specific responsibilities include:

1. Complying with OGC instructions relative to litigation cases;
2. Engaging their local IT support staff and/or the UA to assist in preservation, search, and production functions;
3. Preserving applicable information. This may include suspending any personal practices regarding destruction of relevant ESI (such as deletion of emails or voice mail) and disabling known automated delete functions;
4. Conducting searches per OGC provided criteria to identify relevant ESI;
5. Collecting and preserving relevant information without alteration;
6. Providing relevant personal or university-owned devices to OGC or as instructed by OGC; and
7. Notifying their Departmental Management of the litigation hold.

Note: As a general rule, and in accordance with Privacy and the Need to Monitor and Access Records (SPG 601.11), data holders are expected to maintain business records separate from personal records; preservation and production should not typically include their personal information. However, there are cases where personal information of data holders may be captured in the eDiscovery process. Efforts will be made to protect the confidentiality of such information

D. **Departmental IT Staff**: Departmental IT staff members may be notified by OGC or Data Holders of litigation holds so that they can support and assist the data holders in their areas. Specific responsibilities include:

1. Documenting departmental instructions for suspending deletes, search, preservation, and production;
2. Assisting department data holders in conducting search, preservation, and production activities, engaging the UA if necessary.

F. **Departmental Management and Administration:** Departmental managers and administrators are notified by Data Holders of litigation holds involving data holders in their departments and are expected to support these individuals. Specific responsibilities include:

1. Ensuring data holders comply with OGC requests relative to eDiscovery;
2. Ensuring data holders are supported and assisted by departmental IT staff;
3. Conducting preservation and search of non-electronic media for individuals who may not be available as requested by OGC.
4. Assisting in the preservation of the litigation hold by ensuring that devices or files are maintained as instructed especially if the Data Holder is no longer able to do so.

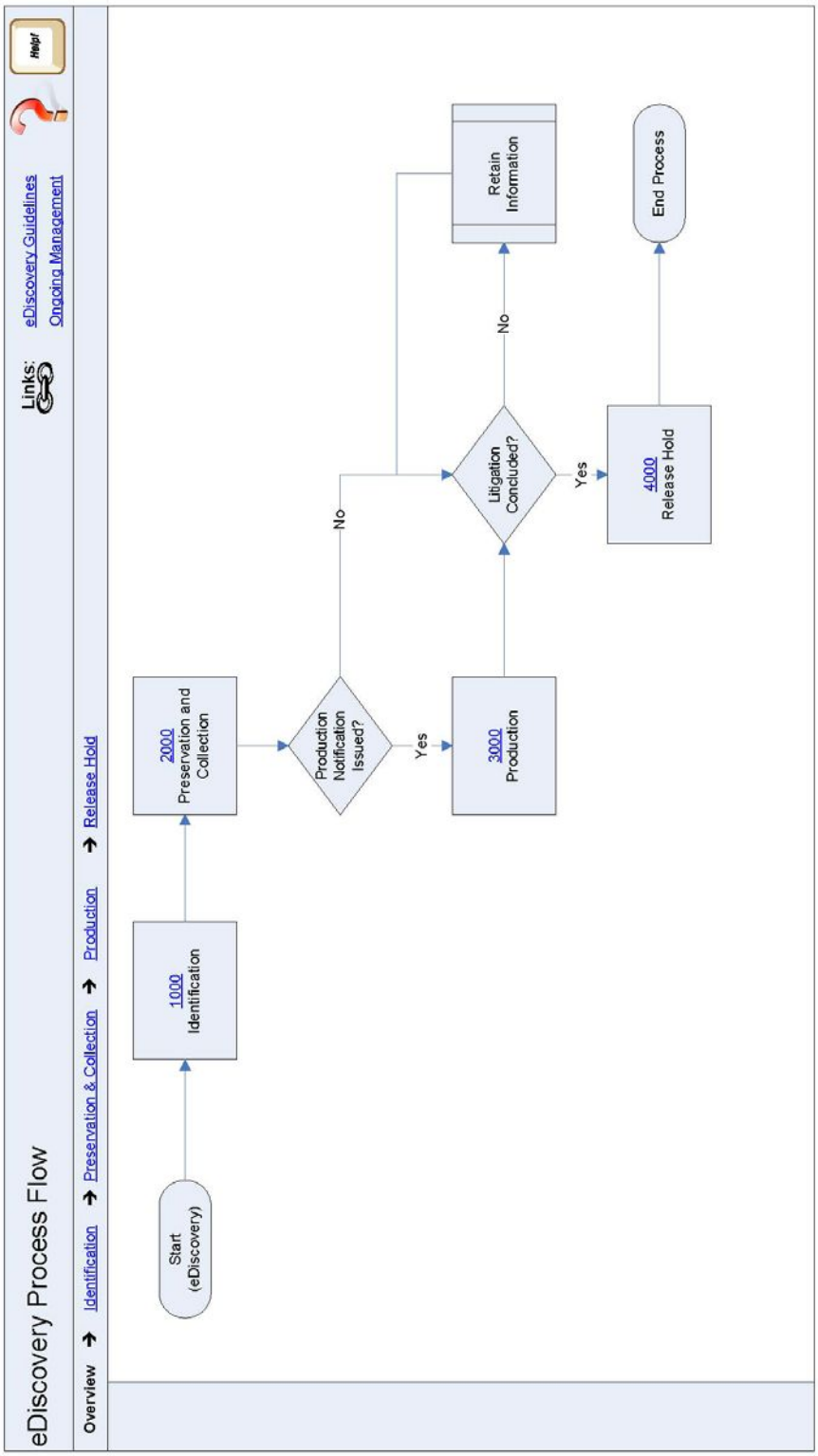
Department managers and administrators are encouraged to maintain and administer appropriate document retention policies in order to responsibly manage the ESI related to that department's activities. Such retention policies should be explicitly subject to any directions from OGC concerning discovery matters.

V. References

Privacy and the Need to Monitor and Access Records (SPG 601.11)
Personally Identifiable Information, Sensitive Data Guide, Safe Computing
Educause E-Discovery Guideline and Toolkit

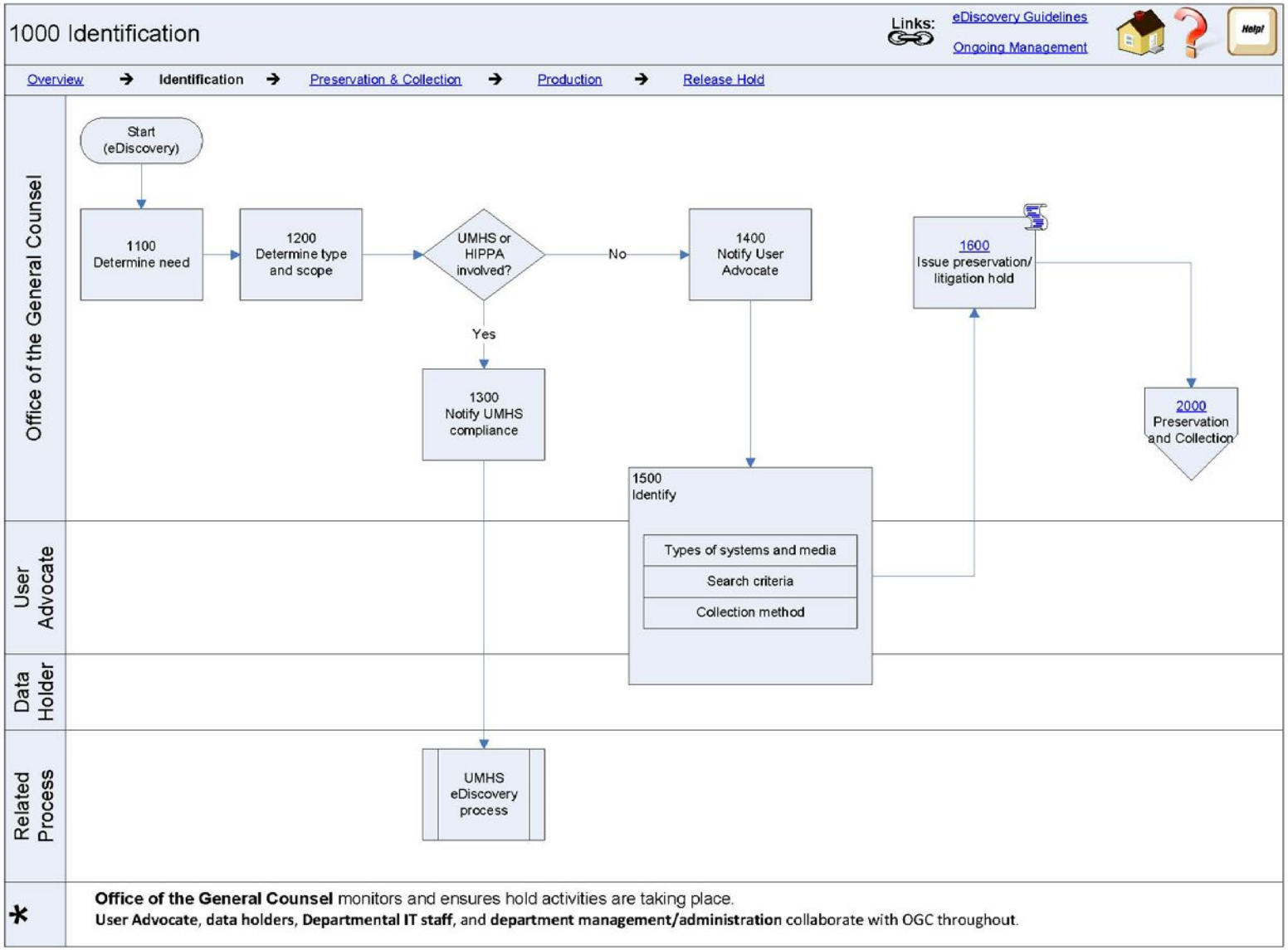
For additional information, please contact ITS Service Center, 4Help@umich.edu, (734) 764-4357

Attachment 1: The eDiscovery Process Flow

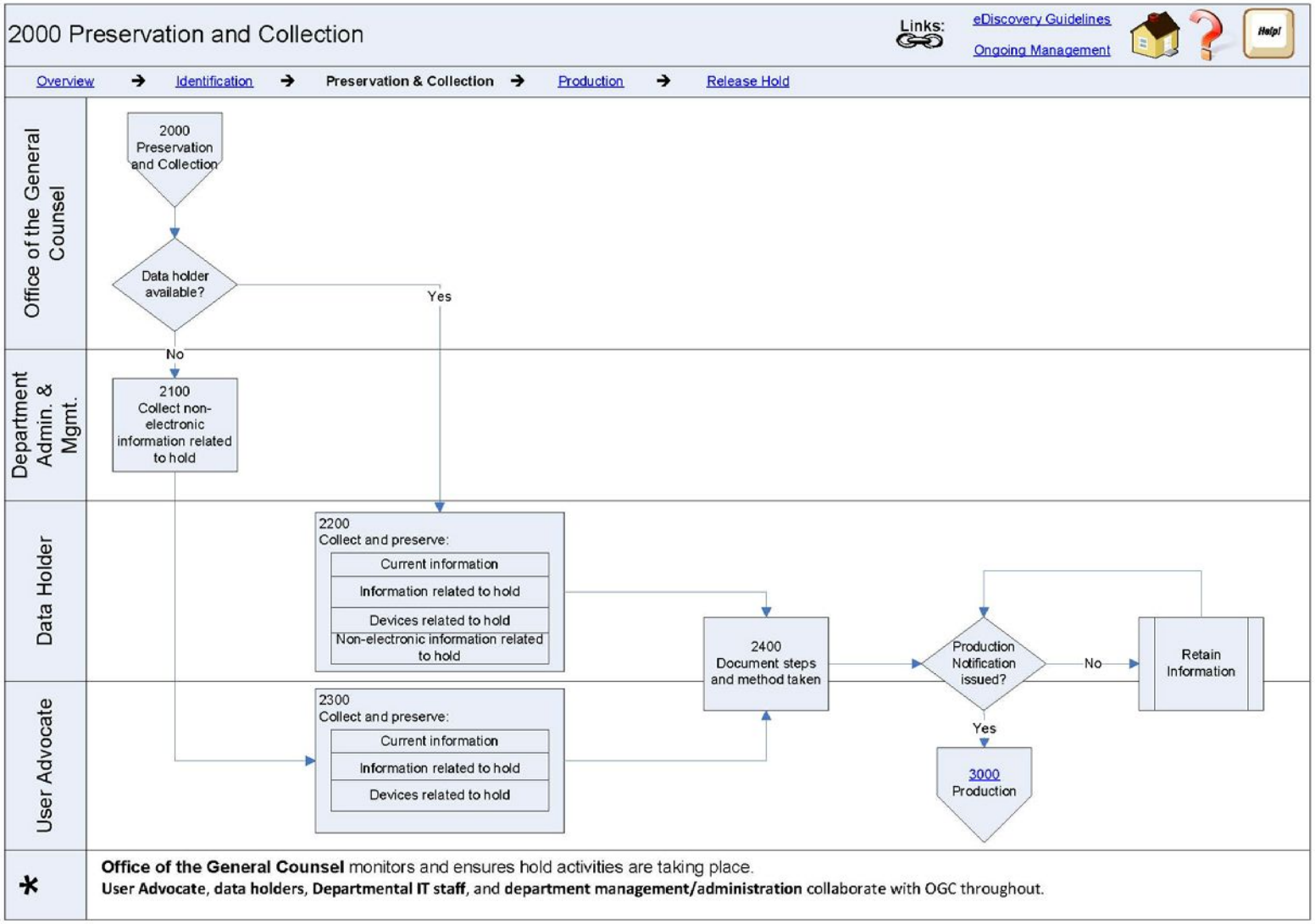


1000	2000	3000	4000
• Office of the General Counsel (OGC) • User Advocate (UA)	Office of the General Counsel User Advocate Dept. IT Staff Dept. Admin. & Mgmt. Data Holder	• Office of the General Counsel • User Advocate • Dept. IT Staff • Dept. Admin. & Mgmt • Data Holder	• Office of the General Counsel • User Advocate

Maintained by Knowledge Support



Maintained by Knowledge Support

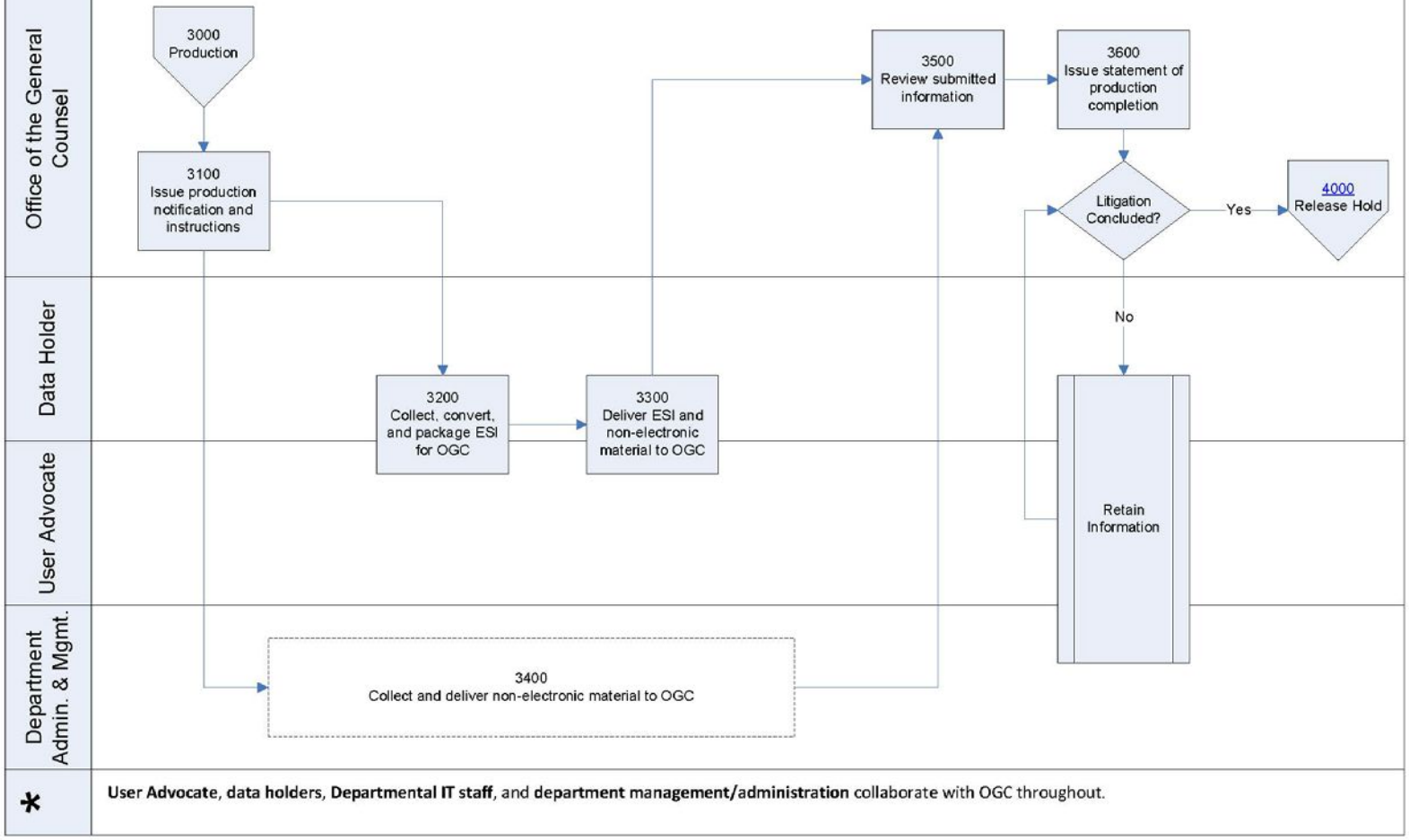


Maintained by Knowledge Support

3000 Production

Links: eDiscovery Guidelines
Ongoing Management

Overview → Identification → Preservation & Collection → **Production** → Release Hold



Maintained by Knowledge Support

Process Steps

	Responsible	Process Steps
1000	**Identification**	

	OGC	• Determine the need to issue a preservation/litigation hold
		• Determine the type and scope of the hold to be issued (i.e. preservation only or preservation and production)
		  ○ Establish case number and associated tracking folders
		  ○ Communicate with the university "client" who provides information about the scope of a given case
		  ○ Determine type of case
		  ○ Establish time frame for conducting the litigation hold
		  ○ Identify the specific individuals who may have applicable ESI and/or documents
		  ○ Identify the IT providers and others who can assist in protecting and preserving relevant ESI
		• If the litigation case involves the Health System or HIPAA related information, inform MCIT and UMHS Compliance and follow the "MCIT eDiscovery Process" (instead of the steps listed below)
		• Otherwise, inform the User Advocate of the need for a litigation hold and possible snapshots.

	OGC/UA	• Identify the types of systems and media that need to be searched, the searching criteria, and the appropriate collection methods
	Data Holders/ Departmental IT Staff/ Departmental Management & Administration	• Assist OGC and the UA in identifying individuals, systems, media types, and collection methods.

	OGC	• Issue a preservation/litigation hold
		  ○ Provide specific instructions to data holders including time frame for response
		  ○ Include reference to the eDiscovery guidelines (this document) to inform those notified of the process and their responsibilities
		  ○ Copy department managers, administrators, IT providers, and UA
		  ○ Request department managers/administrators to immediately notify OGC if named data holders are not available
		• Inform UA if individual data holders are not available and identify searches/preservation that would need to be performed by UA

2000	**Preservation/Collection**	

	Data Holders	• Comply with OGC instructions accompanying the hold • Solicit assistance from local IT support as necessary • Preserve current information ○ Suspend any personal practices regarding destruction of relevant ESI, such as deletion of emails, voice mail

	Responsible	**Process Steps**
		○ Disable any known automated delete functions • Conduct search per OGC provided criteria to identify relevant ESI • Collect and preserve relevant information without alteration • Preserve relevant devices – personally owned computers and other mobile devices • Preserve relevant paper documents as instructed by OGC • Document data collection and preservation methodology and the steps that have been taken to collect and preserve data • Notify Departmental Management of the litigation hold.
	UA	• Conduct searches and preservation when data holders are not available, unresponsive, uncooperative and in other cases as instructed by OGC • Assist data holders and departmental IT staff in complying with OGC requirements relative to litigation/preservation hold ○ Provide consulting and support in conducting search, preservation, and production and in protecting sensitive information • Ensure private information that may be preserved as a part of a litigation hold is appropriately protected • Document the steps that have been taken to collect and preserve data
	Departmental IT Staff	• Assist department data holders and the UA in conducting search, preservation, and production activities
	Departmental Management & Administration	• Inform OGC of any data holders who may not be available to comply with the preservation request • Support individuals who are requested to participate in preservation/litigation hold (data holders) and ensure they comply with OGC requests • Conduct search and preservation of relevant non-electronic materials when individuals are not available • Assist in the preservation of the litigation hold especially if the Data Holder is no longer able to do so.
	OGC	• Monitor the hold and ensure participants are conducting preservation activities as instructed
3000	**Production**	
	OGC	• Issue production notification and instructions ○ Specify the appropriate media to be used for production (consult with the UA for recommendations)

	Data Holders/ UA	• Conduct targeted searches to reduce volume of ESI • Convert ESI, as necessary, to formats suitable for review and production as indicated by OGC • Ensure any private or sensitive information is handled appropriately • Collect ESI from multiple sources and package • Collect any relevant non-electronic data • Deliver ESI and non-electronic materials to OGC using appropriate delivery mechanisms and ensure the integrity and readability of the materials that are provided to OGC
	Departmental IT Staff	• Assist data holders and UA in search and production activities • Perform any additional activities requested by OGC

	Responsible	**Process Steps**
	Departmental Management & Administration	• Collect and package non-electronic materials for individuals who are not available and provide to OGC
	OGC	• Collect and review ESI and relevant non-electronic information ○ Segregate private personal information and other confidential information that should not be provided • Monitor production activities • Provide data holders and the User Advocate with certification templates so that they can attest that information produced is complete • Develop overall statement attesting that information produced is complete
	UA	• Assist OGC as needed ○ Assist in developing statement of completion
4000	**Release Hold**	
	OGC	• Issue instructions to release hold • Continue to retain any data that was originally sent out as a part of the litigation case
	Data Holders/ UA	• Release/delete data as instructed by OGC
5000	**Ongoing eDiscovery Management Activities**	
	OGC	• Monitor active litigation cases and create periodic reports • Monitor the amount of time and any other costs associated with eDiscovery activities
	Data Holders/ UA	• Continue to retain any data that was included in a preservation/hold request until specifically instructed by OGC to purge
	Departmental IT Staff	• Document departmental instructions in applicable environments for suspending deletes, search, preservation, and production

	UA	• Provide guidance and templates for departmental eDiscovery instructions • Monitor the amount of time and any other costs associated with eDiscovery activities
	Departmental Management & Administration	• Monitor department involvement in any litigation cases and inform OGC if data holders terminate or transfer

Attachment 2: Frequently Asked Questions

Adopted from Educause (2006)

1. What do "electronic discovery" and "data preservation" mean?

"Discovery" is the process by which relevant information is exchanged between parties in a lawsuit. It is conducted via the exchange of information, production of documents, production of written statements, and the taking of depositions. Federal and state courts have long recognized that electronic data is subject to the same discovery rules as other evidence relevant to a lawsuit. The issue has received national attention because of a series of court rulings resulting in the imposition of large sanctions on parties for their failure to preserve electronic data and because of amendments to the Federal Rules of Civil Procedure that took effect on December 1, 2006.

According to these federal rules, the university and all of its faculty and staff members are now under a legal duty to preserve all evidence, whether hard copy or electronic, that might become *relevant* to the lawsuit upon notice that a lawsuit has been commenced against the University or if it is reasonably anticipated that a lawsuit may be brought (or a charge filed) against the university.

2. What information needs to be preserved?

Generally, the university is required to suspend routine or intentional purging, overwriting, re-using, deleting, or any other destruction of electronic information relevant to a lawsuit, including electronic information wherever it is stored – at a university work station, on a laptop, or at an employee's home. It includes all forms of electronic communications – e.g., e-mail, word processing, calendars, voice messages, instant messages, spreadsheets, videos, photographs, information in PDA's, and data in any other locations where electronic information may be stored. This electronic information must be preserved so that it can be retrieved – if necessary – at a later time. The information must be preserved in its original electronic form, so that all information contained within it, whether visible or not, is also available for inspection – i.e., it is not sufficient to make a hard copy of electronic communication.

3. What will I have to do as a "data holder"?

You will be notified of the duty to preserve electronically stored information through a notice called a "litigation hold" (or a "preservation hold"). You will then be asked to cooperate with the Office of

the General Counsel (OGC), the User Advocate, and your local IT personnel to ensure that all potential sources of electronically stored information in your possession or under your control are identified and preserved. You should be careful not to delete, destroy, purge, overwrite, or otherwise modify existing electronic data relevant to the case. You should also be careful to disable any automated purge or delete functions that may destroy relevant information. You should notify OGC if you believe other sources of relevant information exist of which OGC is not aware.

4. Who is involved in the preservation hold process?
While different individuals have particular responsibilities concerning eDiscovery, it is essential that the eDiscovery process is collaborative and all lines of communication remain open. For example, in order to ascertain the scope of potential eDiscovery, OGC will require reliable information from the Data Holders and User Advocates concerning the underlying facts of the dispute and the location of relevant ESI. Similarly, Data Holders and User Advocates may have questions for OGC that arise throughout the process. Detailed information regarding the responsibilities of the OGC, User Advocate, Data Holders, Departmental IT Staff and/or Departmental Management and Administration is outlined in the Guidelines section of this document.

5. For how long do I need to preserve this information?
OGC will notify you when you are no longer obligated to retain the preserved information. Generally, this will be when the statute of limitations has expired with respect to the claim or – if litigation has been commenced – when the lawsuit and all appeals have been concluded. If at any time you question whether to continue holding this information, you need to check with the OGC contact identified in the litigation/preservation hold before destroying any information.

6. Do I need to also preserve data on my home computer?
Yes, the same rules apply to any computer that stores information potentially relevant to a lawsuit. Thus, if you use your home computer for university-related business (including e-mail on your university e-mail account or on a personal account such as Gmail, etc.), you must preserve the data on that computer as well.

7. How will I know what information I need to preserve?
OGC will specify the search criteria that you will need to apply to select required information. Retrieved information should not be filtered, unless so instructed by OGC. OGC will segregate the information at a later time as needed.

8. Can I take personal or sensitive material that isn't relevant to the case off my computer?
You may remove data from your computer (or segregate it from the data that will be preserved) if you are absolutely certain that it is unrelated to the claim (e.g., correspondence entirely unrelated to university employees or university business, income tax returns, your music library, etc.). However, note that it is often difficult at the beginning of a lawsuit to be certain about what might later turn out to be relevant. So, you should examine each and every file you are considering deleting – i.e., do not make wholesale deletions of data. An attorney representing the opposing party about what data you may have destroyed may question you under oath at a later date.

9. I already deleted something that might be relevant --should I be concerned about that?
The duty to preserve information generally arises when you receive a preservation or litigation hold notice or when you otherwise reasonably anticipate litigation. Information not normally preserved before that time should not create a problem.

10. What if I am involved in an ongoing matter relating to the person who is suing the University?
You must also preserve any new electronic information that is generated after receipt of a *litigation hold* that may be *relevant* to the dispute (such as an employment claim by a current employee where relevant new documents may be created during the ongoing employment relationship).

11. Who will pay for the cost of preserving ESI?
The costs associated with complying with the e-discovery requirements will generally be handled in the same manner as other litigation expenses are presently handled. Internal costs, such as time
spent by employees and applicable storage costs will be absorbed by the department. If preservation appears to cause unusually high expense, the User Advocate and/or OGC may be consulted to recommend a course of action.

12. Who will be looking at my data?
Initially, no one will review your data. If and when a discovery request is made, you may be asked to conduct a search of the data or the User Advocate will conduct the search. The User Advocate will also store all preserved data. OGC (and possibly others) may need to review electronically stored information to assist in answering the lawsuit or to comply with discovery obligations.

13. Who decides what data will be turned over to the opposing party?
The same rules of relevance and privilege that apply to "paper" discovery also apply to the discovery of electronically stored information. Before any data is turned over to the opposing party, OGC will review it for relevance and determine that it is not otherwise protected or privileged.

14. What format or media should I use to preserve and produce required information?
In general, information should be preserved in its native form. It may include references and hidden information that should be preserved as well. For production, OGC will specify the required format and media type that will facilitate access to the information.

15. Since when did we have to go to all this trouble?
Electronically stored information has been discoverable since the 1980's. Because of the egregious misconduct by several defendants and because of the ever-widening use of computers, over the last several years the courts have developed rules specific to the preservation of electronic data. The new amendments to the Federal Rules of Civil Procedure addressing electronic discovery took effect December 1, 2006.

16. What if I don't want to disclose my data?
The university and its employees have a legal duty to preserve, and subject to the rules governing discovery, turnover electronically stored information. In short, the law does not offer us a choice. Failure to abide by the law may result in judicially imposed monetary sanctions and adverse findings in the litigation. We will take steps to protect your privacy and to ensure that protected/privileged information is not disclosed, but ultimately the court will be the arbiter of whether sensitive information must be disclosed. You may also want to refer to SPG 601.11 which addresses your and the university's responsibilities relative to privacy and the need to monitor and access records.

17. Will I be called to testify in court about information that I have preserved?
This will be very unlikely. Generally, any questions around the accuracy and completeness of

preserved information are addressed internally with OGC, the User Advocate, and the data holder. On rare occasions, the User Advocate may be called to testify about a particular case.

18. What should I do with my electronic data if I leave the University?

If you plan to leave your employment with the university during the pendency of a lawsuit for which you have received a preservation hold, you should confer with OGC or the User Advocate before relinquishing control of your computer.

19. Do Litigation Holds apply to backup and disaster recovery storage?

The answer to that is "it depends." This is a judgment call that would be generally left to OGC. The considerations are whether the information on such sources is likely to be discoverable and not available from other reasonably accessible sources. If in doubt, OGC should be consulted to make this determination. OGC, in turn, may solicit advice from the User Advocate and from other IT providers.

20. What if I have additional questions?

Contact the attorney or legal assistant who issued the preservation or litigation hold notice. For general information, contact one of the following legal offices with whom you most frequently interact:

Office of the General Counsel
5010 Fleming Bldg.
503 Thompson Street
Ann Arbor, MI 48109-1340
(734) 764-0304
ovpgc@umich.edu

User Advocate
For technical assistance relating to data preservation and production
itua-admin@umich.edu.

Office of the General Counsel: Michigan Medicine
300 North Ingalls Bldg, Room 3B04
Ann Arbor, MI 48109-5476
(734) 764-2178
ovpgc@umich.edu

Office of Technology Transfer
1600 Huron Pkwy, Bldg 520, 2nd Floor
Ann Arbor, MI 48109-2590
(734) 763-0614
techtransfer@umich.edu

Development Legal Office
9000 Wolverine Tower
3003 S. State St.
Ann Arbor, MI 48109-1288
(734) 647-6095
ovpgc@umich.edu