LEGAL HOLDS AND E-DISCOVERY GUIDELINES

UNIVERSITY OF OREGON

TABLE OF CONTENTS

A. INTRODUCTION

Court decisions and rules now place substantial obligations on public and private organizations to preserve all electronic materials that could be relevant to pending or anticipated lawsuits and to produce such materials in the course of litigation. These obligations apply to the University of Oregon and its employees. Failure to meet them could subject the university and the individuals involved to sanctions and liability.

The scope of these preservation duties is broad. They apply to business-related electronic information *wherever it is stored*—on a university work station, laptop, tablet, or handheld device, and even on an employee's home computer. This includes all forms of electronically stored information, including word processing documents, e-mails, text messages, calendars, images, videos, or any other digital information.

The rules concerning preservation of hard copies have not changed. All printed documents under the control of involved individuals must be preserved. While these preservation rules do not require the university to change any general records retention policies, they may require suspension of those policies in order to comply with legal preservation obligations, as explained in the guidelines.

Although legal duties require that information must be *preserved*, the preserved information need not be *disclosed* to other parties without first being appropriately reviewed to be sure that legally privileged information is removed. In other words, the university and its attorneys still can and will take steps to see that information that is legally protected will not be disclosed to the opposing party.

The guidelines below are intended to be a resource for the university community as it develops and implements policies, procedures, and/or best practices to comply with the aforementioned federal and state law obligations. Such practices or procedures may need adjustments if, for example, the relevant records include confidential student health care or survivors' services information, pursuant to the university's policy on confidentiality of client/patient health care and survivors' services information. We encourage you to contact the Office of the General Counsel for any questions regarding the content of the guidelines and for further discussion of appropriate handling of specific events where document preservation, retrieval, and/or production may be required.

B. THE LANDSCAPE OF ELECTRONIC RECORD SYSTEMS

1. University E-mail Infrastructure

The University of Oregon is a decentralized community—electronically and otherwise. With multiple campuses, numerous schools, colleges, and research centers, clinics, and largely-autonomous faculty, many computing solutions have been developed independently in an attempt to suit local needs. One aspect of this is that various departments and units operate independent e-mail systems. Thus, even though e-mail infrastructure operated by Information Services (IS) accounts for the vast majority of university e-mail, there are other e-mail messages being sent from and delivered to servers managed and operated directly by colleges, schools, departments/ units, and research projects within the UO.

2. University E-mail Storage

Although most e-mail comes into the university via central or departmental servers and often stays there until deleted, some people keep some or most of their e-mail in "local folders" on their individual desktop or laptop or other "client machine." In fact, e-mail messages may be stored locally instead of, or in addition to, being kept on an e-mail server.

3. Typical E-mail Use Patterns

The following are common ways that university employees handle their e-mail.

a. Centrally: Where e-mail inboxes and other folders are kept on a central Information Services (IS) server, with information technology (IT) professionals maintaining the servers and backups.

b. Centrally, then locally: Where the e-mail is initially sent to an inbox on a central server, but is frequently or always pulled to a desktop/laptop/handheld and may be erased from the central server. In such cases the folders are usually or always stored on the desktop, laptop, or handheld device.

c. Departmentally: Where e-mail inboxes and other folders are kept on a departmental, school, or research-group server.

d. Independently: Where e-mail comes directly to an inbox on an individually-managed server, which stores the user's folders.

The reality is that many individuals have "inherited," rather than consciously chosen, one of the alternatives above and may not even realize how their e-mail is handled. For example, copies of inbox messages may be stored on a local computer without the individual realizing it.

4. Storage of Other Electronic Records

In addition to e-mails, university faculty and staff create and use many other electronic materials ranging from word-processing documents and spreadsheets to databases, digital images, audio, video, web pages, instant messages, text messages, blogs, calendars, and more. While many of these records and data are stored on network servers managed by the university, individual users may be able to store them (or copy or move them) to individual desktop and portable devices. University data may also be stored on third-party cloud services.

5. Disaster Recovery Processes

Most servers at the university hosted by Information Services (IS) include a disaster recovery process that periodically copies its electronic data to tapes or other storage media to enable content restoration in the event of an emergency. Many of these processes recycle the storage media on a very short cycle. For normal preservation purposes, emergency recovery copies of data are not practically accessible and interrupting their recycling would be extremely impractical and expensive. As a result, such disaster recovery processes will usually be considered outside the scope of a litigation hold, unless otherwise directed. In contrast, other non-automated methods for archiving or backing up files are presumed subject to litigation holds. (For additional details, see the FAQs.)

C. EMPLOYEE RESPONSIBILITIES FOR RECORDS MANAGEMENT

Each employee is individually responsible for handling and maintaining records (including university e-mail and other electronic records) in accordance with university records retention policies and schedules. university managers, supervisors, and unit administrators are responsible for providing faculty, staff and other employees with appropriate access to such records and for overseeing the proper handling of records during employee transitions. The following outline provides additional information about these responsibilities:

1. New Employees

a. In general, each new employee is set up with a UO Duckweb ID and provided with e-mail, document, calendaring, and other software, with appropriate rights to create, use, and modify university electronic records, as determined by university policies and the employee's manager/supervisor.

b. Employees should be informed of university policies regarding electronic records, including but not limited to the university's acceptable use policy. Employees should also be reminded that all records relating to university business—including all electronically stored information, wherever located—are the property of the university, and that such information is subject to the Oregon public records law.

2. During Period of Employment

a. Records Maintenance and Management: Each employee is required to maintain records the employee is responsible for in accordance with university and departmental records management policy and procedure.

b. Records Retention: Records are to be retained according to the applicable university records retention schedule.

c. Records Preservation: Upon receipt of a legal hold notice or other instruction from university management (including the Office of the General Counsel), the employee is responsible for preserving the described records as instructed until notified otherwise.

d. Records Production: Upon receipt of a request to find and produce records (for a public records request, litigation, or other reason), the employee is responsible for diligently searching for requested records and providing them to the designated university representative.

3. Before Separating from Employment

a. Before an employee leaves a university position, the employee's manager, supervisor, or unit administrator is responsible for working with the employee to develop a plan for determining which employee maintained records should be preserved for business reasons or in accordance with university records retention policies and schedules and which records may be otherwise disposed of. An employee subject to a legal hold must contact the Office of the General Counsel at least two weeks before the separation date so that the university can ensure all relevant data are preserved after the employee's departure.

b. The employee and manager, supervisor, or unit administrator are then responsible for arranging for the appropriate transfer and disposition of the records.

4. After Employee Separation

a. The former employee's supervisors or administrators are responsible for managing records that are associated with a separated employee in accordance with UO policies and procedures.

b. To allow time for the department or unit to appropriately transfer ownership or dispose of the records, systems administrators should establish procedures to assure that e-mail and other electronic records associated with a separated employee are not automatically deleted.

D. SPECIAL PRESERVATION OF RECORDS

When a lawsuit is filed—or reasonably anticipated—the university has a legal duty to take special precautions to prevent the loss of potentially relevant electronic data (as well as data on paper and in other forms). Unless particular circumstances require a different approach, the following protocol will be followed to comply with these legal obligations.

1. Document Preservation Plan

When a lawsuit is commenced against the university—or information is received such that a lawsuit is reasonably anticipated—the Office of the General Counsel, in conjunction with the affected individuals/unit/information technology (IT) personnel will develop a preservation plan outlining the immediate steps that need to be taken. The plan will generally include some or all of the following basic steps:

a. Identify the department(s) and individuals who might possess relevant records;

b. Send a "legal hold" or "litigation hold" notice to the appropriate individuals;

c. Designate a specific individual to serve as the point-of-contact;

d. Assist the Office of the General Counsel in working with the opposing party's legal counsel to define parameters for relevant electronic data, including such things as the start date and time period for relevant records, specific categories of materials to include in searches, and other specific search criteria.

Where the matter is complex or unusual, the following steps may also be considered:

e. Gather a summary of the hardware and software involved;

f. Determine whether more aggressive steps are warranted, such as "imaging" hard-drives, sequestering computers, stopping rotation of disaster recovery tapes, or taking snapshots of network folders;

g. Establish a method for following up, which may include reminders, preservation questionnaires, conducting preservation compliance checks, and addressing new questions or issues from university employees with potential evidence.

The Office of the General Counsel should be consulted for assistance with any questions about an appropriate preservation plan. The preservation plan may need adjustments if relevant records include confidential student health care or survivors' services information, pursuant to the university's policy on confidentiality of client/patient health care and survivors' services information.

2. Legal/Litigation Hold

Receipt of a legal hold does not necessarily mean the recipient is directly involved in the matter. Rather, it means the evidence which the university is obligated by law to preserve may be in the person's possession or scope of responsibility and that the person, as an employee of the university, has a duty to preserve such information effective immediately. Though the contents and instructions of any legal/litigation hold you receive at the UO will come in the form of attorney client privileged communications (and constitute attorney work product), most legal/litigation holds typically include:

a. A brief description of the claims made or anticipated to be made in the litigation;

b. Identification of the categories of information to be preserved;

c. A direction to preserve relevant electronic records and paper documents and information on how to do so;

d. A direction to the administrator or responsible information technology (IT) staff to suspend any centralized or automatic destruction or alteration of records as well as instruction to affected individual employees to disable any user-established auto delete or auto-archive programs for electronic information that could result in destruction or alteration of any relevant materials;

e. A definition of what constitutes a "document";

f. General information on how to preserve documents, possibly including, depending on the circumstance, copies of a systems checklist; and

g. Contact information for the Office of the General Counsel attorney(s), risk management professional, Information Services (IS) or other IT professionals, departmental lead, or any other necessary contacts.

3. Typical Duties of Persons Receiving a Legal Hold

As a general matter, all recipients of litigation holds have a legal obligation to:

a. Cease automatic or manual/personal destruction of any relevant documents;

b. Preserve and protect all relevant documents in their original form; and

c. Follow all legal hold instructions and consult with the designated OGC, IT, and department personnel regarding any questions or concerns that arise.

4. Litigation: Actual or "Reasonably Anticipated"

The obligation to preserve evidence arises most commonly when a lawsuit has already been filed. However, the obligation can also arise when the university knows, or should know, it is "reasonably likely" that a lawsuit *will* be filed. Determining when facts or context indicate that a filed lawsuit is reasonably likely requires a case-by-case assessment of the facts and the application of experience and professional judgment. If, after reviewing this section and the factors described below, you believe litigation is reasonably foreseeable, please contact the Office of the General Counsel immediately.

The mere possibility of litigation does not necessarily mean that the filing of a lawsuit should be "reasonably anticipated." Rather, a duty to preserve is triggered only when credible facts and context indicate that a specific, predictable, and identifiable litigation is *likely*. Factors to consider in deciding whether litigation is "reasonably foreseeable" or "reasonably likely" may include, among other things:

a. Historical Experience: Look at whether similar situations have led to filed lawsuits in the past.

b. Filed Complaints: Be aware of complaints filed with the university or an enforcement agency, which may indicate a likelihood of a future court filing.

c. Significant Incidents: Pay attention to events resulting in known, significant injury.

d. Attorney Statements: Examine any statements by an individual's attorney regarding a dispute with the university.

e. Employee Statements: Consider statements by university employees and officials regarding the potential of litigation.

f. Initiation of Dispute Resolution Procedures: Give considerable weight to an action by a contractor to initiate a dispute resolution clause in a contract.

g. Public Records Requests: Consider whether a public records request suggests the likelihood of future litigation. Although the university routinely receives thousands of public records requests that are unrelated to litigation, sometimes a specific request may foreshadow a lawsuit.

h. Common Sense: Use your common sense. If an unfortunate or bad event occurs, especially if it is an unusual event or causes significant damage or distress, it might be reasonable to anticipate that litigation will follow.

5. Ending Preservation Responsibilities

When the litigation (or threat thereof) that prompted the legal hold has ended, the person or unit issuing the hold will inform those who received the notice that they are no longer under any special obligations to preserve the identified categories of materials. At that point, only the university's normal retention schedule will apply to the records.

E. RETRIEVAL AND PRODUCTION OF RECORDS FOR DISCOVERY

It is likely that records subject to a legal hold will never need to be retrieved and produced. In most cases, any need to actually produce preserved electronic records will come, if at all, weeks or months after the preservation has occurred. When the university receives a request from an opposing party for production of relevant records (what the law calls a "discovery" request), the university's counsel will determine the best approach to take in order to efficiently produce the complete and accurate response, as required by law. The response may consist of any or all of the following: (1) supplying the requested information; (2) attempting to obtain a modification of the request (e.g., by narrowing the request's scope or obtaining agreement as to specific search terms); and/or (3) declining to provide some or all of the requested data based upon privilege, expense of production, or some other appropriate and acceptable reason.

1. Options for Records Retrieval

Where some or all of the requested records must be retrieved, reviewed, and potentially disclosed, the following options should be considered to select the best approach to the specific request:

a. Relying on the Computer User: In many instances, it is reasonable and sufficient to simply ask the computer user to identify, copy, and provide potentially-responsive electronic records and to certify that these steps have been taken. In these instances, the production of electronic data resembles the typical production of physical documents.

b. Enlisting University Information Services/Information Technology Support: Sometimes particular concerns about an individual user's time, skill, or dependability in identifying the universe of responsive records will warrant the direct involvement of the relevant system administrator or other university technical support personnel.

Such personnel are often able to bring to bear sophisticated tools for searching and extracting large volumes of responsive records.

c. Using Outside Consultants: Where identification or recovery of records requires technical expertise beyond that readily available from internal resources, an outside firm may be called upon for some or all of the work.

2. Factors to Consider in Records Retrieval

a. Thoroughness: While the approach in a specific case should be reasonably calculated to gather all relevant records, the scope of discovery, at least in federal court, is limited to non-privileged matters that are *both* relevant to any litigant's claim or defense *and* proportional to the needs of the case—i.e., the record will reveal something of use in the case without excessive cost to uncover it. The old federal law standard, which required production of even inadmissible or irrelevant evidence if it was "reasonably calculated to lead to the discovery of admissible evidence," was recently eliminated from the new rules. This means discovery in federal cases will no longer be permitted merely when something "might" lead to the discovery of admissible evidence. (The relevant Oregon rule, however, has not yet changed.)

b. Operational Efficiencies: The activities required should be operationally efficient and proportional to ensure timely preservation and processing of the data.

c. Individual Privacy: The processes implemented to respond to discovery should take into account statutory or regulatory privacy concerns.

d. Risk of Data Loss: Reasonable steps will be needed to protect data from loss through inadvertent or intentional loss or deletion of files, metadata, or storage media.

e. Individual Disruption: Procedures should take account of the potentially significant impacts in terms of time and distraction for individuals named in the lawsuit.

f. Procedural Consistency: While the appropriateness of some procedures may vary depending on the circumstances of the case, once a process has been adopted, it should be consistently followed and executed.

3. Post-Retrieval Review

As potentially-responsive records are gathered, university attorneys will review the retrieved data for legal relevance and privilege or other protected status, and will handle all formal and informal responses to the discovery requests.

4. Post-Production Duties

The duty to preserve and produce information related to a lawsuit does not end with an initial production of records. Relevant information and records generated after the litigation hold must be preserved for future retrieval as the lawsuit progresses.

FREQUENTLY ASKED QUESTIONS

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

"Discovery" is the process by which relevant information is gathered by the parties in a lawsuit. One of the ways a party to a lawsuit can obtain "discovery" of relevant information is by asking other individuals or entities to produce documents. Federal and state courts have long recognized that the term "documents" includes electronically stored information (ESI) and that ESI is thus subject to the same discovery rules as other evidence relevant to a lawsuit. The issue has received substantial national attention over the past several years, however, because of a series of court rulings resulting in the imposition of huge sanctions on parties for their failure to preserve electronic data and because of amendments to the Federal Rules of Civil Procedure beginning in 2006. Upon notice that a lawsuit (or complaint to an administrative agency) has been commenced against the university, or if it is reasonably anticipated that a lawsuit may be brought, the university and all of its employees are under a legal duty to preserve all evidence, whether hard copy or electronic, that might be relevant to the lawsuit.

2. What data needs to be preserved?

The federal rules require a party to suspend routine or intentional purging, overwriting, re-using, deleting, or any other destruction of electronic information relevant to a lawsuit, wherever it is stored—at a university work station, on a laptop or cellular phone, at an employee's home, on a social media site, etc. It includes all forms of electronic communications, e.g., e-mail, word processing documents, calendars, voice messages, instant messages, spreadsheets, Wiki materials, videos or photographs. 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 (e.g., metadata), is also available for inspection. In other words, it is not sufficient to make a hard copy of electronic records.

3. What will I have to do?

You will be notified of the duty to preserve electronically stored information through a notice called a "legal hold" or "litigation hold." You will then be asked to cooperate with personnel from Information Services (IS) and the Office of the General Counsel to ensure that we identify and preserve all potential sources of electronically stored information (ESI) in your possession or under your control. You may be asked to complete and return a questionnaire identifying all potential sources of ESI. If so, it is critical that you complete and return the questionnaire without delay. You may also be asked to complete a signed statement confirming that you have completed the required search and retention as requested. Until information technology personnel have taken steps to preserve your ESI, you should be particularly careful not to delete, destroy, purge, overwrite, or otherwise modify existing ESI.

4. Does receipt of a legal hold mean I did something wrong or that I am somehow involved in the case?

Receipt of a legal hold does not necessarily mean the recipient is directly involved in the matter. Nor does it mean the recipient has done anything wrong. Rather, it means the evidence which the university is obligated by law to preserve may be in the person's possession or scope of responsibility and that the person, as an employee of the university, has a duty to preserve such information effective immediately.

5. How long will this go on?

The Office of the General Counsel will advise you when you and the university are no longer obligated to retain the preserved data. 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.

When the duty to preserve evidence ends, the preserved data will be returned to you or destroyed in accordance with university retention schedules. If at any time you question whether to continue retaining the records, you need to contact the appropriate contact person listed in the litigation hold communication before destroying any documents.

6. Do I need to also preserve data on my home computer?

Yes, if you use it for work. The same rules apply to any computer that stores information potentially relevant to a lawsuit involving the university. 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, Yahoo, etc.), you must preserve the data on that computer or account.

7. 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, such as income tax returns, your music library, etc.). However, we often find that it is 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. You may be questioned under oath at a later date by an attorney representing the opposing party about what data you may have destroyed.

8. I previously deleted something that might be relevant—should I be concerned about that?

The duty to preserve information arises only when there is a reasonable anticipation of litigation. Electronically stored information (ESI) deleted before that time pursuant to retention policies should not create a problem.

9. 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).

10. Who will be looking at my university data?

This depends on the reason for the litigation hold. If the matter involves a complaint or claim that requires investigation (e.g., a Title IX complaint), appropriate university personnel from departments such as the Division of Student Life (Title IX Coordinator), the Office of Affirmative Action and Equal Opportunity, the Office of the General Counsel, and perhaps others may be reviewing some of your records in the course of the investigation. In other cases, it may be that no one will initially review your records until and if there is a lawsuit filed with discovery requests made.

11. Who decides what data will be turned over to the opposing party?

The university, as owner of the data, will make these decisions based on advice from its attorneys. Before any data is turned over to the opposing party, the university's attorneys will review it for relevance and protect (e.g., withhold, redact, or obtain a protective order as to) any portions that are protected or privileged.

12. 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 organizations 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 amendments to the Federal Rules of Civil Procedure addressing electronic discovery first took effect in December 2006. They were most recently amended in December 2015.

13. What if I don't want to disclose my university data?

The university and its employees have a legal duty to preserve and, subject to the rules governing discovery, turn over 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 (or other) sanctions against the university and/or you individually and adverse findings in the litigation. We will take steps to protect your privacy and to ensure that protected or privileged information is not disclosed, but ultimately the court will be the arbiter of whether sensitive information must be disclosed.

14. 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 litigation hold, you should confer with the Office of the General Counsel and other contacts listed in the litigation hold notice.

15. What if I have additional questions?

Please contact the Office of the General Counsel and/or the points-of-contact listed in the litigation hold notice.