E-DISCOVERY IDENTIFICATION & PRESERVATION GUIDE FOR LAWYERS
Version 2.0

(Revised November, 2015)

This document is a concise guideline offered by the NY City Bar Association.
It is not a checklist of required procedures.
For a more detailed explanation of an attorney's duties and responsibilities concerning e-discovery, readers are referred to the non-exhaustive index of e-discovery-related resources located at the end of this document.

I. Checklist of Substantive Steps To Identify and Preserve Data:

Documents need to be preserved at the outset of litigation or as soon as litigation is reasonably anticipated. Follow these steps immediately upon retention for a new litigation or potential litigation, regardless of whether you are engaged by the plaintiff or the defendant, to facilitate the collection, analysis, and preservation of electronically-stored information ("ESI") that may be relevant to the matter (and to keep costs down). Remember to **carefully document each step taken**. It may be several years before you or your client need to defend and explain the preservation measures undertaken at the beginning of a retention. You should memorialize your preservation efforts contemporaneously.

Substantive Steps

1. Determine what rules apply.[1]

2. Identify the key claims or defenses in the lawsuit.

3. Identify the names of all key players who might have information relevant to the claims or defenses of any party to the lawsuit (the "Key People"). This includes third parties over whom your client has control, as well as any documents and records of former employees that are still within your client's custody and control.

4. Identify the time frame for relevant materials.

5. Issue preliminary verbal instruction to the client not to destroy any documents that might be relevant to the litigation, and then work with the client to issue an appropriate litigation hold letter.

6. Preserve a written record of your analysis, actions and conclusions concerning Steps 1 through 5.

[1] Depending on the forum in which your case is litigated, the amendments to the Federal Rules of Civil Procedure (effective December 1, 2015) may significantly impact the manner in which you conduct electronic discovery, particularly with regard to proportionality (Amended Rule 26 (b)) and preservation obligations (Amended Rule 37(e)).

Additional Steps to Consider

1. If you are in a law firm, be sure to meet with the attorney responsible for the client relationship ***before*** contacting the client about this protocol, and keep the relationship attorney in the loop concerning all steps of the protocol.

2. Think about metadata. When your client accesses ESI, their actions are reflected in document properties (the "metadata"). There is a risk that metadata will change if the employee interacts with the ESI (forwards, saves, edits, etc.) after the hold has been issued. You should assess the possible impact on your case of such changes. If the legal hold directs employees to hold data in place in the ESI environment, you may want to direct the client not to access ESI that is on legal hold – this means they should not open a relevant document or forward a relevant email, etc. If a client needs to continue to access any ESI that is on legal hold, consider making a preservation copy of the data and associated metadata. The preservation copy should be created in a manner that maintains the data and metadata as it exists when the hold issues. This preservation copy can be made of the relevant, generally accessible ESI (referred to as a "forensically sound copy") or of all data, including deleted data if any (referred to as a "forensic image"). Consideration should be given to what is important for the particular matter.

3. If forensic images are made, ensure that proper records are maintained to establish the chain of custody and authenticity of any imaged files.

4. Conference with the client's IT department and go over the below ***Checklist to Define the Scope of Electronic Discovery***.

5. Preserve a written record of your analysis, actions and conclusions concerning Steps 1 through 4.

II. <u>Checklist to Define the Scope of Electronic Discovery:</u>

"***WHO"***

1. Identify the internal and external personnel responsible for the management and maintenance of the technology infrastructure and all of its components, with contact information (the "Technology Personnel"). The firm's IT department can help you identify the personnel and components.

2. Identify the names, addresses, and contact information for any third party over whom your client has control that holds or has access to company ESI that contains information that may be relevant to the lawsuit, and make sure they are told to comply with a litigation hold. A litigation hold letter should be sent to any such third party. Maintain copies of such litigation hold letter(s), as well as all communications with the third party..

3. Complete a preliminary list of the Key People (referenced above) who might have information relevant to the claims or defenses of any party to the lawsuit.

4. Preserve a written record of your analysis, actions and conclusions concerning Steps 1 through 3.

"WHAT / WHERE"

1. It is important to obtain a detailed description of the relevant types of categories of ESI and the architecture and elements of the client's computer system and ESI storage, including, but not limited to, hardware systems (the amount and types of computers); operating systems, and software applications, including customized applications, with graphical representations if available. This description should include:

    A. Servers and Mainframes
        a. Network file systems
        b. Shared Network Drives Folder Structure
        c. Individual User Network Drives Folder Structure
    B. Workstations
        a. Hard Drives Folder Structure
    C. Voice mail
    D. Fax machines (these usually store data as well)
    E. The "Cloud." (This is an evolving area. You should understand how the Cloud affects the e-discovery you are working with).

2. Obtain a detailed description of the architecture of the electronic mail system, including, but not limited to, server and workstation software and versions, lists of e-mail users, and location of e-mail files and folders and archived emails.

    A. Be aware that email systems are often integrated with contact lists, calendars, and to-do lists, all of which may contain relevant ESI.

3. Identify whether custodians of ESI use additional methods to engage in business activities, such as:

    A. Local hard drives on work computers (desktops and laptops);
    B. Personal home computers, including laptops, tablets and netbooks;
    C. PDAs / Cellphones / iPhones / Android Phones/ Blackberries;
    D. CD-ROMs / DVDs;
    E. Thumb drives / Flash media;
    F. Removable / portable hard drives;
    G. Floppy diskettes;
    H. Zip disks;
    I. Data archives (e.g., tape archives, cloud archives, etc.);

J. Digital cameras;
K. Third-party data archives:
    a. Social media sites (including LinkedIn, Facebook and Twitter)
    b. Consider whether employees are using personal email and instant messaging accounts for business purposes (e.g., Gmail, Hotmail, AOL, AIM, Skype etc.). Typically, a certain amount of these emails are maintained on a client's personal computers, but much more data is kept at the "source" vendor, e.g., kept at Google. If a production request is received and such accounts are used for business activity, these "source" vendors should be contacted by the employee who owns the account to determine the ability and cost of obtaining back-up emails.

4. Obtain a detailed description of the client's computer-use policies and procedures, including, but not limited to:

    A. employee guidelines;
    B. company policies on e-mail usage;
    C. company policies on Internet usage;
    D. password use;
    E. security controls;
    F. information sharing.

5. Describe any monitoring or logging of employees' computer usage.

6. Preserve a written record of your analysis, actions and conclusions concerning Steps 1 through 5.

"HOW PRESERVED"

1. If the company has a document retention policy, obtain a copy ***and confirm that it has been suspended*** in a manner appropriate to the litigation.

    A. Whether or not the company has a formal document retention policy and litigation-hold policy, confirm with the Technology Personnel that the preservation steps set forth in the litigation hold letter you issued to the client have been implemented.

2. Although backup tapes may not ultimately be produced in the litigation, it is necessary to understand the details of any backup policies, procedures, and schedules, including, but not limited to, details concerning hardware and software used to back up and archive information, documentation of what data is backed

up, and locations of all backup media devices. Also determine the frequency of the backups (monthly, weekly, daily, etc.) and whether the backups are incremental. If the company utilizes backup tapes, it is recommended that the earliest backup tapes are pulled out of circulation and preserved.

3. Obtain a description of the company's procedures with respect to employees who are terminated after the implementation of the litigation hold and ensure that all ESI that may be relevant to the action relating the Key People are preserved even if a Key Person is terminated after the litigation hold is implemented.

4. At some point in the preservation process, a determination should be made as to whether to take images of servers, hard drives on laptops, desktops and home computers (used for employment-related work), text messages residing on PDAs such as iPhones, and fax machine memory.

    A. Consider the potential benefits of using a professional to make a forensic image of the relevant data.

5. As the case progresses, periodically confirm in writing with the Technology Personnel that the preservation steps set forth in the litigation hold letter you issued to the client have continued to be followed. The burden to preserve ESI falls on both inside and outside counsel in New York.

6. Preserve a written record of your analysis, actions and conclusions concerning Steps 1 through 5.

III. Resources

1. The Sedona Principles, Second Edition: *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, June 2007.

2. Joint E-Discovery Subcommittee of the Association of the Bar of the City of New York, *Manual for State Trial Courts Regarding Electronic Discovery Cost Allocation*, Spring 2009.

3. The New York State Unified Court System, *A Report to the Chief Judge and Chief Administrative Judge, Electronic Discovery in the New York State Courts*, February 2010.

4. Report of the E-Discovery Committee of the Commercial and Federal Litigation Section of the New York State Bar Association: *Best Practices in E-Discovery in New York State and Federal Courts*, Version 2.0, December 2012.

5. The Sedona Conference "*Jumpstart Outline*", March 2011.