



100 California Street, Suite P-10, San Francisco, CA 94111 | 415.392.2900 | [www.sanfranciscolegal.com](http://www.sanfranciscolegal.com)



## Electronic Discovery Checklist

### Before litigation – BE PREPARED!

- ✓ E-discovery team in place and trained, including Legal, IT, Compliance, Human Resources, Records Manager and other potential stakeholders
- ✓ Litigation protocol drafted and key personnel trained.

### At reasonable anticipation of litigation

- ✓ Evaluate type of litigation involved. (Serial? Class Action? MDL?)
- ✓ Litigation protocol implemented and process documented
- ✓ Preservation and litigation hold notices sent? Tracking initiated? Management of litigation hold implemented? Manager of litigation hold identified and fulfilling duties? Custodians aware of project manager?
- ✓ Other reporting required? 10-K, Regulatory, etc.

### WHO?

- ✓ Have all custodians been identified?
- ✓ Interview of custodians for relevant information
- ✓ Are custodians inside or outside the U.S.? (Privacy issues may exist for personnel and data residing outside of U.S.)
- ✓ Include past employees
- ✓ Identify and interview assistants and others with access to data of key custodians
- ✓ Identify where data is stored in organization
- ✓ Discuss redundant storage, backup plans and disaster recovery plans

## WHAT?

- ✓ What types of data? (Format, applications, operating systems, email platform for both client and for others from whom you expect discovery)
- ✓ What is the scope of the engagement or discovery request? (Servers and workstations, VPN, home computers, cell phones, PDA's, laptops, thumb drives, copiers, scanners and fax machines, back up tapes, email, Lotus, GroupWise, Exchange)
- ✓ Any third party vendors that need to be involved? (Encryption, custom database?)
- ✓ Privilege and Protected Data (Consider nature of data, i.e. trade secret or privacy protected? Attorney-client protected? Other?)
- ✓ Are agreements in place regarding privileged or protected material? (Clawback or quick peek agreements.)
- ✓ How does court prefer to handle eDiscovery?
- ✓ Who is paying for this discovery?
- ✓ Insurance? Cumis counsel issues been addressed?
- ✓ Entity? Funding approved and available?
- ✓ Identify "inaccessible" ESI. (undue burden or cost)

## WHERE?

- ✓ Analyze data map of organization (Identify and be prepared to discuss what and where data resides in your environment, particularly with regard to identified custodians)
- ✓ Document retention policies. (Identify and understand and be prepared to disclose and discuss ALL retention policies that may apply to the data.)

## WHEN?

- ✓ When does the planning need to be complete?
- ✓ Are there time constraints for collection? Production? Rolling basis or one time? Meet and Confer?
- ✓ What is the anticipated time frame of the action?
- ✓ Legacy systems -- Have prior systems been included in planning? If mergers were involved, has archived data been included in the process?

## HOW?

### Collection Protocols

- ✓ Defensible, use properly trained personnel or vendors
- ✓ Proper documentation of methodology and chain of custody
- ✓ Document serial numbers of custodian's workstations and photograph, where appropriate
- ✓ Need to produce to outside counsel? Opposing counsel?
- ✓ How many copies of the data set are needed?
- ✓ Ensure no changes are made to metadata or content during collection

### Preservation of digital evidence (ESI)

- ✓ Keep in secure room, locked and climate controlled.
- ✓ Maintain chain of custody with original media

### **Production – how is data to be produced?**

- Native      – Paper
- Tiff        – Coding
- PDF        – OCR

### **Review tool - choice**

- ✓ Server/station based or net based
- ✓ Native review
- ✓ Clustering tool

### **Review tool requirements?**

- ✓ Load file needs
- ✓ Access permissions management and control
- ✓ Pre-processing electronic data
  - De-duplicating                      – Tracking processes
  - Filtering                                – Clustering
  - System file removal

### **NEXT**

- ✓ Archiving -- Compliance, by code or regulation, future litigation, etc.
- ✓ Re-use and ongoing use of data
- ✓ Testimony during deposition or trial? Who is going to be your testifying expert on how the data was collected? 30(b)(6) designee for Litigation Hold; for data collection; for infrastructure.
- ✓ Trial presentation needs

### **ALWAYS**

- ✓ Document processes employed; why chosen; how implemented; results; hash values and authentication; chain of custody; audit trail for all data.

### **QUESTIONS?**

Contact Joel Resnick

San Francisco Legal Director of Collections and eDiscovery

415.392.2900 or email [joel@sanfranciscolegal.com](mailto:joel@sanfranciscolegal.com)