



## Issues to Think About When Maintaining Integrity of Data:

---

- Use of forms, checklist, trip reports and written procedures is crucial as document collection staff will not have to rely on memory during a deposition or trial.
- Gather contact information from the document custodian as well as the person doing the collecting.
- Make use of serial numbers and asset tags to tie data collected to a specific machine and thus a specific person.
- Track the external devices on a custodian's machine to ensure knowledge regarding the machine's external media capacity. For example, recording whether a CD drive is a read-only drive will reduce the likelihood that the opposition can allege that CD back ups were produced from that computer.
- Describe the data:
  - Media type, standard and manufacturer
  - Serial numbers and/or volume names
  - Writing on labels
  - Characterization of data
  - Amount of data
  - Type of data
  - Write-protection status
- Describe data collection procedures:
  - List of tools used for each procedure
  - Name of individuals conducting each procedure
  - Outcome of procedure
  - Problems encountered, if any.
- Record the movement of data, including reason for transfer.
- Document rationale for what document custodians and what data you decide to include in your data set.
- Document the name and contact information for each person that handled the data.



- Document the system configuration, hardware, software and operating system.
- Document how it was transferred to its current format.
- Ensure the accuracy of the date, time, and other authenticating stamps on the data.
- Document where on the hard drive individual files physically located.
- Document what metadata is available, and what file does it link to?
- Document what was the relationship between e-mails and their attachments.
- Document dates for when data was collected, where it stopped along the way and when it arrived at its final location.
- For off site collections, securely package the data and send or hand carry to its final destination with the chain of custody form. Document your packaging and transportation method.
- Fully inventory and uniquely number each file in the data population for 100% file accountability.
- Digitally fingerprint each file to ensure a legally defensible audit trail.
- Identify documents by state-of-the-art signature analysis not by extension.
- Ensure original data is never compromised by virus scanning all data to prevent cross-contamination. Record any viruses found.
- Prior to examining any media or making copies, ensure the originals are write-protected so that no data is added or changed during inspection and copying.
- Mirror image hard drives sector-by-sector. Simply making a file-by-file backup may be deemed inadequate for evidentiary purposes.
- Use a reliable copying process that (1) meets industry standards for quality and reliability; (2) is capable of independent analysis; and (3) creates tamperproof copies.
- Use duplication techniques that do not alter data.
- Print directory listings for each piece of media.
- Label the media with time, date and source.
- Maintain a written log of all procedures the data was put through.
- Restore each piece of media to a file with a name that corresponds to the number assigned to the media being restored.
- Verify all files on the directory listing appear in the copy restored.
- When printing a particular document, insert a distinct header or footer that gives the full directory listing for the document printed.



- Protect data from magnetic fields and other dangers that can damage data.
- Provide state-of-the-art security for data storage, including secure buildings, processing centers, and employees. Firewall intrusion detection and protection, secure digital certificates, and a minimum 512-bit SSL keys with 128-bit SSL encryption for any data transmissions is also prudent.
- Isolate experts who will testify for chain of custody purposes from the people helping with the review strategy.
- Be able to aggregate and convert electronic data into common formats such as HTML, TIFF, and PDF, creating a unified and secure database of original content and metadata, fully indexed and optimized for searching.
- When it is possible to download original documents, i.e. during a review of native files, control who can download copies of the original documents, and all downloads should be logged, enabling you to track who downloaded what material on specific dates.



## Questions You'll Need to Answer:

---

Your Document Custodian may be asked a series of questions in court to verify the authenticity of the data, which includes a thorough documentation of the chain of custody for each item of data. They must be able to answer these questions:

- What is the data and what does it purport to be?
- Where did it come from?
- Who created, discovered, and recovered it?
- How was it created, discovered, and recovered?
- Were there any material changes, alterations or modifications during the recovery of the data such that it may no longer be what it once was?
- What has happened to it since the time it was created, discovered or recovered? Is there any chance that the data was changed, altered, or modified between the time you obtained the data and today?
- Are individual directories purged when a person leaves the company?
- Are passwords and access codes revoked when an employee leaves the company?
- Are workstations reassigned to incoming employees? If so, are hard drives wiped and reformatted for the new user? Are hard drives backed up before the new user takes the system?
- Describe how used equipment is disposed of or sold.
- Describe how used disks or drives are treated before destruction or sale.
- Have you used outside contractors to upgrade hardware or software?
- Are changes or modifications made to software recorded?
- Are there any logs kept for the deployment and destruction of systems?
- Describe your companies back up procedures.
- What systems, computers, servers are backed up?
- What applications are used to archive and back up data?
- What are the rotation procedures?
- Is there a retention policy?
- How are files removed or deleted from your system?
- Is there a disaster recovery procedure?



- Do employees have external access to the internal system?
- Are there logs that track access?
- Are there passwords to gain access?
- Is removable media used by employees?
- Have any computer hardware upgrades been performed in the last 6 months?
- Have any computer software upgrades been performed in the last 6 months?
- Are there any utility applications used on either local machines or servers?
- Are there any disk cleaning applications used on either local machines or servers?
- Are there routines on the server that control purging of logs or other maintenance information?