Five Types of ESI Chain of Custody Documentation

Maintaining a complete chain of custody record involves multiple types of documentation, reports Indiana lawyer Helen Geib for **QDiscovery**. What types are used in a particular case depends on what the evidence is and how it's handled. These are the five major categories of ESI chain of custody documentation.

a) Collection forms – Collection forms should record:

– Client, case or project name, and client-matter number;
– Date and time, location, and the name of the collection technician;
– The copying programs and/or other collection tools used;
– Description of collection target (e.g., network share, cell phone);
– Custodian name or similar identifying information for the data source;
– Details about the collection such as the number of files copied and errors;
– Description of destination media (e.g., external hard drive with inventory number);
– Unique project and collection tracking numbers; and,
– Any pertinent notes about the collection.
– You can download a sample PDF copy of the QDiscovery collection form at http://qdiscovery.com/images/QDiscovery_Data_Collection_Form_Sample.pdf.

b) Photos – Photos should be taken of physical evidence, electronic devices, and media like hard drives and DVDs. In the ESI context, this typically means photos of labels and any noticeable damage such as a bent cell phone casing.

c) Delivery and shipping logs –A combination of logs and forms is used to document basic information like date, sender and recipient, courier/shipper, and tracking number. Shipping labels and packaging are typically documented with photos, although these may also be scanned or even stored as-is, space allowing.

d) Transfer and handling logs – Evidence intake, check-in/check-out, and hand-off is documented with logs recording the what, who, when, where, and why of the transfer. The "what" of electronic devices and physical media includes a description of the item (e.g., make and model, serial number), any labels, and a list of peripherals like power cords. The "what" of ESI is data volume/file size and other information sufficient to identify the data, such as custodian name, folder name, how it was transmitted, and hash value.

e) Software logs –Copying and other ESI-related software programs automatically generate various verification, tally, and error logs. These are programs used for:

-Making forensic images of computer hard drives and other electronic devices and media;
-Copying electronic folders and files;
-Forensic examination of physical evidence or in the ESI context, electronic devices, media, and files;
-ESI processing in connection with using a document review database; and,
-Generating document production sets.

f) Other supporting documentation – The final type is supporting documentation about chain of custody procedures, software tools, and evidence repositories. For example, validation documentation is available for forensics software and hardware. This category also includes forensic lab best practices and security protocols for evidence lockers and media storage rooms.