ISO/IEC 17020
8.4 CONTROL OF RECORDS

8.4.1 The office shall establish procedures to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of its records related to the appropriate control of records. This requirement means that all records needed to demonstrate compliance with the requirements of the standard are to be established and retained. A unique case number is assigned to every case when evidence is initially received by the office.

Records: Case records consist of technical and administrative records; i.e. autopsy and related laboratory and consultation reports, diagrams, body transport forms, chain of custody, purchasing and inventory forms, consultant agreements, personnel records, facilities and equipment records, and employee files. An information management system (IMS) will be the primary depository for all case records. Technical records not stored in the IMS will have a statement in the case file to notate where the records are stored and shall meet all technical record requirements pertinent to the IMS. Technical and quality records not stored on the IMS will be maintained so as to prevent damage, deterioration or loss. If an original record, paper or other media is captured as an electronic record, and the original record will be destroyed, ensure the electronic record is complete prior to destruction. All records shall be legible. All alterations, changes, corrections, etc. will be made in such a way that nothing is erased, obliterated, made illegible or deleted. Anything needing modification shall be struck through with a single line and the correct or appropriate information (if applicable) entered alongside. All alterations shall be initialed by the person making the change. Electronic records will be modified in an equivalent manner.

Security: Only authorized individuals may access case files. These are individuals who are trained and have authorized access by issuance of access privileges on the IMS. All individuals will sign a document concerning the security of their passwords and PINs. Audit trails are established on all transactions on the IMS. All electronic records are backed up and stored by an electronic system separate from the main IMS.

Technical records: Technical records or the analytical file/examination documentation are the analyst notes (including any and all original written documentation of observations and measurements), charts, graphs, data, worksheets, conversation records, photographs/images and other material generated in the processing of a case.

Worksheets may be used, when available, and all administrative data will be completed on the worksheet. All notes will be neat, legible, clear, and concise. Any drawings will be representative of the object. All handwritten records will be generated in ink. All abbreviations or symbols used within the technical record will be clarified within official manuals, forms or worksheets.

Each technical record generated in an analytical file/examination document will contain the case number, item/submission number (if applicable), the identity of the person responsible for creating the technical record and the date the record was generated. Technical records that apply to multiple cases, multiple items within the case or the entire case (e.g., controls, conversation records, standards, etc.) do not require the addition of an item/submission number. The date of technical record generation is the same as the date of insertion in the IMS

unless otherwise noted. Any image opened in the IMS for viewing will have tracking information of who reviewed the image prior to release and the date of review.

Information concerning the traceability of the technical data/examination document contained within the case record as images can be obtained through queries of the IMS database.

Record keeping: All technical records relevant to a particular service request will be stored in the appropriate case record indefinitely.

Personnel responsible for sampling and performance of each test/activity can be determined based on information provided within the technical record. The handwritten initials or signature or secure electronic equivalent of the individual who prepared the technical record will be recorded on the examination records representing his/her work.

Any individual who makes changes or annotations to examination documentation must also include their initials or signature.

The analyst assigned to the service request is responsible for ensuring the accuracy of calculations, which are not part of a validated electronic process.

The analytical file will contain all records used by the employee to prepare a final report. Dates will indicate when the work was performed.

Technical data considered to be invalid will be stored under the appropriate case request and will be labeled to indicate that the data is invalid. The reason(s) the data is deemed invalid will be recorded.

When test data or observations are rejected, the reason(s), identity of the individual determining taking the action and date will be recorded within the technical record(s).

All examination documentation will be of sufficient detail that the employee, the peer reviewer and another competent analyst or supervisor can evaluate the test performance and interpret the data. If analytical data or photographs are not of sufficient quality or detail to document the basis for the conclusions derived from the evidence examination, then worksheets and/or notes must provide the necessary details to satisfy these requirements. In no instance shall a photograph or data contradict supplemental information without explanatory comments (i.e., poor quality image, interference, etc.).

Peer review documentation will contain the identity of the reviewer.

Verifications of findings will only be performed by qualified examiners. The record of the review shall indicate the identity of the verifier, the date of the verification and the specific finding that was verified as being in agreement. The record of the verification shall be traceable to the verifier (initials or electronic equivalent).

All administrative documentation in the case file will include the specific case number.

The IMS contains the description of evidence, images of packaging and seals if warranted, chain of custody and customer information.

Once an image file has been stored within the case record, no modification to the image other than annotation of additional information on a particular image can occur. Images may only be deleted from a case record by individuals with appropriate security permissions. This information is traceable through the databases associated with the IMS.

Timeliness: All data will be recorded at the time of the examination, along with the date the examination was performed.

Corrections and changes: Nothing in the examination documentation will be obliterated, made illegible, deleted or overwritten. Changes to hard copy data will be performed by a single strikethrough of the incorrect notation. The initials of the individual making the change will accompany the change/correction written adjacent to the original location.

Changes to hard copy documents after they are scanned to the IMS will be made as above to the hard copy. The corrected document will then be scanned into the IMS. The corrected document will not overwrite the original. Alternatively, the image of the document can be annotated and initialed.

Corrections to image annotations will be performed by a single strikethrough of the incorrect annotation. The initials of the individual making the change will accompany the corrected information.

Changes in the IMS generate an audit trail within the database. The original data is recoverable.

8.4.2 The office shall establish procedures for retaining records for a period consistent with its contractual and legal obligations. Retention schedules take into consideration legal requirements, when applicable. Access to these records shall be consistent with the confidentiality arrangements.

Confidentiality: All records are considered confidential. State laws specifically define those individuals, such as family members, who may obtain copies. Defense counsel and other interested parties may access these records through the legal discovery process.

Retention: All documents will be retained indefinitely in the IMS.