## Policy Circular 40 — September 2012

**Issued**: September 2012

# Forensic Operations Module

# 1. Introduction

To apply for the Forensic Operations Module (FOM), the facility must already hold accreditation in any of NATA's current fields or programs.

This module is applicable only to facilities which may be required to have test results used in legal proceedings.

**Note:** Facilities conducting paternity testing for non legal purposes are not permitted to apply for the FOM to cover court proceedings. Accreditation in Forensic Science is required.

Accreditation for the FOM is generic and deals with the facility's ability to have a system in place to ensure results and processes are able to undergo legal scrutiny. The FOM may cover the entire scope of accreditation currently held or only parts thereof as identified by the facility.

The requirements for accreditation covered by the FOM can be split into the following main categories:

- Control of records
- Handling of test and calibration items
- Assuring the quality of test results

# 2. Requirements

The activities described in this module are in addition to those required by the relevant standard(s) and Field Application Documents (FADs) for which accreditation is held. The requirements to be adhered to are as follows:

### Control of records - Technical and administrative records

In addition to requirements as detailed in the relevant standard(s) and FAD(s), the records system must include all data and observations and any other analytical/examination or administrative records which support conclusions.

Examples of administrative records include case-related conversations which support or impact on the outcome, evidence receipts, description of evidence packaging and seals and subpoenas.

Examples of analytical/examination records would include reference to procedures followed, tests conducted, standards and controls used, diagrams, printouts, autoradiographs, photographs, digital records (including digital photographs, video and audio records), observations and results and reports of examinations. Electronic storage of records is acceptable.

Instrument charts and graphs of analyses that are batched (e.g. blood alcohol determinations, drug screening) may be more appropriately kept in a central location as specified in the facility's procedure manuals.

In general, the records required to support conclusions shall be such that in the absence of the analyst/examiner, another competent analyst/examiner or supervisor can evaluate what was done and interpret the data.

The facility must maintain a case record in a designated location(s) under a unique case designator, usually a facility case number.

Administrative, examination records and analytical documentation generated by a facility on a particular case, either on paper or electronically, constitutes a case record.

Since case notes and records of observations are subject to subpoena or discovery, they must be of a permanent nature. Handwritten notes and observations must be in ink not pencil. Pencil (including colour) may, however, be appropriate for diagrams or making tracings.

Abbreviations are acceptable only if they are readily comprehensible to a reviewer.

Where appropriate, observations or test results must be preserved by photography or electronic scanning (e.g. electrophoretic runs, physical matches, quantitation results). Photocopies may also be suitable (e.g. thin-layer chromatography results, questioned documents). This will need to be evaluated on a case by case basis. It may be necessary to augment case records to verify opinions or interpretations reported.

Where instrumental analyses are conducted, operating parameters must be recorded including those not specified in the method

When a test result or observation is rejected, the reason(s) must be recorded (e.g. instrument or standard failure, a result off scale or outside acceptance criteria for the method).

Each page of every document in the case record must bear the facility's unique case identifier. Where pages are secured as bundles the case identifier need only be applied to the first page.

**Note**: Electronically-generated records meet the requirements if they include the printed case identifier and the analyst/examiner's name or initials.

It must be clear from the case record:

i) when each stage of the analysis/examination was performed (i.e. relevant date(s) and, where appropriate, the time(s);

ii) that all analysts/examiners and checkers are identified.

The facility must have a system to uniquely identify all records in or pertaining to the case record. The total number of pages in the case record must also be clearly identified.

An index to the contents of the case record or a page numbering system may be appropriate.

Documented facility procedures must include a description of the storage of records, such as chromatograms, not stored in the case record.

It is acceptable for physical records such as chromatograms, photographs, impressions/moulds etc to be stored in the case record in a bag/envelope secured to prevent loss which contains an itemised description of contents, case number, analyst's identification and that the bag/envelope itself is identified as part of the case file.

The requirement to initial and date all changes to original data generated by the facility does not necessarily apply to situations where notes are created contemporaneously. It must however be clear where contemporaneous notes begin and end.

### Security and access

a) Policies and procedures on facility security must be documented.

b) The facility must have arrangements in place to detect unauthorised access, (all exterior entrance/exit points to the facility must be controlled in order to prevent access by unauthorised personnel and all security doors must have keys or other access devices limited to authorised personnel).

The entire exterior perimeter of a facility must inhibit unauthorised access. For example, in the absence of intrusion alarms, suspended ceilings which permit undetected entry to the facility are unacceptable.

The facility must be monitored during vacant hours by an intrusion alarm or by security personnel.

The action to be taken in the event that an unauthorised access to the facility is suspected, must be documented.

c) Where a facility exists within a host agency facility, documented procedures may be required to permit out-of-hours entry for emergencies. Such arrangements are acceptable if they include, for example, the breaking of a storage seal to access a key or code and/or notifying an authorised staff member.

Each emergency access to the facility must be recorded.

d) Access to the operational area of the facility must be controllable and limited.

Visitors must not have unrestricted access to the operational areas of the facility.

A record must be retained of all visitors to operational areas of the facility.

Persons, other than facility staff who have a legitimate reason for requiring access to the operational areas of the facility (e.g. use of shared equipment, cleaners) may be given authorisation by the facility director for access to specific areas of the facility without the need to be 'accompanied' by a member of the facility's staff.

There must be documented procedures for the authorisation of such persons and a record must be maintained of their time spent in the facility. In general, it is expected that such persons will meet appropriate security standards as required by the facility and will be made aware of relevant procedures/requirements and of the limitations of their access.

e) Each out-of-hours access to the operational area of the facility must be recorded.

f) Internal areas requiring limited/controlled access must have a lock system.

Short-term and long-term evidence storage areas require limited/controlled access.

g) Each access device (keys, magnetic cards etc) must be uniquely identified and recorded in a register.

h) Policies and, where necessary, procedures, must be documented on the access allowed by customers or their representatives to the facility, facility records and exhibits. Examples may include access to relevant areas of the facility to witness tests/examinations, access either on-site or off-site to case records, provision of exhibits or samples for independent tests/examinations.

**Handling of test and calibration items**

The facility must have a documented evidence/sample control system.

Procedures for the receipt of evidence (or potential evidence) must ensure that wherever possible, items stored in the facility are properly sealed.

Photographic records (including video) or items taken from the scene(s) of investigation are considered to be evidence.

Each individual item of evidence must be marked with the unique case designator for identification. Should the item not lend itself to marking, its proximal container must be marked.

Labelling on caps/lids alone is not acceptable because of the risk of wrongly replacing lids during testing of batches of like samples.

## Sample/evidence integrity

The facilities procedures for maintaining the integrity of evidence or samples under its control must cover contamination issues and tamper proofing. The latter could be achieved by storing the item under tamper evident seal.

All evidence or samples must be sealed and identify the person sealing the evidence. The use of uniquely numbered seals is acceptable provided readily available supporting records detail the person sealing the evidence. Where tape is used to seal containers it must be initialled or otherwise identified. Heat sealed packages must have initials or other identification across the seal.

A container is properly sealed only if its contents cannot readily escape or become contaminated and only if entering the container results in obvious damage/alteration to the container or its seal. Compliance can be achieved in a variety of ways and the adequacy of each facility's procedures will need to be determined on a case by case basis. The use of tamper-evident tape may not be necessary if the critical factors are satisfied.

Sealing large exhibits may be impractical or inappropriate. Accordingly, facilities must adopt procedures to ensure that the feature or area of the item subject to examination is protected from loss, damage and contamination. For example, items could be secured in limited access rooms, garages etc. It may be also possible to 'seal' or protect by covering the section/part of the exhibit that is of interest.

Some forms of electronic evidence, depending on the nature of the investigation, may require both physical and electronic containment to ensure integrity is maintained.

It is not necessary for negatives, Polaroids etc. to be sealed. Appropriate security is achieved by storage in cabinets, cupboards etc which can be locked for overnight storage.

It is understood that facilities receive evidence from numerous sources making it difficult to ensure that all evidence submitted is properly sealed. Packaged evidence received by a facility which does not bear the identification of the person sealing the evidence container is not considered to be properly sealed.

An examiner in the process of examining evidence who needs to store it temporarily in a secure area need not seal the evidence each time it is stored.

Containers must be closed for overnight storage to protect evidence from accidental loss or contamination.

A chain of custody record (e.g. signature, date, time, description of evidence/sample) must be maintained which provides a comprehensive history of each evidence transfer over which the facility has control.

There is no requirement to keep a chain of custody record for negatives, Polaroids over and above the record of the name of the examiner(s) in the case record as these are not deemed to be primary exhibits.

## Sample/evidence storage

A secure area for overnight and/or long-term storage of evidence either physical or electronic must be available.

Proper security can be achieved by storing the evidence in locked cabinets, vaults, or rooms. If, during the process of examining evidence, an examiner needs to leave for a short time, such as for lunch, it is not necessary to pack up the evidence being examined if it is in a secure area (e.g. a limited-access laboratory room). This is also true for large and/or cumbersome items where it is advantageous to have the evidence remain out and there is controlled access to the area.

Items of evidence which are in the process of being examined may be left in examination areas overnight, providing the areas are adequately secured and staff with access to the areas are aware of the need to ensure that such items be protected from loss, damage or contamination.

Additional protective measures may be required for items being examined for trace evidence to minimise the possibility of loss or cross-transfer of evidence.

No special measures are required for 'sub-samples' which are defined as a portion taken from the original sample (or item) submitted to the facility for examination.

### Assuring the quality of test results - Case record review

A procedure must be available for the on-going technical and administrative review of case records. The procedure must include:

a) who may conduct each type of review;

b) the criteria to be used for each type of review;

c) the number/percentage of case reports to be reviewed;
   i) Technical reviews: the percentage of reviews undertaken could vary.
   ii) Administrative reviews: all or most case records must be reviewed to ensure completeness and compliance of the case file and the reporting criteria of the reports issued. It is acceptable for administrative and technical reviews to be performed as part of one review process.

d) a requirement that the reported conclusions fall within the range of acceptable opinions of knowledgeable individuals or are supported by sufficient scientific data;

e) the course(s) of action should a discrepancy be found.

Records of reviews conducted must be kept and include the identity of the reviewer and the date of the review. Use of initials or initialled signature is satisfactory provided the reviewer can be clearly identified.

It is important to note that a technical review, while important to the facility's quality assurance program, is not be carried out to the extent that it shifts the perceived responsibility for the scientific findings from the examiner to the reviewer as it is the examiner who presents sworn testimony regarding the findings.

### Court testimony monitoring

A facility may choose to use one or a combination of methods to perform the monitoring. Review of transcripts of testimony alone, however, is not sufficient since such reviews cannot address demeanour, appearance or conduct.

It is recognised that court appearance may be very infrequent. In these instances, court appearances must be monitored when ever possible. Monitoring of moot court participation may be considered.

The facility must have a documented procedure covering the monitoring of testimony of each analyst/examiner in each year testimony is given or when next in court.

The procedure must include:

a) who may conduct the evaluation;

b) the evaluation of the analyst's/examiners objectivity, appearance, poise, performance under cross-examination as well as effectiveness of presentation (e.g. technical knowledge, ability to convey scientific concepts in understandable terms);

c) the remedial action that is to be taken should the evaluation be less than satisfactory;

d) the need for timely feedback to the analyst/examiner.

A record must be kept of each evaluation including details of who conducted the evaluation and the date.

# 3. Further Information

Further information can be obtained by contacting Neil Shepherd, in our Melbourne office by telephone on 03 9274 8200 or email to neil.shepherd@nata.com.au

### References

ISO/IEC 17025 Field Application Document, Forensic Science. *Supplementary Requirements for Accreditation*.

**AMENDMENTS**

The table below provides a summary of changes made to the document with this issue.

| Section | Amendment |
|---|---|
| 2 | 'Security and Access' subsection added. |
| | |
| | |
| | |