General Accreditation Criteria

Legal management of facility activities (Forensic Operations Module)

Issue date: March 2019

Effective date: May 2019

Table of Contents

Legal management of facility activities

(Forensic Operations Module)

Introduction

This document provides interpretative criteria and recommendations applicable to facilities who may seek accreditation for the legal management of their activities (i.e. conformity assessment activities).

The criteria cover the need for having a system in place to ensure results and processes are able to withstand legal scrutiny and include:

- control of records - technical and administrative;
- security and access;
- sample/evidence integrity;
- assuring the quality of results - case record review;
- court testimony monitoring.

Accreditation against the criteria of the Forensic Operations Module (FOM) may provide greater reassurance in legal proceedings of the activities performed by facilities.

A facility may only seek accreditation for the FOM if it also holds accreditation in any of NATA's current programs. Accreditation against the FOM may cover a facility's entire scope of accreditation or only parts thereof as requested by the facility.

Applicant and accredited facilities must comply with all relevant documents in the NATA Accreditation Criteria (NAC) package applicable to their scope of accreditation (refer to *NATA Procedures for Accreditation).* The criteria detailed below are additional.

Applications for accreditation against the FOM criteria can be made by contacting your NATA Client Coordinator or a NATA office. For facilities already accredited, the request will be treated as a variation to scope of accreditation. For applicant facilities, the request will be treated as part of the formal application in the relevant NATA program. Refer to the *NATA Procedures for Accreditation* for further information.

Criteria

Control of records - technical and administrative

The records system must include all data and observations and any other analytical/examination or administrative records which support conclusions.

Notes: Examples of administrative records include case-related conversations which support or impact on the outcome, evidence receipts, description of evidence packaging and chain of custody seals, subpoenas and other pertinent information.

Examples of analytical/examination records would include reference to procedures followed, tests or examination (s) 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.

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

The facility must maintain all documentation for each given "case" in a specified location(s) under a unique designator, which could be in hardcopy or electronic form.

Note: A case is a compilation of documents and records applicable to a single event. Administrative and examination records, together with analytical documentation generated by a facility on a particular event, either on paper or electronically, constitutes a case record.

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

Note: Electronically-generated records satisfy the criteria if they include the printed unique identifier and the analyst/examiner/investigator's name or initials.

It must be clear from the case record:

- when each stage of the analysis/examination/investigation was performed (i.e. relevant date(s) and, where appropriate, the time(s));
- that all analysts/examiners/investigators and reviewers are identified.

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

Different mechanisms for record keeping must be considered where necessary, including:

- photography or electronic scanning (e.g. electrophoretic runs, physical matches, quantitation results);
- photocopying (e.g. thin-layer chromatography results, questioned documents).

The type of mechanism will need to be evaluated on a case-by-case basis. Case records are to support how opinions and interpretations were made.

Where instrumental analyses are conducted, operating parameters that deviate from the method must be recorded.

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).

Documented procedures must describe the storage of records if not stored in the case record (e.g. chromatograms),

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 the bag/envelope itself identified as part of the case record.

The requirement to identify the personnel and date all changes to original data 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

Procedures on facility security must be documented. This must include the access allowed to customers or their representatives to the facility, exhibits and facility records. 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.

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

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.

Access to the operational area of the facility must be controlled and limited. Area requiring limited/controlled access must have a lock system.

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

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 personnel who have a legitimate reason for requiring access to the operational areas of the facility (e.g. use of shared equipment, cleaners, contractors) 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. In such cases, 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.

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

Sample/evidence integrity

Electronically recorded evidence items (e.g. digital photographs) must not be subject to any processes that cause permanent alteration.

Identification/labelling of samples/evidence

Each individual item of evidence must be marked with unique 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.

Sealing of samples/evidence

The facility's procedures for maintaining the integrity of evidence or samples under its control must cover contamination issues and tamper proofing.

Procedures for the receipt of evidence must ensure that wherever possible, items stored in the facility are properly sealed and identify the person sealing the evidence.

It is understood that facilities receive evidence from numerous sources making it difficult to ensure that all evidence submitted is properly sealed. If the facility seals an exhibit following receipt there must be documented records of who sealed the evidence.

A container is properly sealed only if its contents cannot readily escape or become contaminated and only if opening the container will result 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 evidence of tampering can be determined.

If tape is used to seal containers it must be initialled or otherwise identified.

The use of uniquely numbered seals is acceptable provided readily available supporting records detail the person sealing the evidence.

Heat sealed packages must have initials or other identification across the seal.

Where the integrity of the evidence is potentially compromised (e.g. poorly sealed) this must be documented in the final report.

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.

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, deterioration and contamination.

Sample/evidence storage

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 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 facility 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, provided 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.

Assuring the quality of results - case record review

A procedure must be available for the ongoing technical and administrative review of case records. All cases must be both technically and administratively reviewed unless risk assessments have been completed for reducing the number/percentage of cases to review. It is acceptable for administrative and technical reviews to be performed as part of one review process.

Note: Administrative case record review is a procedure that checks the case file documentation to ensure that:

- the minimum set of elements are included within the file (electronically or in hardcopy);
- each element is correctly identified;
- laboratory policy has been followed.

Technical case record review is an examination of analysis records and test reports to ensure that:

- the proper procedures and protocols were followed;
- the results and conclusions/reports are valid and accurate.

The procedure must include:

- who may conduct each type of review;
- the criteria to be used for each type of review;
- the number/percentage of case records to be reviewed where this is not 100%;
- details that the reported conclusions fall within the range of acceptable opinions of knowledgeable or are supported by sufficient scientific data;
- 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 signature is satisfactory provided the reviewer can be clearly identified.

Any significant difference in the interpretation or opinions must be recorded.

It is important to note that a technical review, while important to the facility's quality assurance program, is not to 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

The facility must have a documented procedure covering the monitoring of testimony including:

- frequency of monitoring court testimony;
- who may conduct the evaluation;
- the evaluation of the analyst's/examiner's objectivity, appearance, poise, performance during examination as well as effectiveness of presentation (e.g. technical knowledge, ability to convey scientific concepts in understandable terms);
- the remedial action that is to be taken should the evaluation be less than satisfactory;
- the need for timely feedback to the analyst/examiner.

A facility may choose to use a combination of methods to perform the monitoring. This may include:

- review of transcripts;
- barrister feedback forms;
- formal moot court attendance.

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

Further information

Please contact Mr Andrew Griffin or Ms Gillian Treloar, in the NATA Melbourne office by telephone on 03 9274 8200 or email to Andrew.Griffin@nata.com.au or Gillian.Treloar@nata.com.au.

References

This section lists publications referenced in this document. The year of publication is not included as it is expected that only current versions of the references shall be used.

NATA publications

Relevant *NATA Accreditation Criteria (NAC)* package.

NATA Procedures for accreditation.

Amendment Table

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

Section or Clause	Amendment
Document title	Changed to Legal management of facility activities (Forensic Operations Module)
Whole document	Editorial amendments, including revised headings / subheadings. Deletions may reflect accreditation standards now covering the issue; the issue not aligned with contemporary practice; the issue not adding value. Additions may cover matters which are expected / implicit. Several additional notes have also been added to provide clarity.
Control of record - technical and administrative	<u>Deletions</u> • 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. • 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.
Sample/evidence integrity	<u>Deletions</u> • Photographic records (including video) or items taken from the scene(s) of investigation are considered to be evidence. • 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. • 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. <u>Addition</u> Electronically recorded evidence items (e.g. digital

	photographs) must not be subject to any processes that cause permanent alteration.
Court testimony monitoring	Additional examples provided, including: • barrister feedback forms; • formal moot court attendance.