Technical records

Introduction

The increased use of computers and computer systems in laboratories have led to an increased number of electronic records. There are a lot of advantage with electronic records, e.g. no need for a physical space for an archive, good posibilities to search for records, etc. Most laboratories have electronic records even though there are still a lot of physical records produced. However, a lot of laboratories do not exactly know how to handle electronic records. In the standard ISO/IEC 17025:2017 there are some requirements on how a laboratory should handle records in general and those requirements are of course valid also for electronic records.

Procedures for technical records

ISO/IEC 17025:2017 clause 7.5 *deals with all kind of technical records referred to each laboratory activities. Records are therefore not only referred to an analytical value but also to all the information and parameters that could affect results and/or activity repetition. This could include:*

- Environmental conditions
- Personnel name
- Date and time of activity
- Information about used instruments / tools
- Reagents and materials
- Calibrations
- Details of set up
- Conditions of test sample
- Sampling conditions
- Raw data
- …

ISO/IEC 17025:2017 requirements are of course valid for both handwritten and electronic records.
For handwritten records is necessary to maintain a clear and suitable set of documentation as the laboratory decides to implement in its Management System (Lab. log, Diary, Project note, …). This kind of paper documentation is usually stored in a project folder together with all other project documents (quotation, contract, report, …).
Besides raw data or measurements results, each kind of handwritten agreement / modification made on a document referred to a specific project can be considered “technical data”.
For electronic records, the requirement is fulfilled by having documented in the management system how the files are named, where the records are filed and stored (what server, networks, electronic folders etc.) and the personnel that have access to the storage places, both physically and electronically.
Electronic records are also mail messages containing information, agreements, decisions or any other kind of information related to the laboratory activity.

Under the above circumstances a “laboratory management system” has to be intended as the set of rules the laboratory define and implement for the management of information and technical data; “laboratory management system” has not to be intended as a computer program or application.
In order to keep records under control, a laboratory should develop set of templates for the electronic records it will produce and the templates should be protected against unintentional changes by the staff. A defined template, such as a check-list or a table with fixed fields, is

usually a good reminder in order to record all necessary information and minimize the possibility for the staff to make mistakes.

Storage of technical records

Technical records must be retained for a certain period of time, as defined by national legislation, accreditation rules, contractual agreements; this is usually a long-term period running from 3 to more than 10 years.
It’s therefore mandatory to implement specific measures in order to safely store data and prevent data loss.
Paper records are usually not influenced by long term retention time providing the environmental conditions in the storage area are adequate; temperature and humidity of the storage area might be evaluated and periodically checked.
Thermal printing (chemical paper) has a limited life-time running from few days to some weeks, mainly depending on ambient temperature or contact with chemical solvent (glue, adhesive tape). This kind of support cannot be stored “as is” and must be transferred to other kind of physical support (copy or scan) for long-term retention.
Electronic devices (e.g. memory sticks, hard disks, CDs) for data storage have limited life-time. When using cloud storage, specific agreements with the provider (e.g. lifetime, access, data security, transfer and integrity, confidentiality) are suggested. Use of this kind of electronic support only for short-term storage or transfer of data providing a dedicated means is implemented in order to guarantee data integrity/readability after transfer of data to other kind of support.
Proprietary data format, usually identified by a proprietary extension of files, is also an issue in case the original software / application / instrument is dismissed during the retention time and no other “data reader” or “data converter” is available.
Data stored on “data server” are usually safe, providing some basic IT principles are respected:

- the server used for the storage is placed in a facility to which there is limited physical and electronic access (locked room, fire wall and password),
- the climate is controlled,
- the requirements concerning prevention of damage or deterioration and to prevent loss are fulfilled,
- Backups are performed regularly on a different remote support (can be a remote server, a tape stored in a different building, a cloud server, …).

This should of course be described in a MS documentation. In addition, the question about fire protection and the need for burglary as well as fire alarms should be considered.

If the laboratory is using mobile devices for data recording it is recommended to regularly move the data to servers.

Retention time of electronic records
Another issue of importance is the format used to store the information. Due to the very fast technical development in the IT sector there is a risk that data stored in a specific format, e.g. a special format connected to a measurement programme, may be impossible to be read even before the retention time has expired. The best way to avoid such problems is to store the records in a format which is likely to survive during a long time, e.g. in text format or for recorded data in commercial formats. These formats will survive for a long time and if they disappear it will be well known beforehand and commercial solutions of the “retrieving problem” will be available. The laboratory might include in the MS the chosen solution (what format).

In the MS a reasonable retention time (according to national legislation, contractual agreements, accreditation rules, etc.) could also be decided and if and how the records shall be deleted/disposed of, or else what to do, when the retention time has expired.

Raw data

Handwritten raw data could be stored in the specific project folder, taking into account the provisions stated above for storage.
For the laboratory using electronic records this requirement is fulfilled by storing original observations (data taken from the analytical instruments) and/or derived data in digital format. Electronic record can also be a photograph or a movie; in this case the digital “metadata” could be saved together with the file, if available, or integrated by other means in such a way the record can be referred to the specific activity. A good way to store records connected to one project is to place them in an electronic folder.

There is no need to keep the information in its original format as long as you can access it during the retention time and ensure its integrity.

The calibration certificates for the equipment used and the staff records are usually not stored in the same electronic folder as the rest of the information concerning the assignment and it is therefore important to give reference to the equipment used and the staff that performed the assignment, preferably in the test report.

The time the records shall be retained depends on various aspects. There may be requirements from authorities to retain records for 30 years or for eternity. But in the normal case the retention time should be decided by the laboratory itself. The retention time is normally at least 3 years and in most cases 10 years.

Identification of data

The paragraph 7.5.1 requires that “technical records shall include the date and the identity of personnel responsible for each laboratory activity and for checking data and results. Original observations, data and calculations shall be recorded at the time they are made and shall be identifiable with the specific task.”. As said before by using the assignment’s/order’s identification, fulfils this requirement.

Amendments to technical records

While amendments of handwritten records are achieved by simply strikethrough the original text, write the new text with signature (of authorized personnel) and date, the same amendments of digital records may be difficult to handle for some sorts of electronic records.
For complete documents, the “revision” option available on many text editors or spreadsheets is one opportunity, providing the original file is maintained and both files have appropriate revision index.
Usually this kind of files are saved together with a set of data referred to the user and to the last saving or modification; these data are usually visible under a “file property” command.
In this case both a “public information” (revision index and date) and “private information” (file properties) are available to track back to the original information.
Some softwares, such as LIMS or mainframes applications, keep track of everything that is changed, when and who, but this kind of applications are not usually used for raw data.

Output from digital / automated instruments or measuring systems do not generally require amendments; in case a setup or a parameter was wrong during test execution, the test is repeated. In this case, it could be useful to take note about the mistake and save both files; it could be a hint for a preventive action.
The main issue is related to analytical values typed by the operator inside a file (spreadsheet or text editor). In this case, it is not possible to simply write the correct value and save again the file. The original data is completely lost forever!!!
One of the option is to:

- Copy and rename the original file in such a way to clearly identify the wrong file,
- Open the copy of the wrong file (the original copy is therefore prevented from a mistakenly “save” command),
- Strikethrough the original text, as per handwritten data, write the new text, and save the file,
- In most of the cases you can have a lot of possibilities to identify the amended data and the amendment’s executor: remarks on text files, highlights, colour text, notes, … but, of course, also other procedures can fulfil the requirement.