Technical records

Introduction

The increasing use of computers and computer systems in laboratories has led to an increased number of electronic records. There are a lot of advantages of 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 a lot of physical records are being kept. However, many laboratories do not know exactly how to handle electronic records. The standard ISO/IEC 17025:2017 has some requirements as to how a laboratory should generally handle record keeping, and of course these requirements also apply to electronic records.

Procedures for technical records

ISO/IEC 17025:2017 clause 7.5 *covers all kinds of technical records related to each laboratory activity. Records are therefore not only related to an analytical value, but also to all 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
- …

Of course, the requirements of ISO/IEC 17025:2017 apply to both handwritten and electronic records.
For handwritten records, it is necessary to maintain a clear and appropriate set of documentation that the laboratory decides to implement in its Management System (Lab. log, Diary, Project note, …). This type of paper documentation is usually stored in a project folder along with all other project documents (quotation, contract, report, …).
In addition to raw data or measurements results, any type of handwritten agreement/modification made in a document for a particular project may be considered "technical data".
For electronic records, the requirement is fulfilled by documenting in the management system how the files are named, where the records are filed and stored (which server, networks, electronic folders etc.), and the personnel having access to the storage locations, 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.

In the circumstances referred to above, a "laboratory management system" is to be understood as the set of rules that the laboratory defines and implements for the management of information and technical data; "laboratory management system" is not to be understood as a computer program or application.
In order to keep the records under control, a laboratory should develop a set of templates for the electronic records it is producing and protect the templates from inadvertent changes by the staff. A defined template, such as a check-list or a fixed-fields table, is usually a good

reminder to record all necessary information and minimize the possibility of staff making 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 a “data server” are usually safe, providing some basic IT principles are respected:

- the server used for storage is placed in a facility with limited physical and electronic access (locked room, firewall and password),
- the climate is controlled,
- the requirements for avoiding damage or deterioration and for preventing losses are fulfilled,
- Backups are regularly performed on a different remote support (may be a remote server, a tape stored in another building, a cloud server, …).

This should of course be described in an MS documentation. In addition, the issue of fire protection and the need for burglary and fire alarms should be considered.

If the laboratory uses 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 for storing the information. Due to the very rapid technical development in the IT sector, there is a risk that data stored in a specific format, e.g. a special format associated with a measurement programme, may even not be readable before the retention time has expired. The best way to avoid such problems is to store the records in a format that is likely to last for 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 in advance and commercial solutions to the “retrieval problem” will be available. The laboratory might include the chosen solution (which format) in the management system.

The management system could also establish a reasonable retention time (in accordance with national legislation, contractual agreements, accreditation rules, etc.) and whether and how records should be deleted/disposed of or what should be done if the retention time has expired.

Raw data

Handwritten raw data could be stored in the specific project folder, taking into account the above storage provisions.
For the laboratory that uses electronic records, this requirement is fulfilled by storing original observations (data taken from the analytical instruments) and/or derived data in digital format. An electronic record can also be a photo or a movie; in this case, the digital “metadata” could be saved together with the file, if available, or otherwise integrated, so that the record can be related to the specific activity. A good way to store records connected to a 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 on the assignment, and it is therefore important to refer to the equipment used and the staff that performed the assignment, preferably in the test report.

The retention time of the records to depends on various aspects. There may be requirements on the part of the authorities to retain records for 30 years or for eternity. Normally, however, the retention time should be determined by the laboratory itself. The retention time is usually at least 3 years and in most cases 10 years.

Identification of data

Paragraph 7.5.1 requires that “the technical records shall include the date and 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 already stated above, the use of the identification of the assignment/order fulfils this requirement.

Amendments to technical records

While amendments to handwritten records are achieved by simply strikethrough the original text, writing the new text with signature (by authorized personnel) and date, the same amendments to digital records may be difficult to handle for some types of electronic records.
For complete documents, the “revision” option, which is available for many text editors or spreadsheets, is an opportunity, provided the original file is maintained and both files have the appropriate revision index.
Typically, these types of files are stored along with a set of data related to the user and to the last save or modification; this data is usually visible under the “File Property” command.
In this case, both “public information” (revision index and date) and “private information” (file properties) are available to track back to the original information.

Some software, such as LIMS or mainframes applications, keep track of what was changed when and by whom, but this type of applications is not typically used for raw data.
The output of digital/automated instruments or measuring systems generally requires no amendments; in case a setup or a parameter was incorrect during the test execution, the test is repeated. In that case, it might be useful to take note of the mistake and save both files; it could be an indication of a preventive action.
The main issue relates to analytical values that are entered by the operator in a file (spreadsheet or text editor). In this case, it is not possible to simply write the correct value and save the file again. The original data is completely lost forever!!!
One of the option is to:

- copy and rename the original file to uniquely identify the wrong file,
- open the copy of the wrong file (the original copy is therefore protected from an erroneously “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 options to identify the amended data and the amendment’s executor: remarks on text files, highlighting, coloured text, notes, … but, of course, also other procedures can fulfil the requirement.