Shh it's a secret! Confidentiality in the lab

www.masmanagementsystems.com.au

We've all heard the expression knowledge is power. In the hands of cybercriminals, knowledge is also big business.

In a lab setting, it's understood that keeping information safe and secure is in the best interests of clients and your business. If you hold accreditation or certification, it's also a requirement of the standard.

ISO standards define confidentiality as 'the protection of information to ensure that data is accessible only to authorized personnel and is not made available or disclosed to unauthorized individuals, entities or processes'.

A breach of confidentiality can lead to, at a minimum, loss of customer confidence and loyalty but could also result in costly lawsuits.

Confidential information refers to all technical and non-technical information that a customer supplies to the lab. This can include procedures or methods shared by the customer, or their measurement results and reports. But it also includes things like contract documentation and any specifications provided to the lab.

What does ISO/IEC 17025 require?

The standard states that the laboratory 'must keep confidential all information obtained or created during the performance of laboratory activities, except as required by law'.

It's the responsibility of the lab to keep this information confidential. They should only use customer information for the purposes of communication or to assist in lab activities.

The lab's policies and procedures should reflect how this will happen. This includes procedures for protecting electronic storage and transmission of results.

Any information which is already known or available in the public domain can be disclosed without authorisation from the customer. However, if any additional information is to be made publicly available by the lab, they must inform the customer in advance.

If the lab obtains information about the customer from other sources, this shall also be kept confidential. The provider of this information does not need to be shared with the customer unless the source agrees.

The only alteration to this requirement is when a lab is directed to release information by a legal authority having appropriate jurisdiction. In this case, the lab must comply with this request and might not need to advise the customer in special circumstances of the law prohibiting disclosure to the customer.

Protection of information in the lab

The measures put in place must ensure that confidential information is well protected within the lab.

Keep paper documents and records in a secure location that can't be accessed by personnel who are not a part of your organisation. Shred confidential paper documents when they're no longer required.

Store electronic documentation on a secure network and only view them on secure devices. Share this information with other personnel only when necessary and if authorised. Think about this now that a lot of information is stored in the Cloud.

Confidentiality training

Make all lab personnel aware of the lab's confidentiality requirements and train them in the lab's policies and procedures.

Training in confidentiality should be part of the lab's induction process or completed within a reasonable timeframe once new staff begin working in the lab.

The approach to confidentiality is often a part of the culture of an organisation. If there is a culture of allowing "loose lips", then you could be in danger of breaching any confidentiality policy. Remember those loose lips sink ships!

A good idea is to restate and remind staff of these policies and procedures in regular staff meetings and in annual management reviews. Encourage employees to ask questions about the policies and raise scenarios for clarification if required.

The ISO/IEC 17025 standard states that the lab is responsible through legally enforceable commitments for confidentially managing the information it obtains. For this reason, labs could also have personnel sign a formal confidentiality or non-disclosure agreement.

This is standard practice for many businesses and can remain in effect indefinitely, protecting the lab even after personnel leave.

Other issues to consider

Printing: you may have a procedure in place for filing and securing documents.

But we've all had that moment when you printed a document, got distracted, and hit the print button again. If your printer is in a busy area, this could lead to an inadvertent breach of confidentiality. Check before you print or consider using password protected printing options.

Mobile phones: all smartphones have the capacity to take photos and video.

While this is useful for those Instagram moments, in a lab setting it could lead to a serious breach.

Labs must consider how they will manage the use of mobile phones by staff and visitors. Banning phones could be unreasonable but regular reminders about appropriate use is an important step.

Computer training: when assessing lab staff competency, employers may look primarily at their technical abilities.

Providing staff training on lab specific software will help mitigate instances of accidental deletion or corruption of information. Assessing their abilities on email and document creation software would also be useful.

Support when you need it

As we always say, you don't have to do this alone! You can call Maree on 0411 540 709, email info@masmanagementsystems.com.au or head to the Contact Us page on our website.

If you're looking for legal advice, our friends at Law Law can provide counsel and support with any matters relating to your lab. Email info@lablaw.com.au and of course, all discussions will be completely confidential.

Remember you don't have to do this alone!