Why ISO/IEC 27001 for healthcare?
An organization stores information digitally, on paper and as employee knowledge. Secure information is an important factor when it comes to patient safety in healthcare institutions. Patient journals and data such as laboratory reports are sensitive and should only be accessed and used by those with correct authorisation. Also, timely access to updated information is crucial for medical personnel in order to maintain safety and ensure correct medical treatment based on correct data. Failing to provide necessary patient or medical information can, in worst case, result in lives lost. IT systems are necessary to store and access patient data, as well as conduct medical research. An efficient management system will help you to ensure both data and patient safety.

ISO/IEC 27001 is an internationally acknowledged management system standard for information security. By implementing an information security management system compliant with ISO/IEC 27001 you ensure that your organization identifies and mitigates the risks related to handling sensitive and vital data. A certified management system is compliant with applicable national legislation and international best practice. Certification assures patients, authorities and other stakeholders that you are handling all relevant information security aspects.

How ISO/IEC 27001 certification supports your organization
A certified information security management system demonstrates commitment to the protection of information and provides confidence that assets are suitably protected - whether held on paper, digitally, or as employee knowledge.
Such systems take a systematic approach to minimising risk and ensure compliance with legal and other requirements. More specifically, it helps you to:

- Control, manage and correctly handle the information that your organization possesses.
- Take an active approach to data management and to securing vital information.
- Identify and mitigate risk related to handling of information.
- Comply with relevant national and international legislation.
- Ensure continuity of operations in case of information security incidents.
- Provide assurance to patients, authorities and other stakeholders that sensitive information is safe.

**How do I get started?**
These are important steps to get started:

- Get familiarised with the ISO/IEC 27001 standard. Training programs are available, and the standard can be acquired on iso.org.
- Identify all applicable legal requirements that you must comply with.
- Get an overview of the information assets in your organization.
- Make a risk assessment to identify and understand the risks to your organization’s data. Third party pre-assessments may prove valuable in an early phase of the implementation.
- Prioritise the risks and choose actions to be implemented to mitigate risk and ensure an acceptable risk level.
- Ensure top management commitment. Effective implementation of a management system requires commitment from top level through to the entire organization.
- Engage an accredited certification body, such as DNV GL, to get started with the certification process.

Certification and continuous improvement of your management system is a journey. As your third party certification body, DNV GL will perform yearly audits and re-certification every third year. Additionally you will need to conduct internal audits and management reviews in order to develop the management system in line with a changing risk landscape.

**Risk Based Certification™ - tailored to your needs**
DNV GL applies our Risk Based Certification methodology to provide more value to your organisation through focused audits. We start by asking you to identify the most significant risks to your information security. In addition to measuring against the selected standard, we tailor the audit to address the identified risks. This is vital in helping you pinpoint key improvement areas, and allows you to focus on the areas that are most important to you. We tailor both the certification audits and the yearly audits. We help you improve in your focus areas, and will customise the audits as your risk landscape changes.

**Training and other related services**
Knowledge fosters an organization’s ability to embed standards and create lasting cultural change. Our goal is to help you to engage your organization in a process that supports continuous learning and improvement at every level.

We deliver trainings in your local markets that are tailor made for the healthcare sector. Courses include introduction to ISO/IEC 27001, internal auditor trainings, management review trainings and risk management. Contact your local DNV GL office to get an overview of what we can offer you locally. We can also support you with pre-assessments of your management system before certification in order to identify risks, gaps and areas that need improvement in order to comply with the standard.

**Why partner with DNV GL?**
As a world-leading certification body with objectives to safeguard life, property and the environment, DNV GL is committed to support healthcare organizations improve patient safety. With operations in over 100 countries, we are uniquely positioned to serve the needs of the global healthcare community, having certified or accredited close to 2,400 healthcare organizations internationally.

DNV GL works with national healthcare authorities and healthcare providers around the world to effectively manage risk and improve healthcare delivery. Our healthcare activities are supported by a multidisciplinary research group based in Oslo that is committed to improving patient safety through collaborative research.

DNV GL’s team of healthcare and risk management specialist has an innovative, advanced approach to help healthcare providers globally achieve excellence by improving quality and patient safety through hospital accreditation, managing infection risk, management system certification and training.

* *Risk Based Certification is a registered EU trademark of DNV GL AS.*

Contact us:
business.assurance@dnvgl.com
www.dnvgl.com/healthcare