bsi.

ISO 27799
Information security management in healthcare

ISO 27799:2016 serves as a tool to protect personal health information and is a companion to International Standard ISO/IEC 27002, and defines guidelines to support the interpretation and implementation in health informatics. This standard provides guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

Benefits of adoption

Certification to ISO 27799 will demonstrate your commitment to protecting personal health information with the added potential benefits of:

- Effective implementation of Information Security Management System in healthcare industry
- In-depth understanding of information security controls and their relationships with each other i.e. responsibilities, strategies, acquisition, efficiency and general human relations.

- Improved skills for the better management and proper usage of ISO 27799 in healthcare industry.
- Gaining the competency skills to perform risk assessment in healthcare organization.
- Enhanced protection of patient's personal and confidential data.

Business issue	How ISO/IEC 27799 can help	Benefit to your organization
Reputation	• Helps you identify risks to your information and put in place measures to manage or reduce them • Helps you put in place procedures to enable prompt detection of information security breaches • Requires you to continually improve your Information Security Management System (ISMS)	• Improved reputation and stakeholder confidence • Better visibility of risk amongst interested parties • Builds trust and credibility in the market to help you win more business
Engagement	• Requires you to identify all internal and external stakeholders relevant to your Management System ISMS • Requires you to communicate the ISMS policy to and ensure that the workforce understands how they contribute to it • Top management need to define ISMS roles and ensure individuals are competent	• Improved information security awareness amongst all relevant parties • Reduces likelihood of staff-related information security breaches • Shows commitment to information security at all levels of the business

Business issue	How ISO/IEC 27799 can help	Benefit to your organization
Compliance	• Gives you a framework which helps you to manage your legal and regulatory requirements • Makes you review and communicate your regulatory requirements to other interested parties	• Reduces the likelihood of fines or prosecution • Helps you comply with relevant legislation and helps make sure you keep up-to-date
Risk management	• It makes you assess risks to information security so you can identify potential weaknesses and respond • Requires you to put in place controls that are proportionate to the risks • Requires you to continually evaluate risks to your information security and make sure the controls you put in place are appropriate	• Helps you protect your information so you can continue business as usual and minimize disruptions • Gives cost savings by minimizing incidents • Ensures information is protected, available, and can be accessed

Who needs ISO 27799?

Hospitals, healthcare consumer app/software developers, healthcare IT/Cloud providers, HIMMS (Consortiums), Research/academia, cybersecurity partners/firms, healthcare information security partners, medical device/pharma manufacturers, technology companies.

Why BSI?

• BSI is committed to a secure digital world and helps build information resilience in organizations worldwide. With the ever-changing landscape for the healthcare industry, from technological advancements, digitization and complex regulations, BSI can help organizations to adapt and embrace these changes.

• As a Royal Charter, independent, non-profit distributing organization, we're able to re-invest 100% of our profit back into our company. One of the key assets we invest in is our people. Our passion, expertise, integrity, inclusive nature and commitment to continual improvement set BSI apart.

• Established in 1901, BSI is a world-leading national standards body that helps our clients operate in a way that is safer, more secure and more sustainable. Our unique combination of consulting, knowledge, assurance and regulatory services makes organizations more resilient, and in turn inspires trust in their products, systems, services, and the world we live in.

• We help the organizations we work with become stronger, more resilient, more sustainable and ultimately more trusted.

Hear what our clients are saying

"ISO 27799 certification is the fruit of HUAWEI CLOUD's in-depth understanding of healthcare digitization and accumulation of patient privacy protection technologies. It is also an important exploration of HUAWEI CLOUD's advanced security technologies for protecting information security in the healthcare industry."

Zhang Yuxin, Chief Technology Officer of HUAWEI CLOUD

"We chose to pursue these ISO standards because of the importance of providing secure healthcare solutions while adhering to the highest industry security standards. Our mission is patient safety, and we see security as part of that mission."

Robert Mehler, Co-Founder, Chief Operating Officer, and Chief Information Security Officer, MaxQ AI

For more information:
bsigroup.com/healthcare