Chapter IV
Implementation of Information Security Management System (ISMS)

INTRODUCTION

Fundamental to ISO 27000 (ISO/IEC 27001:2005, 2005) is the concept of an information security management system (ISMS). The information security management system (ISMS) is the part of the overall management system, which is based on a business risk approach, to establish, implement, operate, monitor, maintain, and improve information security. The management system includes organization, structure and policies, planning activities, responsibilities, practices, procedures, processes, and resources. For the management of information security, its scope, administration and resources will depend on the size of the healthcare organization and information resources in question. The ISMS should be effective if it is to be useful to the organization. Information security should be an integral part of the healthcare organization's operating and business culture. Information security is primarily a management issue, rather than a technical issue, although one should not ignore the technical problems especially given the widespread dependence on the use of IT. Information security management is not a one-off exercise, but should be seen as an ongoing activity of continual improvement. Well-managed
information security is a business enabler. No organization can operate successfully in today’s world without information security. A well chosen management system of controls for information security, properly implemented and used, will make a positive contribution to the success of the healthcare organization, not just a cost against the bottom line.

IMPLEMENTATION OF ISO 27000 IN PACS

Implementation of ISO 27000 (Calder, 2006) (ISO/IEC 27001:2005, 2005) using the Plan-Do-Check-Act (PDCA) model, provides an approach to developing, implementing and improving the effectiveness of an healthcare organization’s ISMS. Details are discussed in the following sections.

Plan Phase

a. Study the benefits and merits of the standard to the healthcare organization, hospital, medical centre, or clinic. It should include the quality and quality management improvements, legal, and regulatory compliance, and customer satisfactory.

b. A decision should be made by hospital management to implement the standard

c. Allocation of resources in terms of money, people and time

d. Define the scope of the ISMS in terms of the characteristics of the healthcare business, the organization, its location, assets and technology. The scope of the ISMS may be a limited part of the healthcare organization and independently defined, or the scope may be defined to be the whole organization. The ISMS scope needs to be well defined and complete. The scope needs to take into account of the interfaces with other systems, organizations, third party suppliers, and it also needs to take into account of any dependencies, e.g. security requirements that need to be satisfied by the ISMS.

e. Define a ISMS policy in terms of the characteristics of the healthcare business, the organization, its location, assets, technology and take into account of any legal and regulatory requirements, and contractual or third party obligations or dependencies. The ISMS policy has to be approved by management. This policy shall include a framework for setting objectives, giving management direction and action, establishing the risk management context and criteria against which risk will be evaluated.

f. Define a systematic approach to risk assessment this should be an approach that is best suited to the ISMS. The healthcare organization needs to include
16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/chapter/implement...security-management-system/19322?camid=4v1

This title is available in InfoSci-Books, InfoSci-Medical, Healthcare, and Life Sciences, Business-Technology-Solution, Communications, Social Science, and Healthcare, InfoSci-Select, InfoSci-Select. Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

Operationalizing the Science
www.igi-global.com/chapter/operationalizing-science/53670?camid=4v1a

Socio-Technical Structures, 4Ps and Hodges' Model
www.igi-global.com/chapter/socio-technical-structures-4ps-hodges/27329?camid=4v1a

GIS Application of Healthcare Data for Advancing Epidemiological Studies
www.igi-global.com/chapter/gis-application-healthcare-data-advancing/55154?camid=4v1a
Integrating Telehealth into the Organization’s Work System
www.igi-global.com/chapter/integrating-telehealth-into-organization-work/53692?camid=4v1a