Abstract

Introduction

Increasing usefulness of health information systems has resulted in implementation of a number of systems during the past decade. As a result, a lot of sensitive information have been stored in digital form within these systems. In an era where most of the information communication is happening via the Internet, securing integrity and confidentiality of information while preserving the availability of information is indeed challenging. Assessing level of security and establishing sound information security protocols can prepare health organizations to confront security breach incidents.

Methods

Information system administrators play an important role in management of information security. This study has assessed the knowledge and practices of the system administrators in selected state sector health institutes. A comprehensive literature review was carried out to identify the guidelines, standards, policies and frameworks in Sri Lanka and other countries. The assessment was performed using mixed methods with a self-administered questionnaire and a key informant interview as study instruments. The information systems implemented in the selected institutes were enlisted. Security practices and the knowledge of system administrators were assessed by the questionnaire while the perception of the participants on overall information security of their institutes was assessed in the interviews. Descriptive analysis of the questionnaire and thematic analysis of the interview data was used for the data analysis.

Results

Questionnaire was responded by 19 participants from distinct institutes and 15 of them participated in key informant interviews. Majority of health institutes were found to have implemented more than 50 percent of the information security practices assessed by the questionnaire while only 3 institutes had implemented more than 75 percent of the measures. Most of the participants claimed that the level of information security of their institutes is either low or moderate. Challenges related to human factors were commonly faced by the participants while implementing information security measures. Awareness and training and allocation of adequate budget were mutual suggestions of the participants to enhance the quality of information security.

Conclusion

Novel solutions are being implemented worldwide to mitigate the risk of information security. Current practices in the selected state health sector institutes of Sri Lanka, in information security may not be adequate to confront information security threats in health industry. Nevertheless, assessment of information security risks, rectifying the practices by adhering to the guidelines, updating guidelines, standards and policies could ensure health information security in Sri Lanka and facilitate a trustworthy health care delivery.