

STATEMENT:

Security Risk Assessments will be conducted on a regular and on-going basis. The objective of the Security Risk Assessment is to identify and prioritize assets of the Healthcare Facilities (HCFs) primary mission and operations, identify threats to and vulnerabilities of those assets, and develop reasonable risk mitigation strategies to protect the assets.

INTENT:

- a. Security risk assessments should be conducted by a qualified professional who has training and experience in healthcare security.
- b. The HCF should identify assets by broad categories, such as:
 - 1) People assets to include employees, patients, visitors, family, and non- employed support personnel
 - 2) Property assets both physical and tangible such as buildings, equipment, medical gases, medical equipment, utilities and cash, as well as intangible assets, business records, information assets and the organization's reputation.
- c. The HCF should prioritize assets based on those that are mission critical to the organization.
- d. An inventory of identified risks and mitigations that may include policies, procedures, practices, physical/electronic security equipment, systems, and security personnel.
- e. The inventory process should include a review of all available security documentation such as security plans, security officer deployment, training, and post orders.
- f. The inventory may be accomplished using:
 - 1) An outside-in approach (begin at the perimeter and work toward the identified critical assets through each line of defense)
 - 2) An inside-out approach (begin at each critical asset and work out to the perimeter)
- g. Threats should be identified, assessed and trended quantitatively and qualitatively related to the prioritized list of the HCFs identified assets. Meaningful data should be gathered from several sources, including:
 - 1) Internal data from security incidents, facility statistics, and staff interviews
 - 2) Local police crime statistics
 - 3) IAHSS Healthcare Security Design and Basic Guidelines
 - 4) Exchange of information with similar organizations
 - 5) Other security and law enforcement sources
 - 6) Industry publications and news clipping sources

- h. Consider improvements of the organization’s protection of assets in light of the threats to and vulnerabilities identified to determine security enhancements needed to mitigate risks. A cost-benefit analysis of options may be needed to select appropriate measures that reduce risk to an acceptable level and comply with applicable healthcare industry standards, guidelines, and regulatory agency requirements.
- i. Results of formal risk assessments should be documented for on-going review and forwarded to appropriate leadership.

REFERENCES:

- Colling, Russell L. and York, Tony W. (2010). *Hospital and Healthcare Security*. Woburn: Butterworth-Heinemann.
- Vellani, Karim H. (2007). *Strategic Security Management: A Risk Assessment Guide for Decision Makers*. Woburn: Butterworth-Heinemann.
- “Risk Assessment Toolkit CD”, (November 2012), IAHSS.
- “Healthcare Security Industry Guidelines”, (2014), IAHSS
- “Security Design Guidelines for Healthcare Facilities”, (March 2012), IAHSS

Approved: April 2009

Last Revised: January 2015