TITLE Information Risk Management			**IDENTIFICATION NUMBER** A13-065
ORGANIZATION(S) University of Kentucky / UK HealthCare	**SITES AFFECTED** X Enterprise ☐ Chandler ☐ Good Samaritan ☐ KCH ☐ Ambulatory	**CATEGORY** X Enterprise ☐ Nursing ☐ Department ☐ Guideline ☐ Protocol	**REPLACES:**
REVIEW CYCLE ☐ 1 year X 3 years **REVIEW DATES:** 12/18/2012; 6/8/2015; 8/19/2019; 7/18/2022		**EFFECTIVE DATE:** 8/15/2022	

POLICY STATEMENT

UK HealthCare is committed to the total process of identifying, managing, and minimizing information system related risks to a level commensurate with the value of the assets protected. The goal of UK HealthCare's Information Risk Management Program is to protect the organization and its ability to perform its mission and maintain compliance with relevant laws.

PURPOSE

The purpose of this policy is to define UK HealthCare's information risk management approach.

SCOPE

Information risk management adapts the generic process of risk management and applies it to the confidentiality, integrity, and availability of information and information systems. An effective information risk management process is an important component of a successful information security program. Risk cannot be eliminated entirely. The risk management process allows UK HealthCare to balance the operational and economic costs of protective measures and achieve gains in mission capability.

PROCEDURES

Methodology

UK HealthCare has adopted appropriate industry best practices, frameworks, and guidance for its information risk management program. These include, but are not limited to:

1. ISO/IEC Guide 73 Risk Management Vocabulary
2. ISO/IEC 27005 Information Security Risk Management
3. ISO/IEC 31000 Risk Management – Principles and Guidelines on Implementation
4. ISO/IEC 31010 Risk Management – Risk Assessment Techniques
5. NIST SP 800-30 Risk Management Guide for Information Technology Systems
6. NIST SP 800-39 Managing Information Security Risk

Risk Management Process

The information risk management process is a continuous improvement process that consists of context establishment, risk assessment, risk treatment, risk communication, risk monitoring and review.

1. **Context Establishment** is the strategic, organizational and risk management context in which the rest of the process takes place. At this phase, the criteria for risk evaluation are established and the structure of the analysis is defined.
2. **Risk Assessment** is composed of risk identification, risk analysis, and risk evaluation.
    a) Risk Identification is the process of identifying sources of risk, areas of impact, events and their causes, and their potential consequences.
    b) Risk Analysis is the determination of existing controls and analysis of risks in terms of consequence and likelihood in the context of those controls. The analysis considers the range of potential consequences and how likely those consequences are to occur. Consequence and likelihood are combined to produce an estimated level of risk.
    c) Risk Evaluation compares estimated levels of risk against the pre-established criteria. This enables risks to be ranked so as to identify management priorities. If the levels of risk established are low, then risks may fall into an acceptable category and treatment may not be required.
3. **Risk Treatment** is the development of a comprehensive strategy to treat identified risks. Risk treatment applies appropriate controls that:
    a) Reduce risks by knowingly and objectively accepting risks.
    b) Avoid risks by not allowing actions that cause risk occurrence.
    c) Transfers associated risks to third parties.
4. **Risk Communication** involves consulting with internal and external stakeholders (when appropriate) during each stage of the risk management process. Risk communication enables UK HealthCare to minimize losses and capitalize on opportunities.
5. **Risk Monitor and Review** is the process of reviewing and updating the effectiveness of risk assessment and treatment. It incorporates significant change to the information system or environment of operations, or other conditions that may impact the security state of the system. It allows for the identification of emerging changes, trends, or risks.

APPROVAL

NAME AND CREDENTIALS: Douglas Fee **TITLE:** Chief Information Security Officer	**NAME AND CREDENTIALS:** Cecilia Page **TITLE:** Chief Information Officer
SIGNATURE	**DATE**
SIGNATURE	**DATE**