LSU - HEALTH CARE SERVICES DIVISION
BATON ROUGE, LA
INFORMATION SECURITY RISK MANAGEMENT PROGRAM

POLICY NUMBER: 7702-23

CATEGORY: Information Security

CONTENT: Information Security Risk Management Program

APPLICABILITY: This policy applies to all employees of the HCSD headquarters and Lallie Kemp Medical Center (LKMC) including classified employees, unclassified employees, students, contractors and agents of HCSD and LKMC.

EFFECTIVE DATE: April 3, 2015
Revised: January 8, 2019
Revised: February 22, 2023

INQUIRIES TO:

Information Technology
LSU Health Care Services Division
PO Box 91308
Baton Rouge, LA 70821 1308

Note: Approval signatures/titles are on the last page

LSU - HEALTH CARE SERVICES DIVISION
INFORMATION SECURITY RISK MANAGEMENT PROGRAM

I. PURPOSE

This policy establishes the scope, objectives, and procedure of LSU HCSD information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

II. SCOPE

The scope of the information security risk management process covers the administrative, physical, and technical processes that enable and govern ePHI that is received, created, maintained or transmitted

III. DEFINITIONS

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

LSU HCSD HIPAA Security Committee - Individuals who are knowledgeable about the organization's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and procedures outlined below. This team is generally comprised of the Information Security Officer, Compliance and Privacy Officer, Chief Information Officer, Systems Analyst(s), and Security/Technology subject matter experts. Other individuals such as the Physical Plant Security Officer or designee may be included in the team on an as needed basis.

Non-Disclosure Agreement (NDA) - A legally binding contract that establishes a confidential relationship.

Risk - The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets.

Risk Analysis - (Referred to as Risk Analysis in the HIPAA Security Rule); the process:

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place; Prioritizes risks; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.

Risk Management: This policy refers to two major process components: risk analysis and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

Risk Mitigation: Referred to as *Risk Management* in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

Systems and Organizations Controls 2 (SOC 2): Sometime referred to as SOC II, refers to the American Institute of Certified Public Accountants' (AICPA) SOC 2 framework, designed to help software vendors and other companies demonstrate the security controls used to protect customer data in the cloud, and the framework controls, including security, availability, processing integrity, confidentiality, and privacy.

Threat: the potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:

- Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
- Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
- Natural – fires, floods, electrical storms, tornados, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
- Other – explosions, medical emergencies, misuse or resources, etc.

Threat Source – Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the organization's ability to protect ePHI.

Threat Event – The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

IV. POLICY

A. It is the policy of LSU HCSD Information Technology to conduct thorough and timely risk analysis of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its electronic protected health

information (ePHI) (and other confidential and proprietary electronic information) and to develop strategies to efficiently and effectively mitigate the risks identified in the analysis process as an integral part of the organization's information security program.

B. Risk analysis and risk management are recognized as important components of LSU HCSD's corporate compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).

1. Risk analyses are done throughout IT system life cycles:

    a. While integrating technology and making physical security changes; and,
    b. While sustaining and monitoring of appropriate security controls.

2. LSU HCSD Information Technology performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI.

C. LSU HCSD Information Systems implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

1. Ensure the confidentiality, integrity, and availability of all ePHI the organization creates, receives, maintains, and/or transmits,
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI,
3. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required, and
4. Ensure compliance by workforce.

D. Any risk remaining (residual) after other risk controls have been applied, requires sign off by the senior management, the LSU HCSD HIPAA Security Committee, and, as appropriate, department managers.

E. All LSU HCSD workforce members are expected to fully cooperate with all persons charged with doing risk management work. Any workforce member that violates this policy will be subject to disciplinary action up to and including termination based on the severity of the violation.

F. All risk analysis efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.

V. PROCEDURES

A. The implementation, execution, and maintenance of the information security risk analysis and risk management process for LSU HCSD are the responsibility of the HCSD IT Security Officer and for individual facilities it is the local facility I.T. Security Officer. The Security officer will work in conjunction with the identified LSU HCSD HIPAA Security Committee.

B. **Risk Analysis:** The intent of completing a risk analysis is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

1. Step 1. System Characterization

a. The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media). LSU HCSD has developed an inventory database for tracking all systems, applications, portable devices, and hardware/software that create, maintain, process or transmit ePHI.

b. *Output* – Characterization of the IT system assessed a good picture of the IT system environment, and delineation of system boundaries.

2. Step 2. Threat Identification

In this step, potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. Consider all potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats. The list should be based on the individual organization and its processing environment. *Output* – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

3. Step 3. Vulnerability Identification

a. The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network. \

b. *Output* – A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources.

4. Step 4. Control Analysis

a. The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat-source exploiting a system vulnerability.

b. For cloud hosted applications containing ePHI per Step 1. System Characterization, and if a more appropriate compliance audit has not been completed by the cloud hosting vendor, a SOC 2 report will be collected by the LSU HCSD HIPAA Security Committee. If an NDA is required by the vendor to obtain a copy of the SOC 2 report the LSU HCSD HIPAA Security Committee will be responsible for working with legal and leadership to execute an NDA to obtain a copy of the SOC 2 report. This SOC 2 report will be reviewed, and findings incorporated into the output of this step.

c. *Output* – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.

5. Step 5. Likelihood Determination

a. The goal of this step is to determine the overall likelihood rating that indicates the probability that vulnerability could be exploited by a threat-source given the existing or planned security controls.

b. *Output* – Likelihood rating of low, medium, or high

6. Step 6. Impact Analysis

a. The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting vulnerability. Factors of the data and systems to consider should include the importance to the organization's mission; sensitivity

and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.

b. Output – Magnitude of impact rating of low, medium, or high.

7. Step 7. Risk Determination.

a. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management (the mission owners) must take for each risk level.

b. *Output* – Risk level of low, medium, high.

8. Step 8. Control Recommendations

a. The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

b. *Output* – Recommendation of control(s) and alternative solutions to mitigate risk.

9. Step 9. Results Documentation

a. Results of the risk analysis are documented in an official report or briefing and provided to senior management (the mission owners) to make decisions on policy, procedure, budget, and system operational and management changes.

b. *Output* – A risk analysis report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

C. Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk analysis to ensure the confidentiality, integrity, and availability of ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

1. Step 1. Prioritize Actions –

a. Using results from Step 7 of the Risk Analysis, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources.

b. *Output* – Actions ranked from high to low

2. **Step 2. Evaluate Recommended Control Options** –

a. Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Analysis, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a "most appropriate" control option for each threat and vulnerability pair.

b. *Output* – list of feasible controls

3. **Step 3. As Applicable, Conduct Cost-Benefit Analysis** –

a. Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process. Subject matter experts may be included in these processes.

b. *Output* – Documented cost- benefit analysis of either implementing or not implementing each specific control

4. **Step 4. Select Control(s)** –

a. Taking into account the information and results from previous steps, the LSU HCSD's mission, and other important criteria, the LSU HCSD HIPAA Security Committee determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.

b. *Output* – Selected control(s)

5. **Step 5. Assign Responsibility –**

a. Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous

step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.

b. *Output* – List of resources, responsible persons and their assignments.

6. Step 6. Develop Safeguard Implementation Plan –

a. Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:

i. Each risk or vulnerability/threat pair and risk level
ii. Prioritized actions
iii. The recommended feasible control(s) for each identified risk
iv. Required resources for implementation of selected controls
v. Team member responsible for implementation of each control
vi. Start date for implementation
vii. Target date for completion of implementation
viii. Maintenance requirements.

b. The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to the organization's executive management/leadership team (e.g. the Board, senior management, and other key stakeholders).

c. Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations (often referred to as a work breakdown structure). Additionally, consider including items in individual project plans such as a project scope, a list of deliverables, key assumptions, objectives, task completion dates and project requirements.

d. *Output* – Safeguard Implementation Plan

7. **Step 7. Implement Selected Controls** – as controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical.

Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.

a. Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.
b. Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.
d. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.
e. *Output* – Residual Risk

D. Risk Management Schedule: The two principal components of the risk management process - risk analysis and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of LSU HCSD's information security program:

1. Scheduled Basis – an overall risk analysis of LSU HCSD's information system infrastructure will be conducted every two years. The analysis process should be completed in a timely fashion so that risk mitigation strategies can be brought to Executive Staff for consideration.

2. As Needed – the Security Officer (or other designated employee) or LSU HCSD HIPAA Security Committee call for a full or partial risk analysis in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect LSU HCSD information systems.

E. Process Documentation. Maintain documentation of all risk analysis, risk management, and risk mitigation efforts for a minimum of six years.

Applicable Standards/Regulations:

- 45 CFR 164.308(a)(1)(ii)(A) – HIPAA Security Rule Risk Analysis
- 45 CFR 164.308(a)(1)(ii)(B) – HIPAA Security Rule Risk Management
- 45 CFR 164.308(a)(8) – HIPAA Security Rule Evaluation

Sources:

- HIPAA Collaborative of Wisconsin ("HIPAA COW") Risk Management Policy, January 2013.

Document Metadata

Document Name:	7702-23 - Information Security Risk Management Program.docx
Policy Number:	7702
Original Location:	/LSU Health/HCSD/7700 - Information Security
Created on:	04/03/2015
Published on:	02/22/2023
Last Review on:	02/14/2023
Next Review on:	02/14/2024
Effective on:	07/01/2019
Creator:	Kees, James "Mickey" *HCSD Chief Information Officer*
Committee / Policy Team:	Main Policy Team
Owner/SME:	Kees, James "Mickey" *HCSD Chief Information Officer*
Manager:	Kees, James "Mickey" *HCSD Chief Information Officer*
Author(s):	Wicker, Claire M. *PROJECT COORDINATOR*
Approver(s):	Wilbright, Wayne *Chief Medical Informatics Officer* Kees, James "Mickey" *HCSD Chief Information Officer*
Publisher:	Wicker, Claire M. *PROJECT COORDINATOR*

Digital Signatures:

Currently Signed

Approver:
Kees, James "Mickey"
HCSD Chief Information Officer

02/17/2023

Approver:
Wilbright, Wayne
Chief Medical Informatics Officer

02/22/2023