Risk Assessment and Management Policy

Policy 13	POL-RM	Effective Date	MM/DD/YYYY	Review Date	MM/DD/YYY	Version	1.0

Table of Contents

I. Purpose 1
II. Scope 1
III. Policy 1
IV. Procedures 2
V. Risk Based Controls 4
Risk Assessment Policy and Procedures (RA-1 C) 4
Risk Assessment (RA-3 C) 4
Vulnerability Scanning (RA-5 C) 4
Plan of Action and Milestones Process (PM-4 C) 5
Risk Management Strategy (PM-9 C) 5
VI. Cross References 5
VII. Policy Referencescybersecur 5
VIII. Interpretation, Implementation and Revision 6
IX. Approval and Ownership 7
X. Revision History 7

I. PURPOSE

The University of Chicago Medical Center and the Biological Sciences Division of The University of Chicago (the "**Organizations**") protects information that is the subject of legal, contractual, or enterprise confidentiality and security requirements (collectively the "**Security Obligations**"); such information is called "**Protected Information.**" This policy ensures that the Organizations conduct risk assessments to organizational operations, assets, and individuals resulting from the operation of Organizations' Information Systems and its associated processing, storage or transmission of the Organizations' information. This policy also ensures that identified risks are managed according to the Organizations' expectations.

II. SCOPE

This policy applies to the Organizations' (i) Covered Individuals, (ii) Information Systems and Endpoints, (iii) the Organizations' electronic information and (iv) the business processes run by Covered Individuals leveraging the Organizations' Information Systems, Endpoints and electronic information.

III. POLICY

The Organizations must periodically assess, identify and prioritize the potential risk and vulnerabilities to confidentiality, integrity and availability of organizational operations, Information Systems and Endpoints, and Covered Individuals.

Risks that have been identified by the Organizations are evaluated by the likelihood of threats exploiting vulnerabilities, and its impact to the Organizations. Once evaluated, risks will be managed by the Organizations through a series of risk management techniques that ultimately reduces the level of risk to the Organizations at a level deemed acceptable by the Executive Managers.

Capitalized terms used in this policy are defined in the glossary attached. The CISOs together may change the definitions in the glossary without the approval of the Executive Cyber Risk Committee.

IV. PROCEDURES

1. The CISOs of the Organization must maintain and document technical and administrative processes and procedures that meet the Risk Based Controls set forth below.

2. The CISOs of the Organization ensure the BSD and UCMC apply the same risk ranking mechanisms to ensures consistency.

3. The CISOs of the Organizations periodically conduct risk assessments, using the threat, vulnerability, and impact methodologies, of Information Systems and Endpoints, business processes, third party relationships or affiliations, and information practices.

4. Upon determination of any risks, the CISOs produce a remediation action plan which is designed to reduce the risk down to an acceptable level of tolerance as determined by the Executive Managers. The CISOs and the Executive Managers, Departmental or Unit Leaders, or System Owners will review and finalize the recommended remediation action plan. This remediation action plan can leverage the following risk management strategies:

    a. Remove the risk entirely by decommissioning affected component that has actualized the risk,
    b. Reduce the risk to an acceptable level, as determined by the Executive Managers, by implementing additional controls,
    c. Transferring the responsibility to a third party (non-Organizational entity) and ensuring the risk is appropriate managed through such transfer, or
    d. Accept the risk in its current state, if acceptable by the appropriate Executive Manager.

5. On an annual basis, the CISOs of the Organizations will (i) update the assessment of the current enterprise cyber risk posture, and (ii) conduct a risk assessment of the Certified EHR to meet the Meaningful Use requirements and objectives.

6. To continually assess and manage ongoing cyber risk to the Organizations, Departmental and Unit Leaders, Information System Owners and IT Custodians must notify the respective CISO of the Organizations under the following circumstances:
    a. <u>Department and Unit Leaders</u>
        i. When significant new Information Systems or Endpoints are introduced into the Organizations

ii. When introducing new or updated business processes which includes significant uses of information with third parties,
iii. When significant changes occur to their Information Systems or Endpoints

b. Information System Owners and IT Custodians:
i. When discovering cyber risks during the course of their duties
ii. When introducing significant new Information Systems or Endpoints into the Organizations
iii. When significant changes occur to their Information Systems or Endpoints

The CISOs will evaluate the reported risk pursuant to this policy.

7. Risks that have been identified pursuant to the procedures in this policy will be logged within the Organizations' risk registers by the CISOs, or their delegates.

8. Executive Managers, Departmental and Unit Leaders, System Owners and IT Custodians will participate with the CISOs upon the execution of any risk assessment process or procedure. Their obligations are as follows:
   a. Executive Managers:
      i. Support the Organizations' ongoing risk assessment and management processes
      ii. Accountable for addressing or accepting identified cyber risks
   b. Departmental and Unit Leaders:
      i. Provide resources to facilitate risk assessments and risk management activities
      ii. Accountable for managing risks identified within their departments or units, according to the identified remediation plans
   c. Information System Owners:
      i. Responsible for supporting and providing documentation necessary for conducting risk assessment activities
      ii. Responsible for determining the final remediation plan, in collaboration with the CISOs (or their delegates) and implementing remediation plans that were identified as part of the risk assessment activities, and reporting the status of said activities to the respective CISOs of the Organizations
   d. IT Custodians:
      i. Responsible to provide documentation necessary for conducting risk assessment activities
      ii. Responsible for implementing the controls that were identified as part of the remediation plans

9. Records and compliance reports pertinent to compliance with federal and state laws, such as risk assessments and actions and activities that the HIPAA Security Standards require to be documented, will be kept for a period of six (6) years.

The Organizations will use the Risk Based Controls below to implement the procedures.

V. RISK BASED CONTROLS

Risk based controls are organized in three categories; Core (C), Low (L) and Moderate (M). Core controls are mandatory for all Information Systems. Information Systems designated as FISMA Low must comply with Low controls, in addition to the Core controls. Information Systems designated as FISMA Moderate must comply with Moderate controls, in addition to the Low and Core controls.

Risk Assessment Policy and Procedures (RA-1 C)

Core	The CISO of each Organization define, document and disseminate a risk assessment policy and procedure that ensures Organizational cyber risks are controlled at an acceptable level.
Low	N/A
Moderate	N/A

Risk Assessment (RA-3 C)

Core	Risk assessments are conducted, including the likelihood and magnitude of impact, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the Information System, the information it stores, processes and transmits, or the business processes that run over top of it. Results of the risk assessment are delivered to the appropriate Executive Manager, Departmental or Unit Leader, and/or System owner and documented in the Organizations risk register. The risk assessments will be updated periodically, or upon determination by the appropriate CISO based upon a significant change to the Information System or environment.
Low	N/A
Moderate	N/A

Vulnerability Scanning (RA-5 C)

Core	The Organizations' Information Security Offices: • Scan for vulnerabilities within Information Systems on at a minimum on a monthly basis • Leverages vulnerability management tools that can automate the vulnerability management process by; (i) enumerating the Information Assets platforms, software flaws and configurations, and (ii) measuring the vulnerability's impact • Analyze the results of vulnerability scans and ensure that vulnerabilities are remediated by the applicable System Owner in accordance its level of risk or a standard
Low	N/A
Moderate	The Organizations' Information Security Offices: • Employs vulnerability scanning tools that include the capability to readily update the

	information system vulnerabilities to be scanned • Leverage authenticated scanning to check Information Systems configuration settings compared against checklists and test procedures • Implements authenticated vulnerability scanning to Information Systems with Protected Information to ensure the accuracy of the scans while providing the least amount of impact upon the Information System. • Shares information obtained from vulnerability scanning with Departmental or Unit Leaders and System Owners to help eliminate similar vulnerabilities in other Information Systems

Plan of Action and Milestones Process (PM-4 C)

Core	The Organizations' Information Security Offices will ensure that appropriate remediation action plans are developed, documented and disseminated based upon the results of the applicable risk assessment. This documentation will be kept for a period of six (6) years. The plans will document the remedial information security actions to adequately respond to risk to the Organizations' operations, Information Systems, business processes and Covered Individuals.
Low	N/A
Moderate	N/A

Risk Management Strategy (PM-9 C)

Core	The Organizations Information Security Offices: • Develops a comprehensive strategy to manage cyber risk to the Organizations operations, Information Systems, business processes, and Covered Individuals • Implements the risk management strategy consistently across the organization • Reviews and updates the risk management strategy on an annual basis, or as required, to address organizational changes.
Low	N/A
Moderate	N/A

VI. CROSS REFERENCES

POL-RO Responsibility and Oversight Policy

VII. POLICY REFERENCES

HIPAA Security Rules:

42 C.F.R §164.308 (a)(1)(i), (ii)(A),(B),(E),(iii)
42 C.F.R §164.316 (b)(2)(iii)

VIII. INTERPRETATION, IMPLEMENTATION AND REVISION

Each CISO is responsible for the interpretation and implementation of this policy, and responsible for recommending revisions of this policy to the Executive Cyber Risk Committee.

_____
Kenneth Polonsky
Dean, Biological Sciences Division

_____
Sharon O'Keefe
President, The University of Chicago Medical Center

IX. APPROVAL AND OWNERSHIP

Owner	Title	Date
Privacy & Security Steering Committee	Policy Development Group	
Approved By	**Title**	**Date**
Kenneth Polonsky, MD	Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs	
Sharon O'Keefe, RN	President, University of Chicago Medical Center	

X. REVISION HISTORY

Version	Description	Review Date
1.0	Initial Version	4/11/17