Responsibility and Oversight Policy

Table of Contents

I. Purpose ................................................................................................................................. 1
II. Scope ................................................................................................................................... 1
III. Policy .................................................................................................................................. 2
   A. Management Commitment ............................................................................................... 2
   B. Roles and Responsibilities ............................................................................................... 2
   C. Organizational Commitment ............................................................................................ 4
   D. Cyber Security Documentation Management .................................................................. 5
   E. Cyber Security Governance .............................................................................................. 6
   F. Policy Structure ................................................................................................................ 6
IV. Coordination among organizations, departments and programs ...................................... 6
V. Exceptions ............................................................................................................................ 7
VI. Enforcement ........................................................................................................................ 7
VII. Applicable laws, regulations and industry standards .......................................................... 7
VIII. Interpretation, implementation and revision ..................................................................... 8
IX. Approval and Ownership ..................................................................................................... 8
X. Revision History .................................................................................................................. 9

I. PURPOSE

The UChicago Medicine (including UCMC, The Care Network and the UCM Community Health and Hospital Division CHHD) and the Biological Sciences Division of The University of Chicago (the Organizations) uphold the Organizations’ absolute commitment to ensuring open discourse and the free expression of viewpoints and beliefs, as well as honoring the dignity and privacy of patients, which must meet legal, contractual, or enterprise confidentiality and security requirements (collectively the “Security Obligations”). The goals of the Cyber Security Programs and policies are to:

a) Support the core missions of the Organizations, including their shared mission of clinical care, education and research,

b) Create an environment that supports and enables its initiatives (e.g. community service, strategic growth, strategic operations, world-wide education in areas of science, clinical, translational and basic science research, preeminence of the Biological Sciences Division and the UChicago Medicine and scholarship) and to flexibly manage the risks based upon the environments, goals and information covered, and

c) Safeguards information in a manner that reduces risk and complies with the Security Obligations.

II. SCOPE

This policy applies to employees and students of the Organizations, individuals who fall within the definition of “Workforce” of an Organization, and third parties with access to the Organizations’ Information Systems and/or the Organization’s Information Assets ("Covered Individuals").
III. POLICY

In the pursuit and commitment to cyber security, this policy:

a) Defines the appropriate roles and responsibilities of leadership, Covered Individuals, and Departments and units within the Organizations, and

b) Sets forth the framework for cyber security policies to manage cyber security risks, comply with federal and state regulations, as well as applicable industry standards.

A. Management Commitment

Executive Management within the Organizations comprised of the Dean of the Biological Sciences Division, the President of UChicago Medicine, Presidents and Vice Presidents of its affiliates, Associate Dean’s, Assistant Dean’s, Vice Presidents, and Research Executives take responsibility to lead the cyber security efforts. Operational cyber security responsibilities and accountability have been delegated to the Chief Information Security Officers (CISOs). Executive Management expects the CISOs to seek guidance from compliance leadership, legal counsel, and experts within the industry, and to take into account the various interests within the Organizations.

B. Roles and Responsibilities

B.1 Management

Executive Managers, who are defined above, advocate and expect their Department and Unit Leaders, and their Covered Individuals, to comply with the cyber security policies and to maintain a level of security across the Organizations that aligns the Security Obligations and the Organizations’ mission and goals (as defined within the Purpose section above). Their responsibilities include, but are not limited to:

a) Approving the cyber security policies,

b) Evaluating results of cyber risk analyses and making risk based decisions for the Organizations,

c) Commitment to fund the Cyber Security Programs.

Department and Unit Leaders are leaders within the Organizations (e.g. Department Chairs, Section Chiefs, Executive Directors, Directors, Managers, Supervisors, etc.) who are responsible for overseeing cyber security within their respective areas of responsibility. Such responsibilities include but are not limited to:

a) Responding to remediation efforts necessary to manage cyber security risks,

b) Ensuring that Covered Individuals completes required Security Training

c) Ensuring Information System Owners and IT Custodians complete Security Training, when applicable,

d) Ensuring that each IT Custodian in his/her area of responsibility provides periodic reports with respect to the inventory of Information Assets used in such area to the applicable CISO.
B.2 Cyber Security Management

Chief Information Security Officers (CISOs) are the most senior individuals accountable for the cyber security programs within the Organizations. The CISOs create the cyber security strategy as well as day-to-day management of the Cyber Security Programs, which include leading their respective Information Security Offices, which are groups of information security professionals responsible for carrying out the Cyber Security Programs. Specific responsibilities include:

a) Developing, submitting to Executive Management for review and approval, disseminating, and assisting in the implementation of the cyber security policies,
b) Maintaining and executing the Organizations’ Cyber Security Programs,
c) Assessing cyber security risks on Information Systems in partnership with Information Owners and Information System Owners,
d) Educating and training Covered Individuals on the Security Obligations, cyber security policies, and relevant cyber security matters,
e) Collaborating with the UChicago Medicine Privacy Program, Chicago Biomedicine Information Services (CBIS), the Biological Sciences Division Information Services (BSDIS) and the University’s Information Technology Services (ITS) for strategic, tactical, incident management and enforcement actions,
f) Seeking guidance from and collaborating with the Organizations’ legal counsel to ensure a proper understanding and interpretation of the Security Obligations,
g) Developing the technical requirements, standards, and guidelines necessary to implement these cyber security policies and procedures,
h) Granting and documenting exceptions to any cyber security policy,
i) Facilitating cyber security incident response and recovery within the CISOs respective domain.

Executive Managers have delegated to each CISO the sole authority to conduct the following activities. The CISOs may delegate these activities to their trusted agents.

a) In a manner that must protect the privacy of our Covered Individuals, research subjects and patients, monitor communications and information on the Organizations’ networks, or the Organizations’ Information Systems,
b) Conducting vulnerability scanning of any Information Asset connected to the network supporting the BSD or UChicago Medicine, or Information Systems on third parties' (such as service providers’) networks where the such activities are permitted by the third party,
c) Conducting security assessments of Information Systems and Designated Secure Computing Facility within the Organizations,
d) Disconnecting Information Resources that present a security risk from the UChicago Medicine or BSD networks,
e) In certain circumstances, relating to security incident response processes, in the expert judgment of the CISO, erase all information stored on Information Assets (including organizationally-owned and personally-owned devices used for business purposes) as approved by the cyber security governance processes.
B.3 Information Owners

**Information Owners** are employees of the Organizations who are Director level, faculty, or above. Information Owners are responsible for classifying information according to the Data Classification Policy. Information Owners are responsible for complying with Security Obligations with regard to their information, and they will work in conjunction with the appropriate CISO, or their delegates, to understand their obligations and responsibilities and to ensure safeguards are implemented in accordance with the cyber security policies.

B.4 Information System Owners

An **Information System Owner** is an employee of the Organizations who is a Director level, faculty, or above who has the ultimate responsibility over a particular Information System. Information System Owners may delegate their tasks as appropriate. Information System Owners are responsible for complying with Security Obligations with regard to the Information Systems they control and they will work in conjunction with the appropriate CISO, or their delegates, to ensure safeguards are implemented in accordance with the cyber security policies. Such responsibilities include but are not limited to:

a) Categorizing their Information Systems based on the Asset Inventory and Categorization Standard,

b) Working with their IT Custodians to ensure proper safeguards are in place to address Security Obligations of the Information System,

c) Ensuring Users and IT Custodians are informed of and abide by relevant cyber security policies and procedures.

B.5 Information Technology Custodians

**Information Technology (IT) Custodians** are employees who are technical administrators of the Information Systems and Information Assets used by the Organizations. IT Custodians are responsible for ensuring proper safeguards are in place to address the Security Obligations of the Information Asset. They will create, implement and execute technical procedures that meet the Security Obligations applicable to the Information Assets within their responsibility.

B.6 Users

**Users** are Covered Individuals who are authorized to use Organizational Information and/or Information Assets in the course of their work for the Organizations. Users are expected to be fully informed of their cyber security responsibilities.

C. Organizational Commitment

The Cyber Security Programs ensure the Organizations' compliance with the Security Obligations. The CISOs use the National Institute of Standards and Technology (NIST) Special Publications as the basis of their risk analysis structure and procedures for carrying out cyber security protections.
Responsibility and Oversight Policy

The administrative safeguards: The cyber security policies and cyber security programs are designed to prevent, detect, contain and correct security violations.

The physical safeguards: The cyber security programs have designed the cyber security policies and the resulting procedures to:

a) Limit physical access to the Organizations’ electronic Information Systems and Designated Secure Computing Facilities (e.g. data centers) while ensuring that properly authorized access is allowed,
b) Specify the proper functions to be performed, the manner in which those functions are performed, and the physical attributes of the surroundings of a specific Endpoint or class of Endpoint that can access Restricted or Internal Use Only information,
c) Implement physical safeguards for all Endpoints that access Restricted or Internal Use Only information to restrict access to only authorized users,
d) Manage the receipt and removal of hardware and Electronic Media that contain Restricted or Internal Use Only information into and out of a facility, and the movement of these items within the facility.

The technical safeguards: The cyber security programs require Information System Owners to implement

a) Technical procedures for Information Systems that maintain the Organizations’ information to allow access only to those Covered Individuals or software programs that have been granted access,
b) Hardware, software, and/or procedural mechanisms that record and examine activity in Information Systems that contain or use Organizations’ information,
c) Procedures to protect the Organizations’ information from improper alteration or destruction,
d) Policies and procedures that verify the identity of a person or entity seeking access to the Organizations’ information.

D. Cyber Security Documentation Management

Cyber security policies are the documented policies, procedures, and controls implemented by the Organizations to protect the privacy, security, integrity, and access of information and Information Assets. The CISOs of the Organizations, in consultation with legal counsel, are responsible for creating, reviewing, and revising cyber security policies. All cyber security policies are approved by the Executive Cyber Risk Committee. All cyber security policies will be reviewed with a frequency to ensure that they reflect leading practices, no less than every three years.

Standards are defined security rules that apply to information and/or Information Assets to which Covered Individuals must comply. The CISOs of the Organization are responsible for creating, reviewing, and revising standards prior to approval by the Privacy and Security Steering Committee.

Technical procedures are technical steps that Covered Individuals will follow to further implement the policies, procedures and standards. Technical procedures are local, meaning they apply to particular environments. Information System Owners and IT Custodians, in
consultation with the CISOs of their respective Organization, are responsible for creating, reviewing, and revising technical procedures.

The attached Appendix I is a glossary of terms used in the cyber security policies. The CISOs together may change the definitions in the glossary without the approval of the Executive Cyber Risk Committee.

E. Cyber Security Governance

The Cyber Security Programs are governed and guided through a formal multi-tiered structure through the use of various committees. These committees function within their charters and are chaired by the appropriate Executive Manager:

- UChicago Medical Center Audit Committee
- UChicago Audit Committee
- The UCM Privacy and Security Steering Committee
- Any CHHD Privacy and Security Committees
- BSD Information Systems and Informatics Steering Committee
- UChicago Board of Computing Activities and Services
- UChicago Provost’s Information Technology Committee

F. Policy Structure

The Organizations have determined that the NIST 800-53 security and privacy controls provide an appropriate framework to meet its Security Obligations, including the HIPAA Security Rules. Each cyber security policy sets forth the purpose, scope, policy, procedures, and risk based controls applicable to the topic covered. Risk based controls are organized in three categories; Core (C), Low (L) and Moderate (M). Risk based controls are determined based on the impact analysis procedure conducted by the Information System Owner.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core (C)</td>
<td>Controls mandatory and required across the operating environment</td>
</tr>
<tr>
<td>Low (L)</td>
<td>Controls as defined by the impact analysis and subsequent risk analysis with the resulting designation of &quot;Low&quot;</td>
</tr>
<tr>
<td>Moderate (M)</td>
<td>Controls as defined by the impact analysis and subsequent risk analysis with the resulting designation of &quot;Moderate&quot;</td>
</tr>
</tbody>
</table>

Information Systems designated as a "FISMA Low" implement Low controls, in addition to the Core controls. Information Systems designated as a "FISMA Moderate" implement Moderate controls, in addition to the Low and Core controls.

IV. COORDINATION AMONG ORGANIZATIONS, DEPARTMENTS AND PROGRAMS

As the responsibilities for the security of the Organizations’ information cross departmental and organizational boundaries, the Organizations and all Covered Individuals will work in a collaborative and coordinated manner to maintain required security controls in place for the Organizations.
The Organizations' obligations to consistently comply with certain organizational requirements established by the Security Obligations may be found in the privacy policies. Additionally, the privacy and security programs may carry out obligations together, such as training and incident response. The cyber security policies are universal security policies designed to protect the Organizations, their information, their Information Systems, and to comply with all of their Security Obligations.

V. EXCEPTIONS

If any Covered Individual determines he/she cannot follow a cyber security policy, then he/she makes a formal Policy Exception request to the respective CISO of the Organization that governs the issue. Exceptions can only be granted by the individuals below within their realm of authority:

- the Chief Information Officers
- the BSD Chief Research Informatics Officer
- the Chief Information Security Officers

VI. ENFORCEMENT

Each Information Security Office within each Organization, in consultation with the UChicago Medicine Privacy Program, the Office of Legal Affairs and the University General Counsel, is responsible for interpretation, implementation, and revision of this policy. To the extent there are conflicting interpretations of this policy and another administrative policy, the more restrictive will apply.

A violation of the cyber security policies may result in corrective actions pursuant to each Organization's Human Resource policies. Corrective actions may include:

a) the immediate suspension of computer accounts and network access,
  b) mandatory attendance of additional training,
  c) a letter to the individual's personnel or student file,
  d) administrative leave without pay,
  e) termination of employment or non-renewal of faculty appointment or student status.

Federal and state government agencies have enforcement powers over individuals who violate the law, which can include civil penalties, civil actions, and criminal prosecution.

VII. APPLICABLE LAWS, REGULATIONS AND INDUSTRY STANDARDS

The Security Programs and cyber security policies are intended to comply with federal and state laws, including Illinois laws, and industry standards that apply to information and Information Assets.
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
Responsibility and Oversight Policy

Policy 1 POL-RO Effective Date 9/22/2015 Review Date 9/6/2018 Version 2.0

APPROVAL AND OWNERSHIP

<table>
<thead>
<tr>
<th>Owner</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy &amp; Security Steering Committee</td>
<td>Policy Development Group</td>
<td>7/1/2015</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approved By</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kenneth Polonsky, MD</td>
<td>Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs</td>
<td>9/22/2015</td>
</tr>
<tr>
<td>Sharon O’Keefe, RN</td>
<td>President, University of Chicago Medical Center</td>
<td>9/22/2015</td>
</tr>
</tbody>
</table>

IX. REVISION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Version</td>
<td>9/22/2015</td>
</tr>
<tr>
<td>2.0</td>
<td>Inclusion of Ingalls, Minor Edits, Definition</td>
<td>9/6/2018</td>
</tr>
</tbody>
</table>