I. PURPOSE
The University of Chicago Medical Center and the Biological Sciences Division of The University of Chicago (the "Organizations" or "we") protect information as a valuable asset. This policy classifies the Organizations' information, and third-party information in our possession or under our control, and governs the protection, use, and disclosure of information to protect its confidentiality, integrity, and availability. This policy also provides the steps to take to apply appropriate protections, including access controls, to the materials containing the information based upon the classification level.

II. SCOPE
This policy applies to all of the Organizations' information and all third-party information in our possession or under our control, in any format or media. All Covered Individuals must comply with this policy.
III. Policy

All Covered Individuals have an obligation to safeguard information owned by, or under the control of, the Organizations.

A. Classification

The level of protection required for any information depends on the information's classification. The Organizations classify information based on the information's sensitivity and recognized expectations associated with the sensitivity, its replacement cost, and the degree to which disclosure or misuse could damage or harm a patient, customer, employee, or business partner, or otherwise create liability or risk for the Organizations. Data Stewards are responsible for appropriately classifying all information for which they are responsible.

All of the Organizations' information falls into one of the following three classifications:

RESTRICTED – This classification includes sensitive information requiring the highest level of security and privacy controls to ensure confidentiality, integrity, and availability. Any information marked as CONFIDENTIAL will be deemed as RESTRICTED. The confidentiality, integrity, and availability of this information are of greatest importance to the Organizations, or third parties that have entrusted us with the information. This category also includes information that is subject to governmental regulations restricting its disclosure. Refer to the Appendix for already classified information and further examples.

INTERNAL USE ONLY – This classification includes information that is not RESTRICTED, but that should not be shared widely within the Organizations or publicly. Refer to the Appendix for already classified information and further examples. While not requiring the same level of security and privacy controls as RESTRICTED information, the Organizations, or third parties that have entrusted the Organizations with INTERNAL USE ONLY information, and still value its protection.

PUBLIC – This classification includes information that is already in the public domain or that the applicable Data Steward has approved for public release.

B. Use and Disclosure

Covered Individuals are required to safeguard RESTRICTED and INTERNAL USE ONLY information and only use it or disclose it as expressly authorized or required in the course of performing their job duties and only to the extent otherwise permissible under this and all other policies of the Organizations.

Covered Individuals may only disclose RESTRICTED information to individuals within the Organizations who need to know such information to perform their job duties and only to the extent such disclosure is expressly permitted by the Organizations' written policies or directed by the applicable Data Steward. Covered Individuals may disclose INTERNAL USE ONLY information to individuals within the Organizations who need such INTERNAL USE ONLY information to perform their job duties.
With respect to persons or entities outside the Organizations, Covered Individuals may only disclose RESTRICTED and INTERNAL USE ONLY information
a. as required by law or
b. as permitted by the applicable Data Steward, but only to persons or entities outside the Organizations if such disclosure is made pursuant to a written agreement approved by the applicable Data Steward and negotiated and signed by the Organizations' authorized personnel that contains appropriate confidentiality and security restrictions. The Data Steward's decisions are based upon the Organizations' policies, contractual obligations, and legal requirements.

PUBLIC information may be freely disclosed.

In addition to this policy, when using or handling RESTRICTED and INTERNAL USE ONLY information, Covered Individuals must comply with all other applicable policies of the Organizations. Other policies and similar governance documents that may apply include:

- For clinical research, see the Institutional Review Board (IRB) policies and procedures, and guidance from the Office of Clinical Research
- For obligations relating to University signed agreements see University Research Administration (URA)
- For patient care related information, see the HIPAA Privacy policies and UCMC Administrative Policies
- For employment records, see the University and UCMC HR policies
- For student record, see the University's policies under FERPA
- For credit card processing and eCommerce, see the University’s credit card processing policies
- For research within the BSD that is required to meet FISMA security standards, see the Office of the Chief Research Information Officer.
- University Confidential Information, as described in the University's Human Resources policy number 601 for the Treatment of Confidential Information.

Covered Individuals with questions about the use or disclosure of information should consult the Organizations' policies, their supervisors, or the applicable Data Steward.

IV. PROCEDURES

A. Classification of Information

Data Stewards are responsible for classifying information for which they are responsible in accordance with the classification definitions above. Unless the Data Steward determines that information constitutes RESTRICTED or PUBLIC, the default classification will be set to INTERNAL USE ONLY. When any document, data collection, compilation or other material contains information from more than one classification, the Data Steward should classify the material using the classification of the most sensitive information included in the material. Data Stewards should classify all materials, whether in draft or final form.

B. Notification of Classification
Data Stewards should use reasonable means to notify data recipients of the classification of any data they receive. For example, a Data Stewards may post their classifications on the website for their department or unit and instruct all personnel responsible for regulating data access to inform recipients of the applicable classification.

C. Labeling of Materials/Maintaining Labels

The Data Steward will identify the Covered Individuals responsible for labelling the materials.

As feasible, Covered Individuals should clearly and prominently label any RESTRICTED or INTERNAL USE ONLY materials that they create or that they receive from a third party as directed by the Data Steward.

Data Custodians should not alter, modify, or remove classification labels from any labelled materials they receive. Data Custodians should apply the same label when reproducing any labeled material regardless of the form or format of the reproduction; however, if the material is combined with more sensitive information, the Data Custodian should apply the label applicable to the more sensitive information. For example, if a Data Custodian receives a presentation labeled as RESTRICTED, the Data Custodian should label any printed copies of the presentation as RESTRICTED.

If a Data Custodian determines that any labeled materials have been redacted or modified such that the redacted materials qualify for a lower sensitivity classification, as determined by the Data Steward, then the Data Custodian may re-label the materials with such lower sensitivity classification. For example, materials containing Protected Health Information (PHI) or social security numbers (SSNs) are properly classified as RESTRICTED. If such materials are redacted to remove PHI, SSNs, and all other RESTRICTED, the Data Custodian may re-label the redacted materials as INTERNAL USE ONLY.

D. Printed Materials

When disclosing, delivering, or transmitting printed materials, Covered Individuals should comply with the following guidelines:

When using the Organizations’ internal mail system to send materials containing RESTRICTED or INTERNAL USE ONLY information, the sender should place the materials in a sealed envelope labeled on the outside with the source and destination (both the name and location) and the classification.

Where practical, Covered Individuals should personally deliver materials containing RESTRICTED or particularly sensitive INTERNAL USE ONLY information.

Materials containing RESTRICTED or INTERNAL USE ONLY information should never be delivered to an unattended desk or left in the open or in an unoccupied office.

The sender should track all RESTRICTED or INTERNAL USE ONLY information sent through commercial courier with a weigh bill number and should require a signature upon receipt.
E. Electronic or Digital Materials

When storing, accessing, or transmitting RESTRICTED or INTERNAL USE ONLY information using any information systems or electronic devices (including laptops, desktops, smart phones, and other mobile devices), Covered Individuals must follow the Organizations' cyber security policies and other policies and procedures relating to information systems and electronic devices. Without limiting anything in the Organizations’ other policies, Covered Individuals should comply with the following guidelines:

Covered Individuals should encrypt information, the security of which is regulated, when transmitting it outside the organization in electronic format. Protected Health Information (both patient and employee), passwords, payment card information, and Social Security Number associated with Personally Identifiable Information must be encrypted. Covered Individuals should consult with the Organizations' information technology staff to determine the appropriate encryption technology for their information and devices.

The Organizations' have created a protected environment that is operated out of CBIS. The Organizations' protected environment includes only those emails with the following email address extensions:

@uchospitals.edu
@bsd.uchicago.edu
    Including any departmental extensions, such as
    medicine.bsd.uchicago.edu.
@dacc.uchicago.edu
@radonc.uchicago.edu

Covered Individuals may not forward emails containing Protected Health Information (both patient and employee), passwords, payment card information, and Social Security Number associated with Personally Identifiable Information to another University email address (such as @uchicago.edu unless the email is encrypted.

Covered Individuals may not use personal email accounts, personal cloud storage, or other personal tools or personal systems not approved by the Organizations to transmit, store, or process any RESTRICTED or INTERNAL USE ONLY information.

V. CROSS REFERENCES

POL-RO Roles and Oversight Policy
POL-AC Access Control Policy
HIPAA Privacy de-identification policy

VI. POLICY REFERENCES

HIPAA Security Rules: 42 C.F.R. § 164.302 – 164.316
VII. 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
VIII. 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>4/1/16</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>4/14/16</td>
</tr>
<tr>
<td>Sharon O'Keefe, RN</td>
<td>President, University of Chicago Medical Center</td>
<td>4/14/16</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>4/14/16</td>
</tr>
</tbody>
</table>
X. **APPENDIX A – DATA ELEMENTS AND EXAMPLES**

Below are predefined data elements broken up into the three classifications: Restricted, Internal Use Only, and Public. Data elements that have been predefined may not be classified into a lower classification without the approval of the appropriate Data Steward. It should be noted that this is not an exhaustive list, rather a list that has already had data elements predefined in their classification.

**RESTRICTED**

**Business**
- Passwords
- Board Materials
- Managed care documents/contracts
- Non-public financial information including financial statements, balance sheets, investment information, federal and state tax information and draft returns
- Identities of and communications with potential donors
- Marketing leads for potential physician referrals
- External regulatory and audit reports
- Allegations of wrongdoing, including demand letters, notices from third parties or a government regulator, potential claims
- Investigation materials including compliance investigations and investigations into allegations of wrongdoing
- Incident response and remediation reports, investigation materials and other documents
- Technical vulnerability details

**Clinical Information**
- Protected Health Information, electronic Protected Health Information, Designated Record Set, medical record, billing, insurance and payment information, all patient photos and images, and Highly Confidential Information (specifically HCI patient information)
- Clinical research data
- Medical studies act protected information
- Payor Health Plan Number
- Patient and Employee Insurance Coverage Information
- Safety and quality patient incident review including M&M, sentinel events
- Clinical risk assessment details and reports

**Other Regulated Information**
All information the disclosure of which is restricted by city, county, state, federal, or international laws or regulations, including:
- Personally Identifiable information, including Social Security Number
- Family Educational Rights and Privacy Act governed information including student records, student grades
- Credit and debit card data, and other payment card data regulated by the Payment Card Industry
- Employee health information, including employee PHI, as part of the Medical Center and University health plans
- Human resource information including employee resources files, employee personal information, employment records, salary information, performance reviews
• Attorney-client privilege information
• IRB deliberations and minutes
• Export law controlled materials
• Biometric information
• Juvenile offender information
• Domestic and sexual abuse information of non-patients

Contractually Protected
• Information restricted under a confidentiality requirement or that is contractually subject to a privacy or security obligation or law. Examples include third party software and source code, data subject to FISMA, third party non-public information, contract terms subject to confidentiality
• Non-public grants and contracts

Other
If the following materials contain information categorized as RESTRICTED, then the materials are promoted to that higher classification.

• Safety employee or visitor incident review (e.g. slips, workman comp, etc)
• Internal Compliance Review Documents
• Internal Audit Documents
• Grants and Proposals Applications
• Peer review grants, proposals and notes
• IRB Protocols
• Security reports (e.g. incident reports, risk assessments, technical/architecture reviews, etc)

INTERNAL USE ONLY

If the following materials contain information categorized as high or medium, then the materials are promoted to that higher classification.

• Policies
• Procedures, which includes administrative, patient care, technical and other internal procedures
• Drafts of Documents, including IT documents, network diagrams, statements of work, service agreements, etc.
• Employee identification number
• Personal information of employees, visitors, or guests including non-public demographic information
• Information about corporate strategy including organizational strategic growth, marketing, market share, affiliations, and corporate transactions.
• Internal business communications including hard copy (e.g. reports, memoranda, presentations, training materials) and soft copy (e.g. voicemail, texts, pages, instant messages, and emails)
• Contracts not subject to confidentiality obligations
• Business Plans
• Architectural plans and floor plans in draft form or that are non-public
• Survey Readiness
• Committee Meeting Minutes
• Proprietary Lab Techniques
• Non-Clinical Research Data and data collected pursuant to a research protocol (unless open)
• Information system logs, usage information, network information, and meta data
• Security metrics
• Internal Computer Code (Not 3rd Party Computer Code)

PUBLIC

• Annual Reports
• Content that is publically available on the Web

XI. APPENDIX B: DEFINITIONS

Covered Individuals
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.

Data Stewards
Members of Executive Management and their delegates who are responsible for classifying their information, identifying who may access their Information, and implementing processes to protect the Information.

Data Custodians
An individual or group with administrative and/or operational responsibility over information assets and must follow all appropriate and related security guidelines to ensure the protection of sensitive data and intellectually property residing on systems for which they have accountability.