NORTHEAST OHIO MEDICAL UNIVERSTY	Policy No: 3349-09-18
POLICY TITLE: University Data Policy	EFFECTIVE DATE: June 22, 2017 REVIEWED AND UPDATED: June 1, 2026
RESPONSIBLE DEPARTMENTS: Information Technology	All Data Users and University Data

(A) PURPOSE

This policy establishes Northeast Ohio Medical University's (NEOMED's) framework for the classification, governance, access, protection, and lifecycle management of University Data. It aligns institutional practices with applicable laws and regulations and enables consistent controls that safeguard confidentiality, integrity, and availability of University Data while supporting NEOMED's academic, clinical, research, and operational missions.

(B) SCOPE

This policy applies to all University Data and Data Users, and establishes the roles and responsibilities to properly classify, use, protect, and manage University Data.

(C) DEFINITIONS

(1) "Data Custodian" is defined below in Section (D)(3)(e)(i).

(2) "Data Governance Council" is defined below in Section (D)(3)(b)(i).

(3) "Data Manager" is defined below in Section (D)(3)(d)(i).

(4) "Data Steward" is defined below in Section (D)(3)(c)(i).

(5) "Data User" is defined below in Section (D)(3)(f)(i).

(6) "Personally Created Data" refers to information created, collected, maintained, transmitted, or recorded that is not related to University business but is personal in nature.

(7) "University Data", also referred to "Institutional Data", refers to data created, collected, stored, maintained, transmitted, or recorded by or for NEOMED to conduct University operations. It includes research data and data used for furthering the University's mission but does not include Personally Created Data. University Data may exist in any format (i.e. electronic, paper, audio, visual).

(8) "University Records" refers to documents or items, regardless of form, that document NEOMED functions, policies, decisions, procedures, operations, or

other activities; University Data may reside in Records, be used to produce Records, or itself constitute a Record.

(D) POLICY STATEMENT

(1) Overview

(a) University Data is a valued strategic asset of NEOMED and is to be provided on an as needed basis to Data Users in furtherance of their University responsibilities. This policy establishes the roles and responsibilities to properly classify, use, protect, and manage University Data.

(b) Permission to access, use, disclose, or generate University Data will be granted to authorized Data Users only for legitimate University purposes and based upon their roles and compliance with University, contractual, and legal requirements.

(2) Classification of University Data

(a) The University is committed to the privacy of its community and protecting the confidentiality, integrity, and availability of University Data. As such, University Data classifications have been created to ensure the appropriate security controls are applied for systems and applications containing such data.

(b) All University Data must be assigned to a classification level. The classification level is based on compliance, legal, criticality, operational usage, and risk considerations. The four University Data classification levels from least to most restrictive are:

(i) Public (L1): University Data that is intended for public disclosure and use.

(a) A breach of confidentiality, integrity, or availability would have little to no adverse impact on the University's mission, safety, finances, or reputation.

(ii) Internal (L2): University Data that is used to conduct University business and is not generally available to the public. Internal Data can be shared externally, where appropriate; however, access restrictions should be applied accordingly.

(a) A breach of confidentiality, integrity, or availability could have minimal adverse impact on the University's mission, safety, finances, or reputation.

(iii) Restricted (L3): University Data that due to legal, contractual or other requirements, and may not be accessed without specific authorization.

(a) A breach of confidentiality, integrity, or availability could have moderate adverse impact on the University's mission, safety, finances, or reputation.

(iv) Highly Restricted (L4): University Data that requires the highest level of protection because inappropriate handling of this data could result in criminal or civil penalties, identity theft, and/or financial loss.

(a) A breach of confidentiality, integrity, or availability could have significant adverse impact on the University's mission, safety, finances, or reputation.

(c) In absence of being formally classified, University Data should be treated as Internal Data by default.

(d) When a set or collection of University Data includes different classifications, the set or collection will be classified at the most restrictive level present.

(e) University Data may be classified at a more restrictive level; if so, it must meet the minimum-security controls of that higher classification level.

(f) Requests to modify the classification of University Data must be submitted to and approved by the Data Governance Council.

(3) Roles, Responsibilities & Structure

(a) While the University owns and ultimately controls all University Data, data governance is accomplished through collaborative efforts of a variety of University personnel, grouped according to the nature of their participation, scope of responsibility, and particular activities. The data governance structure and its primary roles, groups and associated responsibilities are described below.

(b) Data Governance Council

(i) The Data Governance Council is a University committee that provides strategic planning, governance, and oversight for University Data to support data integrity, compliance, and accountability.

(ii) Their responsibilities include the following:

(a) Review and approve University Data policies and standards;

(b) Defines and publishes Data Classification assignments and data governance roles;

(c) Resolve escalated or cross-domain data usage and ownership issues; and

(d) Provide compliance oversight (FERPA, GLBA, HIPAA, state laws).

(iii) Implementation and operational execution of University Data policies and standards are the responsibility of designated Data Stewards and Data Managers.

(c) Data Stewards

(i) Data Stewards are senior University officials that are responsible for the overall governance, appropriate use, and protection of University Data within their functional areas.

(ii) Their responsibilities include the following:

(a) Serve as members of the Data Governance Council;

(b) Appoint and oversee Data Managers;

(c) Be accountable for appropriate use of data within their functional areas;

(d) Accept and manage institutional risk associated with the use, collection, sharing, retention, and protection of University Data within their domain;

(e) Approve access criteria and sharing agreements; and

(f) Ensure compliance with law and policy.

(d) Data Managers

(i) Data Managers act on behalf of Data Stewards and are subject matter experts responsible for the operational management, quality, and consistent application of University Data in accordance with approved policies and standards. This is a delegated responsibility and does not confer ownership or final decision-making authority.

(ii) Their responsibilities include the following:

(a) Maintain University Data classifications;

(b) Define and maintain University Data definitions and business rules;

(c) Monitor and improve data quality and integrity;

(d) Review and process routine data access and use requests in accordance with approved criteria;

(e) Maintain metadata, documentation, and data standards;

(f) Identify and escalate data issues, risks, or policy conflicts to the Data Steward; and

(g) Coordinate with Data Custodians to ensure proper implementation of standards.

(e) Data Custodians

(i) Data Custodians are responsible for the technical management, protection, and operation of systems that store, process, or transmit University Data.

(ii) Their responsibilities include the following:

(a) Implement appropriate technical security controls for University Data aligned with institutional policy and data classification standards;

(b) Ensure access is limited to approved purposes;

(c) Provide incident response support;

(d) Monitor University Data usage and policy compliance; and

(e) Notify Data Managers or Stewards of changes that may affect data integrity or access.

(f) Data Users

(i) Data Users are those who access, use, disclose, generate, administer, or manage University Data. This includes, but is not limited to, faculty, staff, students, contractors, volunteers, visitors, sponsored guests, and affiliated entities acting on behalf of NEOMED.

(ii) Their responsibilities include the following:

(a) Properly manage and protect University Data as set forth in this policy;

(b) Report suspected incidents immediately; and

(c) Complete required training annually.

(4) Public Records

(a) Although University Records may be subject to disclosure under Ohio's Public Records Act, the underlying University Data must be protected according to its classification. Public records requests must be handled in accordance with NEOMED's Public Records policy.

(5) Records Management and Data Disposition

(a) University Data may reside in University Records, be used to produce University Records, or itself constitute University Records. Ohio law requires that University Records not be disposed prior to the expiration of the authorized retention period. University Records must be managed in accordance with approved records retention and disposition schedules consistent with the Records Management Policy and Records Retention Schedule.

(6) Reporting Unauthorized or Inappropriate Access

(a) All individuals to whom this policy applies must immediately report suspected unauthorized or inappropriate access, use, disclosure, or generation of University Data to the IT Help Desk or Information Security team, per incident response procedures.

(7) Training

(a) Individuals with access to Highly Restricted (L4) data must complete annual, University-approved training. All others must complete annual

University Data awareness training. Additional training may be required by legal, regulatory, contractual, clinical, or research obligations.

(8) Relinquishing Data

(a) Data Users must relinquish University Data upon the end of employment, affiliation, or as otherwise required due to role changes, Data Manager requirements, provisions with executive leadership, and/or University policy.

(9) Personally Created Data

(a) Information not related to University business that is personal in nature is the responsibility of the individual to back up, save, manage, and maintain; NEOMED does not assume liability for Personally Created Data.

(10) Policy Exceptions

(a) Requests for exceptions to this policy must be submitted to the Data Governance Council for review and approval prior to implementation. Approved exceptions must document compensating controls and an expiration date.

(11) Policy Violations

(a) Violations may result in denial of access to University computing resources and corrective or disciplinary action, up to and including termination or dismissal, in accordance with applicable University policies. The University may temporarily suspend or block access prior to completion of disciplinary procedures and may refer suspected legal violations to law enforcement.