



Ohio Administrative Code

Rule 3349-1-204 Artificial intelligence use rule.

Effective: [September 25, 2026](#)

(A) Purpose

Northeast Ohio medical university (NEOMED) permits the responsible use of artificial intelligence (AI) to support teaching, learning, research, clinical education, administration, and university operations. This rule establishes requirements for the use of AI to protect university data, support innovation, preserve academic and professional judgment, and align with NEOMED's data classification and security framework.

(B) Scope

This rule applies to all faculty, staff, students, contractors, and other individuals who use AI systems in connection with NEOMED business, academic programs, research, clinical education, university operations, or university data.

(C) Definitions

- (1) "Artificial intelligence" or "AI system" refers to any software, platform, model, or technology that generates, summarizes, classifies, analyzes, predicts, recommends, or transforms content using machine learning, generative processes, large language models, or related methods.
- (2) "Export-controlled information" refers to information, software, technology, technical data, defense articles, controlled unclassified information, or other materials subject to the export administration regulations (EAR), international traffic in arms regulations (ITAR), U.S. department of the treasury office of foreign assets control (OFAC) sanctions requirements, technology control plans (TCP), or sponsor-imposed export restrictions.
- (3) "High-assurance AI environment" is an institutionally approved AI system with additional contractual, privacy, security, access, retention, audit, or regulatory protections sufficient for approved higher-risk uses.
- (4) "Institutionally approved AI system" is an AI system reviewed and approved through the university's designated process for the relevant data classification and use case.
- (5) "NEOMED-administered AI system" is an AI system or workspace for which NEOMED owns or controls the workspace, designates administrators, manages access and settings, reviews applicable contractual/privacy/security terms, defines permitted data uses, and can remove access when no longer authorized.



3349-1-204

2

- (6) "Personal AI account" means an AI account not owned, contracted for, or governed by NEOMED, whether free or paid.
- (7) "Public, internal, and restricted university data" refers to the terms and meanings assigned in NEOMED rule 3349-9-18 of the Administrative Code. Specifically:
 - (a) "Public university data" refers to data that is intended and accessible for public use, and is not restricted by law or regulation.
 - (b) "Internal university data" refers to data that is used to conduct university business for which access must be guarded and is not intended for public dissemination, but is not generally restricted by law or regulation.
 - (c) "Restricted university data" refers to data that requires the highest level of protection due to law, regulation, contractual, or industry standards. Unauthorized use or disclosure of this data could be expected to have severe adverse effects on university operations, university assets, or individuals.
- (8) "University data" refers to the terms and meanings assigned in NEOMED rule 3349-9-18 of the Administrative Code, university data rule.

(D) Policy statement

- (1) AI use is permitted when the data classification, AI system/account type, contractual and security protections, and use case risk are aligned. Users are responsible for understanding what type of university data they are entering into an AI system and whether that AI system or account is appropriate for the intended use.
- (2) AI must not be used to avoid or replace required human academic, clinical, administrative, legal, compliance, research, or professional judgment.
- (3) AI should not be held to a higher standard than other university data practices, but AI use may require additional safeguards when it creates new risks related to exposure, retention, access, reuse, accuracy, bias, or decision impact.
- (4) All AI systems must undergo applicable security, privacy, accessibility, legal, procurement, and contractual review before acquisition or use.

(E) Data use requirements

- (1) Users must determine the applicable university data classification, or seek guidance when uncertain, before entering university data into an AI system.



3349-1-204

3

When data of more than one classification is combined, the most restrictive classification controls.

- (2) Public data may generally be used with AI systems, provided the use is lawful, ethical, and consistent with university policy.
- (3) Internal data may be used in AI systems or account types appropriate for internal university business. Personal AI accounts may be used for limited low- or moderate-risk uses when no restricted data is included, user-controlled privacy settings are enabled, any university-required training has been completed, and the use is consistent with university policy and guidance.
- (4) For university work, AI systems or accounts that do not use user data for model training or improvement by default are preferred over those that require users to opt out of such use.
- (5) Restricted data may be used only in an institutionally approved AI system approved for the specific data type and use case.
- (6) Restricted data must not be entered into personal AI accounts or unapproved AI systems.
- (7) Institutionally approved AI systems processing restricted data must support audit logging, monitoring, access controls, and documented retention practices.
- (8) Users must not enter protected health information (PHI), identifiable student education records, identifiable human subjects research data, login credentials, passwords, access tokens, or other authentication information, social security numbers, confidential personnel information, confidential legal or contractual information, or other restricted data into an AI system unless the system and use case have been specifically approved.
- (9) AI-generated or AI-assisted content that documents university business may constitute a university record and remain subject to Ohio public records law and records retention requirements.
- (10) AI-generated content remains subject to university intellectual property, copyright, licensing, and ownership policies.

(F) Academic, curricular, and assessment uses

- (1) AI may be used for academic and curricular purposes, including curriculum mapping, gap analysis, integration across programs, development of new



3349-1-204

4

curricular materials, study resources, assessment items, rubrics, and other teaching and learning materials.

- (2) The appropriate AI system or account for curricular materials depends on the highest-risk data included, applicable legal, security, or contractual restrictions, assessment-integrity concerns, and the intended use.
- (3) Student education records designated as restricted data may only be processed within institutionally approved AI systems intended for FERPA-regulated information and that provide appropriate contractual, technical, administrative, and security safeguards.
- (4) Faculty and course directors must establish assignment-specific AI use expectations, including whether AI is prohibited, permitted only as a study or revision aid, or fully allowed with disclosure and critical evaluation. Students must follow the AI use designation, documentation requirements, and academic integrity expectations communicated for each course or assignment.
- (5) AI may support grading or assessment tasks using de-identified student work as a draft aid, subject to human oversight, verification, and final academic judgment.
- (6) AI must not be used to make or determine student assessment outcomes, grades, progression, remediation, professionalism determinations, or other consequential educational decisions without appropriate human oversight, verification, and final academic judgment.

(G) Research and scholarly uses

- (1) AI may be used for research and scholarly activities, including literature review support, idea generation, coding assistance, data analysis support, manuscript development, grant development, research operations, and dissemination.
- (2) AI use in research must comply with applicable IRB (institutional review board) requirements, informed consent, data use agreements, grant or sponsor terms, privacy and security requirements, publication and authorship standards, intellectual property obligations, and university policy.
- (3) Users must not enter identifiable human subjects research data, PHI, contractually restricted data, sponsor-confidential information, or other restricted university data into an AI system unless the system and use case have been specifically approved. AI-generated research output must be verified by qualified individuals before use in research records, publications, grant submissions, or other scholarly products.



3349-1-204

5

- (4) Research data, technical data, software, controlled unclassified information (CUI), export-controlled information, or other information subject to the EAR, ITAR, sanctions regulations administered by OFAC, or sponsor-imposed restrictions must not be entered into an AI system unless the use has been specifically reviewed and approved by the university's designated export control, compliance, research administration, information security, and legal authorities, as applicable.

(H) Role-specific responsibilities

- (1) Users must complete university-required data privacy, information security, or AI use training before entering Internal, or restricted data into an AI system. Users must complete any required role-based refresher training, as applicable. University IT is responsible for making recommendations to the executive management team.
- (2) All users are responsible for complying with this policy.
- (3) Faculty, instructors, and course directors are responsible for: communicating permitted and prohibited AI uses in courses, assignments, assessments, and learning activities; reviewing AI-assisted instructional or assessment materials before use; and ensuring that AI use supports course objectives, academic integrity, fairness, accessibility, and professional formation.
- (4) Students and trainees are responsible for: following course, assignment, clinical, research, and program-specific AI instructions; disclosing AI use when required; verifying AI-assisted work; and maintaining academic and professional integrity.
- (5) Faculty and staff must follow role-specific data classification and approval requirements.

(I) Prohibited uses

- (1) Unless specifically approved through the appropriate university process, users must not:
 - (a) Use AI in clinical education or clinical settings in ways that exceed the user's role, violate site or supervisor expectations, replace licensed clinical judgment, or involve PHI or other restricted data in an unapproved AI system;
 - (b) Make or substantially determine admissions, progression, discipline, hiring, promotion, compensation, financial, or other consequential decisions



3349-1-204

6

about individuals without appropriate human oversight, verification, and final judgment;

- (c) Process IRB-regulated or contractually restricted research data in a manner inconsistent with IRB approval, consent, data use agreements, sponsor terms, or other applicable requirements;
- (d) Upload, process, analyze, summarize, or otherwise disclose export-controlled information, controlled technical data, CUI, technology subject to a TCP, sanctioned-country information, or sponsor-restricted research information in an AI system that has not been specifically approved for such use.

- (2) AI-related privacy, security, and compliance incidents must be promptly reported through established university incident reporting processes in NEOMED rule 3349-1-203, information security incident response plan.

(J) Ethical and responsible use

- (1) All AI use must follow these principles:

- (a) Human accountability: Users remain responsible for AI-assisted outputs and actions.
- (b) Accuracy and verification: Users must independently validate AI output for accuracy, completeness, bias, hallucinations, fabricated citations, outdated information, and appropriateness before use.
- (c) Human oversight: AI must not independently make consequential decisions affecting students, employees, patients, research participants, applicants, or other individuals.
- (d) Transparency: Users should disclose AI assistance when appropriate, including in teaching, assessment, research, scholarship, administrative decision-making, or student-facing contexts.
- (e) Fairness and accessibility: Users must consider potential bias, inequity, accessibility barriers, or inappropriate assumptions in AI output.
- (f) Privacy and confidentiality: Users must comply with the data-use requirements in paragraph (E) of this policy.



3349-1-204

7

(g) Academic and professional integrity: AI use must comply with course expectations, authorship standards, professional norms, and institutional policies.

(h) Intellectual property and licensing: Users must respect copyright, licensing, publisher, vendor, and third-party ownership restrictions.

(K) Implementation guidance and review

The university shall maintain implementation guidance, AI use matrices, syllabus guidance, training requirements, and an approved AI tools register to help users apply this rule. This rule shall be reviewed periodically. Related guidance may be updated more frequently to address changes in AI systems, legal requirements, institutional needs, and risk conditions.

(L) Compliance

Violations of this policy may result in restriction of AI access, required remediation, referral to the appropriate university office, or other action under applicable university rules, contracts, laws, or regulations. Questions about the classification of university data should be directed to the appropriate data steward, system steward, information security personnel, general counsel, or other designated university authority.