Faculty Handbook	**E30: Research Data Management**
Approved By: Faculty Senate	
Effective Date: **Draft 5/17/2023**	
Responsible Faculty Committee: Research Policy Committee	
Office Responsible for Administration: Vice President for Research (VPR) and Health Sciences Vice President for Research (HSVPR)	

Legend: **New Policy Proposed** –no highlights.

Revisions to the Policy Rationale, Policy Statement, and Applicability sections of this document must be approved by the Faculty Senate.

POLICY RATIONALE

UNM maintains a steadfast commitment to support the academic freedom of its research community and maximizing the impact of UNM's research activities. This includes researchers' rights and responsibilities to determine the direction of their research and scholarly work and dissemination of their findings. UNM's commitment to teaching and research is primary, and this Policy does not diminish the right and obligation of faculty, staff, and students to disseminate research results for scholarly purposes.

This Policy reflects UNM's commitment to complying with research data management laws, agreements, and regulations throughout the research lifecycle. As recipients of sponsored awards, participants in the research enterprise, and stewards of public trust, UNM, its researchers, and other UNM personnel have rights and responsibilities concerning access, use, sharing, privacy, security, confidentiality, maintenance, storage, retention, and disclosure of research data and must comply with this and other UNM policies relating to research data management. Faculty members working with students on research projects must inform students in advance of their responsibilities under this Policy.

POLICY STATEMENT

Research data requirements originating from regulators, sponsors, and publishers; combined with disciplinary norms and institutional values of transparency, replicability of research findings, and compliance with legal and ethical standards produce a complex data management landscape within which UNM research is conducted. The purpose of this Policy is to delineate rights and responsibilities pertaining to ownership and management of data and associated materials for UNM research activities. The Vice President for Research (VPR) and the Health Sciences Vice President for Research (HSVPR) have final authority for compliance with this Policy and are responsible for its implementation. Consistent with this responsibility, the VPR and HSVPR may designate advisory support and enforcement decisions to other individuals or

offices at UNM, and coordinate with research support service providers to facilitate researcher and program compliance with this and related policies.

If state or federal laws or regulatory requirements differ from this Policy, the state and federal requirements shall supersede all relevant portions of this Policy.

1. Ownership and Transfer of Research Data

As research data and materials generated by UNM researchers under sponsored agreements for projects conducted at UNM, under the auspices of UNM, or otherwise with UNM resources are "Technical Information" or "Technological Works," all rights are owned by UNM in accordance with Board of Regents Policy **5.8** and *Faculty Handbook* Policy **E70** "Intellectual Property." UNM's rights apply in all cases except where explicitly precluded by the specific terms of sponsorship, other agreements, (such as sub-award or institutional collaboration agreements), or in the case of student research data as specified in Section 1.1 below.

In the absence of specific restrictions, under applicable law, UNM policy, or contractual obligation, UNM grants to the researcher who creates research data an unrestricted right to use, modify, develop derived products, and redistribute the data as they determine. The researcher is responsible for being cognizant of and remaining compliant with any regulatory, legal, and contract issues related to the research data. The researcher will be informed of regulatory, legal and contract issues during the pre-award process and should contact the VPR or HSVPR for clarification or to address issues when appropriate. If a researcher has questions or concerns about their responsibilities, they may contact their dean or designee, the VPR or HSVPR who will refer the researcher to the appropriate support resources to help them comply with this Policy.

1.1 Student Research Data

Students own research data that they generate or acquire in the course of independent research, unless the research data are:

- generated or acquired within the scope of their employment at UNM,
- generated or acquired through use of substantial UNM resources as delineated in Section 2.2.2, 2.3.3, and 2.3.4 of *Faculty Handbook* Policy **E70** "Intellectual Property."
- generated as a part of a sponsored project, or
- subject to other agreements and regulations that supersede this right, including but not limited to, Institutional Review Board (IRB), Electronic Health Record (EHR), Protected Health Information (PHI) requirements, or other data use agreements.

If there are questions about student ownership of data, inquiries should first be directed to the student's department, then, if unresolved, to the Office of the VPR (OVPR) or HSVPR.

1.2 Research Investigator Leaves UNM

In the event that a research investigator leaves UNM, research data (originals and any duplicates) must be:

- retained by UNM at an appropriate location, and
- if made publicly available, provided persistent identifiers (such as Digital Object Identifiers – DOIs) facilitating citation, discovery, and appropriate authoritative access.

The VPR or HSVPR, or their designee, will work with the departing research investigator and the investigator's new institution (if applicable) to craft an appropriate material transfer agreement to accomplish the transfer of such research data when UNM determines it is necessary or desirable to have such an agreement because of the nature of the research data; or because of regulatory, legal, or contract issues. In the rare event that the research data cannot be divided, replicated, or otherwise reproduced, UNM will work with the departing research investigator and the investigator's new institution to develop an appropriate plan for access, sharing, and continued use of the research data. The departing research investigator(s) must ensure the proper disclosure and transfer of research data to an appropriate UNM steward (defined in **UAP Policy 2580**) prior to completing UNM's separation process. In cases where a final determination of research misconduct has occurred in accordance with *Faculty Handbook* **Policy E40** "Research Misconduct," it is the decision of the VPR or HSVPR as to what if any research data is appropriate for transfer.

2. Research Data Management

Research data management involves responsible access, use, sharing, privacy, security, confidentiality, maintenance, storage, retention, and disclosure of research data. Ensuring appropriate protection of research data is a fundamental responsibility of all members of the UNM research community and others who may have access to research data. The obligation to protect access to research data is rooted in a commitment to confidentiality (i.e., not breaching the trust of collaborators when results are not yet published); integrity (i.e., maintaining the structural and content consistency of data); availability to authorized users; and compliance with commitments made to human subjects, other research participants, data providers, and users (i.e., through contracts and agreements), applicable laws and regulations related to Controlled Unclassified Information (CUI), contractual terms, and other legal requirements (e.g., data retention requirements, export control laws, Health Insurance Portability and Accountability Act (HIPAA,) Family Educational Rights and Privacy Act (FERPA). The requirements listed in all sections of this Policy must be followed to ensure proper research data management.

3. Rights and Responsibilities

As recipients of sponsored awards, participants in the research enterprise, and stewards of public trust, UNM, its researchers, and other UNM personnel have rights and responsibilities concerning access, use, sharing, privacy, security, confidentiality, and maintenance of research data, both in analog and digital form. In addition to this Policy, other UNM policies, including but not limited to UAP 2580 "Data Governance," relating to the rights and responsibilities of researchers and other UNM personnel related to research data are listed in the Related Documents section of this Policy. "Data Governance" defines specific roles and responsibilities relating to UNM data, including research data. These roles are described in the following

sections. *Faculty Handbook* Standard E30#1 "Research Data Management" is being developed to provide standards and guidelines that ensure compliance with this Policy.

3.1 Researcher

For the purposes of this Policy, researcher refers to a UNM faculty member, staff member, student, or collaborator, who participates in or contributes to research activities occurring at UNM, involving use of UNM resources, or otherwise conducted by or on behalf of UNM, regardless of whether the research is supported by external funds. UNM researchers are expected to pursue their work in accordance with UNM policies, ethical standards, award terms and conditions, and all additional requirements set forth in applicable agreements (e.g., Non-disclosure or Confidentiality Agreements, Data Use Agreements, etc.) that govern research data management. Agreements with collaborators should be developed to ensure compliance with UNM policies. The Office of the VPR or HSVPR can assist the researcher in developing such agreements. Depending on the size and complexity of a specific research project, the lead researcher may serve in multiple roles or solely as a research data steward. Specific research data responsibilities and activities related to these roles are outlined in this Policy.

3.2 Research Data Owners

As the designated officers for research at UNM, the VPR and the HSVPR serve as research data owners for all research data covered by this Policy and have ultimate authority and responsibility for research data management within their respective campuses. Research data owners are responsible for:

- Protecting the rights and welfare of human research subjects from which research data is derived.
- Protecting the rights of UNM researchers as provided in this Policy, including their right to academic freedom and right to access data from research in which they participate.
- Protecting the rights of former UNM researchers to retain access to available copies of research data.
- Developing, implementing, and supporting policies, guidance, training, and efficient processes to ensure:
    - A shared understanding of the rights and responsibilities of all participants in the research process relative to research data.
    - UNM compliance with sponsor terms, conditions, and legal requirements, including public access requirements.
    - Effective investigation of allegations of research misconduct and other UNM compliance and audit reviews that may necessitate access to, sequestration of, and analysis of research data.
- Supporting UNM systems and services that enable researchers to maintain research data throughout the data lifecycle in computing and physical environments that meet tiered computational, privacy, security, and physical environmental requirements based on the nature of the data.

3.3 Research Data Stewards

Research data owners appoint research data stewards who have direct operational-level authority and responsibility for research data management for specific research applications. Principal/lead investigators typically serve in this role. Research data stewards are responsible for ensuring that research data and materials are managed in compliance with this Policy, legal and regulatory requirements, other UNM policies, and contractual requirements on behalf of UNM.

Research data stewards are responsible for:

- Determining the roles and responsibilities of the individuals working on the project.
- Assuring continued stewardship of the project's data in case of a change in project leadership.
- Defining administrative, operational, physical, and technical safeguards to reasonably and appropriately protect research data.
- Defining data management standards, permissions for sharing and access, and procedures that apply to the project's data.
- Developing and implementing a written Data Management Plan (DMP) in accordance with **Standard E30 #1** (under development) Research Data Management, Section 2.1 Data Management Planning. In the case of student researchers or researchers with questions about DMP development, this DMP should be developed in consultation with their faculty advisors, instructors, or campus research data support providers listed in Section 4 of **Standard E30#1** (under development).
- Ensuring that institutional data sharing, preservation, and protection obligations documented in the DMP and other research proposal documents and agreements are met.
- Ensuring that the data are retained and subsequently destroyed in compliance with institutional, legal and regulatory retention requirements.

3.4 Research Data Custodians

Research data custodians are individuals and/or units that provide technical services and infrastructure to support researchers, research data owners, research data stewards, and research data users in meeting UNM research data obligations. As researchers (i.e., research data stewards or research data users) retain responsibility for compliance with all research data obligations. However, if they lack the technical capacity to serve or are legally prohibited from serving in the capacity of research data custodian for their data, they should contact the VPR, HSVPR, or the Director of Clinical Translational Sciences Center (HSC) for other resources to serve in that role.

Research data custodians typically are associated with UNM administrative technical functions but may also include systems administrators within academic and administrative units, or research data stewards themselves in the absence of supporting staff. Research data custodians are responsible for the operation and management of technology, systems, and servers that collect, store, process, manage, and provide access to UNM data. In accordance with directions provided by the research data steward, the research data custodian is also responsible for

ensuring that all research data are:

- archived and stored in a secure and persistent manner,
- accessible only to authorized users,
- secured at rest and in transit,
- securely backed up,
- securely transferred,
- securely destroyed when required.

The research data custodian will provide auditing and logging services on the infrastructure.

3.5 Research Data Users

Research data users are individuals who access UNM data to perform assigned research duties or functions. Lead researchers/principal investigators and other UNM researchers or personnel who create, access, maintain, or store research data and research materials are accountable as research data users. When data have been made publicly available, users of research data may be external to UNM. In reference to research data, UNM co-investigators, collaborating researchers, and students are considered research data users.

Research data users are responsible for:

- The appropriate use, management, and application of privacy and security standards for the data they are authorized to use.
- Collecting, recording, managing, documenting, retaining, and sharing research data and research materials in accordance with the terms and conditions of sponsored awards, UNM policies, and any other legal, regulatory or contractual requirements.
- Complying with the research data management requirements of this Policy and Faculty Handbook Standard E30#1 (under development).

APPLICABILITY

This Policy applies to all members of the UNM community including, but not limited to, faculty, staff, students, visiting scholars, and postdoctoral fellows, and any other persons at UNM involved in the creation, acquisition, modification, access, use, management, sharing, storage, preservation, and destruction of research data at or on behalf of UNM. Collaborating individuals and institutions outside of UNM must agree to comply with the requirements of this and related UNM policies prior to being allowed any access to and/or management of UNM research data. This Policy applies regardless of the source of support for the research project/activity and therefore does not distinguish between externally or internally funded and unfunded efforts.

Revisions to the remaining sections of this document may be amended with the approval of the Faculty Senate Policy and Operations Committee in consultation with the responsible Faculty Senate Committee listed in Policy Heading.

DEFINITIONS

Controlled Unclassified Information (CUI). CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

In the context of UNM research examples include, but are not limited to:

- Personally identifiable information, such as that covered by IRB requirements and PHI protocols.
- Data that is subject to HIPAA and/or FERPA regulations.
- Sensitive information about animal species or archaeological sites.

In some cases, data that are not included in the definition of CUI may be subject to more stringent requirements and regulations. Examples include, but are not limited to:

- Export-controlled data.
- Classified data.
- Data contracted or licensed from third parties.

Data Preservation. The process and practice of placing research data into a designated preservation system that is actively managed to ensure preservation of the deposited data for as long as determined necessary for future potential research, teaching, and other forms of beneficial access and reuse.

Data Retention. The process and practice of securely storing research data in compliance with institutional, regulatory, and sponsor requirements – typically in support of audit or investigative activities, or public records requests.

Data Destruction. The process and practice of securely destroying research data in compliance with institutional, regulatory, and sponsor requirements.

Data Transfer. The process and practice of exchanging data between systems or organizations.

Data Sharing. The process and practice of making research data available to collaborators, other investigators, students, and the general public.

Research. *Basic (or fundamental) research* is experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts, without any particular application or use in view. *Applied research* is the original investigation undertaken to acquire new knowledge directed primarily towards a specific, practical aim or objective. The aims and objectives of applied research may also include innovation and commercialization.

Research Data. The recorded factual material necessary to validate research findings and includes original, primary, and raw data, as well as analyzed or synthesized data, including recordings of such data.

Research Data Lifecycle. All stages of data from creation to destruction. A lifecycle view is used to enable active management of the data objects and resource over time, thus maintaining accessibility and usability.

Research Data Management. Processes concerning access, use, sharing, privacy, security, confidentiality, maintenance, storage, retention, and disclosure of research data that ensure compliance with research data policies, laws, agreements, and regulations.

Source Data. Data or other information necessary to perform the research received from a party external to UNM via a properly executed agreement. Source Data do not include original data generated by UNM researchers or the results of analyses conducted using Source Data.

WHO SHOULD READ THIS POLICY

- Students
- Faculty
- Staff
- Department chairs, academic deans and other academic administrators and executives
- External research collaborators who are provided access to UNM managed research data.

RELATED DOCUMENTS

UNM Regents' Policy Manual
Policy 2.9 "University Archives and Records"
Policy 2.17 "Public Access to University Records"
Policy 5.8 "Intellectual Property"
Policy 5.10 "Conflicts of Interest in Research"
Policy 5.13 "Research Fraud"
Policy 5.14 "Human beings as Subjects in Research"
Policy 5.15 "Use of Animals in Education and Research"
Policy 5.17 "Conflict of Interest Waiver Policy for Technology Transfer"
Faculty Handbook
Section B "Policy on Academic Freedom and Tenure"
Policy C07 "Faculty Disciplinary Policy"
Policy C70 "Confidentiality of Faculty Records"
Policy D100 "Academic Dishonesty"
Policy D175 "Undergraduate Student Conduct and Grievance Procedures"
Policy D176 "Graduate and Professional Student Conduct and Grievance Procedures"
Policy E10 "Classified Research Policy"
Policy E40 "Research Misconduct"
Policy E70 "Intellectual Property Policy
Policy E80 "Conflict of Interest Waiver Policy for Technology Transfer"
Policy E90 "Human beings as Subjects in Research"
Policy E100 "Policy Concerning Use of Animals"

Standard E30#1 "Research Data Management" (under development)

University Administrative Policies

Policy 2200 "Reporting Suspected Misconduct and Whistleblower Protection-Retaliation"
Policy 2300 "Inspection of Public Records"
Policy 2500 "Acceptable Computer Use"
Policy 2520 "Computer Security Controls and Access to Sensitive and Protected Information"
Policy 2550 "Information Security"
Policy 2580 "Data Governance"
Policy 3215 "Performance Management"
Policy 6020 "Records Management, Retention, and Disposition"

UNM Health Sciences Center (HSC) Policies and Procedures

HSC-R-801 PR.1 "Research Data and Materials Retention Policy"
HSC-230 "Electronic Data Storage and Transmission"
HSC-300 "ePHI Security Compliance"
HSC-311 "HIPAA Use and Disclosure of Protected Health Information Policy"
HSC-313 "HIPAA Responding to Breaches of Protected Health Information Policy"
HSC-312 "HIPAA Right to Access of PHI by the Patient Policy"
HSC-310 "HIPAA Right to Request to Amend Designated Record Set Policy"

UNM Data Classification IT Standard:
http://cio.unm.edu/standards/docs/DataClassificationStandard041608r.pdf

CONTACTS

Direct any questions about this Policy or its components to the Office of the Vice President for Research (OVPR) or the Office of the Health Sciences Vice President for Research (HSVPR).

PROCEDURES

1. Stewardship of Research Data

Proper data stewardship is expected of all UNM researchers and personnel and is understood as an iterative, lifecycle-oriented set of actions related to routine data management activities such as:

- Planning; data acquisition, management, and analysis; creating and validating backups
- Ensuring data security
- Sharing data with collaborators
- Generating research outputs
- Publishing results
- Preserving and sharing data
- Retaining data in compliance with institutional, state, federal, and sponsor requirements
- Transferring of research data
- Destruction of research data

Additional, data specific administrative activities such as confirmation that data sharing, retention, destruction and preservation requirements have been integrated into project planning throughout the project lifecycle. A representative set of activities includes:

- Preparation of plans for data management that will meet all relevant requirements, in consultation with campus research support service providers such as the University Libraries' Research Data Services program, Center for Advanced Research Computing, the Health Sciences Library and Informatics Center, and Offices of the Vice Presidents for Research (Main Campus and Health Sciences Center).
- Provision and use of secure storage and routine and verified backup capacity. Definition and validation of routine data backup and recovery procedures.
- Documentation of resources, applications, and methods used for data collection and analysis.
- Preparation of data and documentation in support of data retention, destruction, archiving, discovery, access, and sharing for a specified period of time beyond the close of a research project, and in compliance with IRB and other regulatory and contractual requirements.
- Specification of appropriate access and the necessary security provisions to prevent unauthorized access and use.

Responsibilities of researchers, research data owners, research data stewards, research data custodians, and research data users are delineated in the Policy Statement section above.

2. Research Data Use Agreements

Research Data Use Agreements (DUA) may be required when data will be exchanged with recipients or providers outside UNM. Data may be solely incoming, solely outgoing, or both (incoming and outgoing). The need for a DUA is driven by restrictions on data use required by the sender or the recipient. These include research or sponsored projects involving human subject data (including de-identified data), student data, data from or about populations that are subject to special legal protections, a Limited Data Set (LDS), or Protected Health Information (PHI), as defined in HIPAA and institutional policy, and other classes of protected data.

3. IRB Obligation to Human Subjects

Federal regulations require IRBs to determine the adequacy of provisions to protect the privacy of subjects and to maintain the confidentiality of their data. To meet this requirement, federal regulations require researchers to provide a plan to protect the confidentiality of research data. If the IRB finds that researchers have collected data in a manner noncompliant with their approved protocol, or without proper consent, the IRB is obligated to take action in order to protect the human subjects from which the data was derived. This action may include limiting the use of the inappropriately collected data, appropriate consenting of the human subjects, the destruction of inappropriately collected data, or other measures as determined by the IRB.

DRAFT HISTORY

May 17, 2023 –revised for changes to address campus comments.
March 2, 2023 –revised for changes from 3/1/23 Policy Committee meeting. This draft approved by Policy Committee to go out for campus review and comment.
February 2, 2023 – revised for changes from 2/1/23 Policy Committee meeting.
January 24, 2023 –revised to input changes to address questions raised by Policy Committee.
November 17, 2022 –revised for changes from Policy Committee
April - June, 2022 – Presentations to the HSC Vice President for Research, HSC Faculty Council, HSC IT Executive Council, and Health Sciences Library and Informatics Center all hands meeting.
May, 2022 – Endorsement of the draft policy by the FS Research Policy Committee.
April – May, 2022 – Presentations to the Faculty Senate Research Policy Committee and IT Use Committee.
February 21, 2022 – Revised draft to reflect policy formatting and reorganization and creation of a standards document.
August 12, 2021 – New Policy draft developed by Research Data Committee.

HISTORY

None –New Policy Proposed

Additional Areas for Future Policy and Related Institutional Capacity Development

The following topics should be considered for integration into future versions of this policy, but institutional capacity and/or related policy needs to be developed or reviewed to provide specific requirements in these areas.

- ~~Indi~~genous Data Sovereignty: ~~This~~ version of the policy does not address the data management for Native Americans and indigenous data sovereignty specifically, but instead references the CARE principles (see **Standard EXX#1** Section 3.4) as a reference standard that researchers should be aware of. A broader institutional initiative relating to UNM's adoption and implementation of principles around Indigenous Data Sovereignty should be completed before specific integration into this policy.

- Identification and Development of institutional training, support, and infrastructure to enable researcher compliance with this and related UNM policies, legal, and regulatory requirements.

- Review of related policies to more clearly reflect research data in their language and requirements.

- Specific guidance and requirements around the use of personally owned (as opposed to institutionally owned) computers and related devices in research data creation, management, preservation, sharing, and reuse.