# PURPOSE

Describe the risk categories assigned to research data at WVU and alignment with WVU Information Security policy.

# OVERVIEW and SCOPE

This SOP applies to research conducted under the auspices of WVU. This SOP applies to all University employees, dual assignment employees, sponsored employees/students, and students.

The scope of research activities includes:

Research as defined by the [federal definition of Research,](https://ori.hhs.gov/content/chapter-3-The-Protection-of-Human-Subjects-Definitions) including research designated as Not Human Subjects Research (NHSR).

# PROCEDURES

The WVU Research Office categorizes operational research data based on risk related to the source of the data, federal regulations, and institutional policy. The categories are used to clearly communicate researcher responsibilities associated with the operational research data collected, used, or generated during the conduct of research.

 The table below shows the correlation between the WVU Information Security Policy Data Classification and federal regulations:

|  |  |  |
| --- | --- | --- |
| Research Data Classification | WVU Information Security Policy Classification | Examples |
| High | Sensitive | * WVU Health System EMR PHI
* WVU Health System Coded Data
* WVU Health System Limited Datasets
* PII-Collected by a PI in a WVU Covered Entity
* FISMA
* NIST 800-171
* CUI
* WVU Intellectual Property
* External Source Data Agreement Specifications
 |
| Medium | Confidential | * All funded research data, unless designated as High Risk
* RPII – Collected from WVU Non-Covered Entities
* WVU Health System De-identified Data (Must be provided or verified by WV CTSI)
* External Source Data Agreement Specifications
 |
| Low | Public | * Anonymous
* Anonymized
* De-identified data (not from the WVU Health System EMR)
* Publicly available data
 |

 Identifiable Research Data Variables – Link to Web Page

 Data Types (definitions for anonymous, de-identified, etc.) – Link to Data Types Page

* 1. Active Operational Research Data must be stored using a University approved storage plan based on the risk of the data.
	2. Data must be transferred and/or shared based on the risk of the data. High-Risk data and some Medium Risk data will require a Data Agreement to transfer the data out of the University or to share the data with external parties.
	3. The risk level of the data must be managed appropriately throughout the research life-cyle by the PI.

REFERENCES

Research Office SOP RDM 001 Research Data Management & Protection at WVU

Research Office SOP RDM 002 Use of WVU Health System Medical/Dental Records

WVU Information Security Policy

WVU Data Classification Policy

**History of Revisions to SOP**

|  |  |  |
| --- | --- | --- |
| Effective Date | Nature of Revision(s) | Name |
| 6/7/23 | Created the new SOP | R. Casteel |