Are My Data Safe?

Jonathan Wheeler* Karl Benedict†

03/30/18

Principles[1]

Confidentiality

Information requires protection from unauthorized disclosure.

Integrity

Information must be protected from unauthorized, unanticipated, or unintentional modification.

Availability

The system or data must be available for use for intended purposes.

A System View

Component	Strategies & Considerations
storage	replicated, verified backups
access	physical controls, strong passwords, two factor authentication
transmission	secure transmission
encryption	file and volume level encryption

Regulatory Compliance

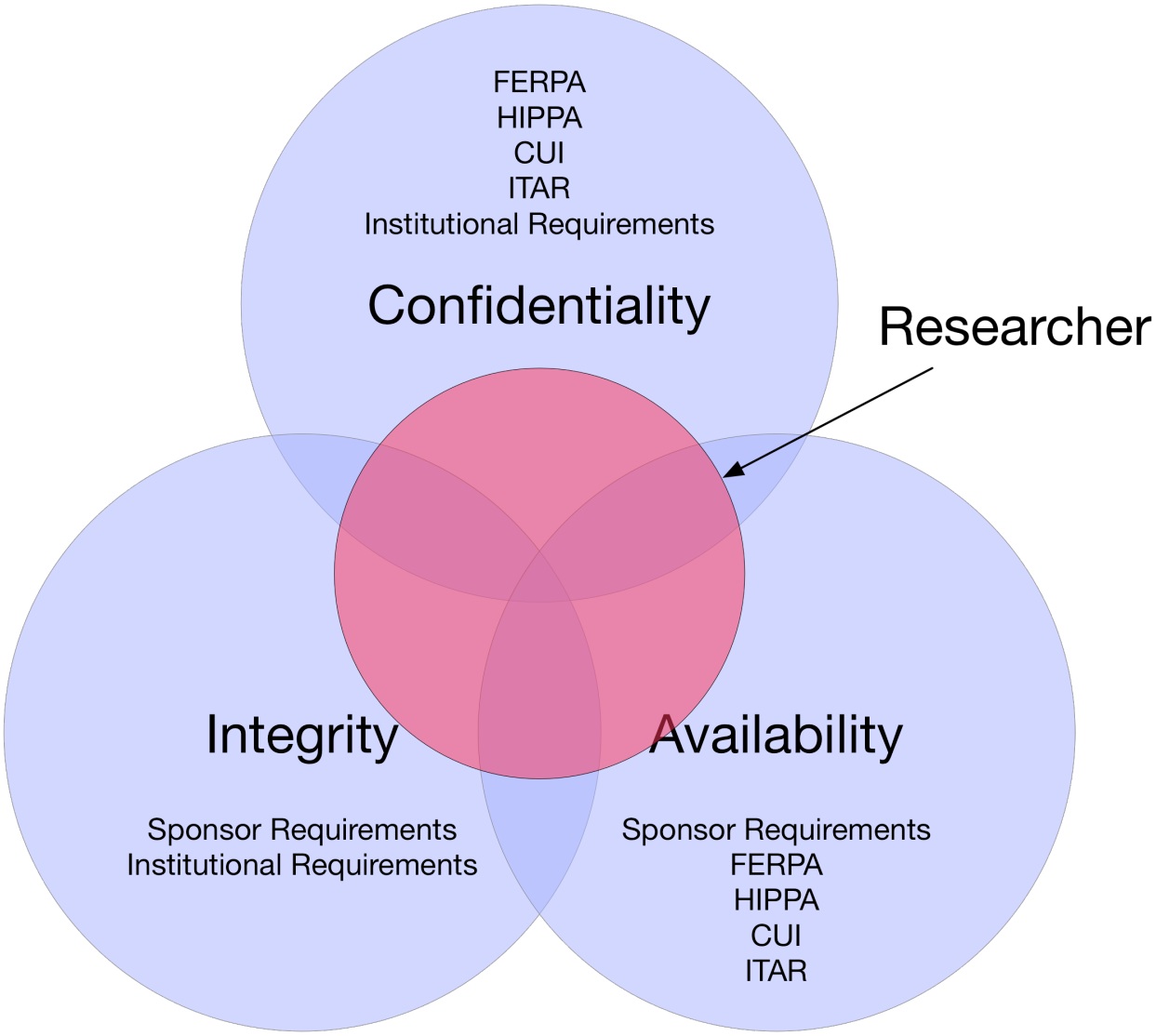
- FERPA
  - Protecting Student Privacy
  - Data De-identification: An Overview of Basic Terms
- HIPAA
  - Summary of the HIPAA Security Rule
- Controlled Unclassified Information (CUI)
  - CUI Registry - Categories and Subcategories
- ITAR & Export Control
- NM State
- Sponsor requirements
- Institutional requirements (reflecting both regulatory and institutional needs)
  - Research Misconduct
  - Information Security

*UNM Research Data Services, jwheel01@unm.edu

†UNM Research Data Services, kbene@unm.edu

[1]Swanson, M., & National Institute of Standards and Technology (U.S.). (2001). *Security self-assessment guide for information technology systems* (NIST special publication ; Computer security, 800-26; NIST special publication, 800-26; NIST special publication, Computer security.3223114). Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology. http://books.google.com/books?id=-AVRAAAAMAAJ

A Synthesis



Download this document: https://unmrds.github.io/bb-security/bb-security.pdf
Github Repository: https://github.com/unmrds/bb-security
