



Proposal
Submission

Award and Account
Establishment

After Research
Commences

Closeout

REQUIREMENTS FOR NIH CONTROLLED-ACCESS DATA

NIH has established heightened security and operational standards to ensure that controlled-access research data (“CADR”) is appropriately safeguarded by eligible NIH-supported repositories. All users of CADR data must implement required cybersecurity measures prior to downloading data.

Full list of CADRs, additional information and resources: [CADR Resources](#).

KEY POINTS

- Applies to all 43 Controlled-Access Data Repositories
- Security baseline is NIST 800.171 (110+ heightened security controls)
- CADR requests will have associated costs moving forward related to compliant data storage
- Recommended Practice: Budget for repository expenses in grant proposals

AVAILABLE SERVICE PROVIDERS

USC:

- Keck Managed Services
- CARC
- LONI (For LONI Researchers Only)

External:

- [AnVIL](#)
- [BioData Catalyst](#)

As more environments are made available, this list will be updated.

WHO TO CONTACT

For Data Environment & IT Director

Questions: USC Office of Cybersecurity (security@usc.edu)

For Compliance and Service

Questions: Office of Ethics and Compliance (OEC) (cullenm@usc.edu)

For Attestation Questions: USC

Stevens Center for Innovation (syedajaf@usc.edu)

