SCU | Southern California University of Health Sciences

Data Management and Security Policy

Policy Statement

Southern California University of Health Sciences (SCU) is committed to collecting, handling, storing, accessing, and using research data properly and securely. This policy establishes the responsibilities of all users in supporting and protecting the research data at SCU regardless of user's affiliation or relation with SCU, and irrespective of where the data are located, utilized, or accessed. All members of the SCU research community have a responsibility to protect the confidentiality, integrity, and availability of research data in accordance with federal laws and regulations, as well as any contractual obligations in conducting research.

Definitions

Electronic Research data are defined as: "the recorded factual material commonly accepted in the scientific community as necessary to validate research findings" (OMB Circular A-110[1], regarding intangible property). Research data includes the protocols, numbers, charts, and graphs used to collect and reconstruct data. The term "research data" refers to both electronic (such as computer software, digital storage, digital images), and hard-copy (such research notebooks, photographs, etc.) formats. As research data cover a broad range of types of information, researchers must keep in mind that privacy will vary widely and must always in compliance with the specific funding agency.

This policy applies to all research data usage, irrespective of format, and storage by faculty, staff, students, researchers, or other users of information technology (IT) resources that connect to SCU networks, and/or store or transmit SCU research data.

This policy does not apply to:

- Preliminary analyses, drafts of scientific papers, plans for future research, peer reviews, or communications with colleagues
- Physical objects (e.g., laboratory samples)
- Trade secrets, commercial information, materials necessary to be held confidential by a researcher until they are published, or similar information which is protected under law
- Personnel and medical information and similar information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, such as information that could be used to identify a particular person in a research study
- Data or records that are personal property of a member of the SCU community, research data, or data created and/or kept by individual employees or affiliates for their own use
- University data that has been de-identified such that it may be classified as Internal or Public

[1] https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-110.pdf

16200 Amber Valley Drive | Whittier, California 90604 | 1-562-947-8755 | scuhs.edu

Procedure & Responsibilities

Functional units are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of data in compliance with this policy. SCU Health Sciences Research (HSR) unit is responsible for managing and maintaining the security of the research data, IT resources, and protected information resulted from research projects under its management.

Research administration at SCU supports research that contributes to the value of health care in the United States, while taking care to respect personal privacy, safeguard the confidentiality of data and to provide a secure environment for data under its management. We meet this commitment by ensuring data anonymity; maintaining principles and policies for the protection of health care data including strict policies which limit access to data and heightened security measures according to both FISMA (Federal Information Security Management Act) and HIPAA (Health Information Portability and Accountability Act) requirements, and assuring that appropriate and current data use agreements, institutional data management reviews and other approvals are in place for research projects.

It is the responsibility of the Principal Investigator, or research data owner, to classify the data, and to manage the access to the research data under their stewardship according to federal regulations and with input from appropriate university administrative units. However, all individuals accessing the research data are responsible for the protection of the data at the level determined by the data owner, or as mandated by law. Issues among research team members involving access, sharing, or use of research data not resolved satisfactorily by the principal investigator will be resolved by the SCU Vice President for Finance and Business Affairs.

"The Federal Government has the right to obtain, reproduce, publish, or otherwise use the data first produced under an award, and to authorize others to receive, reproduce, publish, or otherwise use such data for Federal purposes" (OMB A-110). The SCU researchers are responsible for determining the level of detail needed in all data to be retained and the minimum period of retention based on deadlines specified by sponsoring agencies, or according to federal regulations. All SCU researchers are responsible for being cognizant of any regulatory, intellectual property, export control, and third-party contract issues related to the research data.

SCU researchers with access to sensitive data may be required to sign an internal data use agreement, which outlines expectations and requirements of the individual with respect to confidentiality of research materials and related activities, and which includes specific DUA requirements around data de-identification, CMS suppression policies (if required), DUA scope of work and funding, DUA scope of data access and use, physical security requirements, security awareness, and publication protocols.

Faculty and staff training keeps health information protection matters a constant priority. Specifically, all faculty and staff who are signatories to a DUA - or who signed a signature addendum – are required to be familiar with and adhere to the terms of the DUA. All SCU faculty and staff are required to remain current in CITI trainings on the responsible conduct of research and are required to regularly review and adhere to internal policies to assure alignment with current health information legislation and protection practices.

If a research investigator leaves the University, research data must be retained by the University at an appropriate location, taking into consideration the nature of the research data and the need for access by SCU researchers and others at the University. A departing researcher who wishes to transfer research data from the University may do so if approved in writing by the Principal Investigator, and the Vice President for Finance and Business Affairs. The University will work with the researcher and their new institution to craft an appropriate material transfer agreement (MTA) to transfer the research data when the University determines it is necessary or desirable to have such an agreement due to the nature of the research data. In the unlikely case that the research data cannot be replicated, divided, or otherwise reproduced, the University will work with the researcher's new institution to develop an appropriate plan for access, sharing and use of the research data.

Data Access

All permissions to access confidential data must be approved by the data owner or their designee and a written or electronic record of all permissions must be kept at all times. Private or confidential data shall not be provided to external parties or users without approval from the data owner. In cases where the data owner is not available, approval may be obtained from the Director of HSR.

When an individual who has been granted access to research data changes responsibilities, all their access rights should be reevaluated and any access to protected data outside of the scope of their new position should be revoked.

Data Backup

Research data that are critical to the mission of the university shall be located, or backed up, on centralized servers or other campus-wide approved backup solutions, unless otherwise authorized by the data owner, or the Director of HSR. Research data that is transmitted without encryption may be intercepted, all private and confidential data shall only be transferred through encrypted channels. This may include secure socket layer (SSL), secure shell (SSH), virtual private networks (VPN) or other encrypted sessions

Destruction of Data

Once the research data is no longer needed the data shall be destroyed in a manner that guarantees that it cannot be recovered. Destruction can be done through wipe utilities or physical destruction of the storage device.