THE ODUM INSTITUTE

FOR RESEARCH IN SOCIAL SCIENCE

Odum Institute Data Archive
DATA SECURITY GUIDELINES

Introduction

The challenges of handing data produced from research involving human subjects require that Odum Institute Data Archive staff understand the issues surrounding confidential data and the ethical and professional responsibilities for implementing all necessary measures to protect against unauthorized disclosure of personally identifiable information and protected health information. Along with specific training on the handling of sensitive materials, all staff members are required to successfully complete the University of North Carolina Human Research Ethics Training prior to assignment of archival workflow tasks. Odum Institute Data Archive systems and workflows are designed to uphold all applicable laws and regulations governing the protection of human subjects.

Laws and Regulations

The Odum Institute Data Archive and its systems and processes are bound by the University of North Carolina Information Technology Services (UNC ITS) Information Security Policy and all other applicable ITS policies and guidelines for the storage, management, handling, and transmission of data.

In addition, the Odum Institute Data Archive recognizes the laws and regulations that govern the disclosure of personally identifiable information and that establish obligations of both researchers and data repositories to protect against breaches of confidentiality. Applicable laws and regulations include:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Privacy Act of 1974
- Freedom of Information Act (FOIA)
- Code of Federal Regulations on Protection of Human Subjects (Common Rule: 45 CFR 46; 21 CFR 56)
- Gramm-Leach-Bliley Act
- Other common and codified laws addressing invasion of privacy and defamation

The Odum Institute Data Archive acknowledges that certain customs and traditions outside of codified laws and regulations may dictate acceptable uses of data produced by, about, or in some communities. In these cases, the Odum Institute Data Archive applies all applicable data security measures to respect these customs and traditions.

Applicable Data

Data that fall under the provision of these laws are those that contain personal identifiers, or any information that could be used to directly or indirectly link the data to individual subjects, their relatives, employers, or household members. Personal identifiers are:

- Names
- Geographic subdivisions smaller than a state
- Zip codes
- All elements of dates except year directly related to an individual, including birth or death or dates of health care services or health care claims
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary identifiers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URL)
- Internet protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images
- Any other number, characteristic or code that could be used by the researcher to identify the individual

Note that confidentiality laws and regulations do NOT apply to:

- Dissemination of information that does not describe human subjects
- Information that cannot be directly or indirectly linked to individual subjects

In addition, these laws and regulations do NOT restrict the release of personally identifiable data for which any of the following hold true:

- All the information in the data has been previously released, or its release would not constitute a potential unwarranted invasion of personal privacy (e.g., information in data about identified living persons who are public figures, and where the data relates to their public roles or is not particularly sensitive)

- A sufficient length of time has passed since the collection of the information so that the data can be considered "historic"
- All identified subjects have given explicit informed consent allowing the public release of the information in the dataset
- All the information was collected with an explicit statement concerning the public nature of the data, such as information collected for governmental regulatory purposes
- For federal records (data created by a U.S. federal government agency or under a federal contract), all identified subjects are deceased and no federal statute explicitly restricts the release of the data

Adherence Measures

To adhere to these laws and regulations, the Odum Institute Data Archive employs several techniques to manage disclosure of confidential information. These practices are:

- **De-identification.** The Odum Institute Data Archive Data Deposit Agreement and UNC Dataverse Terms of Use stipulate that prior to deposit into the Archive, all data must be de-identified in such a way that direct and indirect identifiers are removed or modified so that individuals are not identifiable in the data. The Archive may perform de-identification processes on data that are determined to have significant value to the designated user community.
- **Statistical Disclosure Control.** To complement de-identification, the Odum Institute Data Archive uses statistical techniques such as permutation, introduction of random noise, cell suppression, and observation censoring to further ensure individuals are not identifiable in the data.
- **Usage Restrictions.** In cases for which de-identification or statistical disclosure techniques compromise the research utility of the data, or for data that do not contain direct or indirect identifiers but are still considered to be sensitive in nature, the Odum Institute Data Archive sets and enforces explicit usage restrictions. These restrictions may include access limited to authorized users, relegating use of the data to specific locations or for a predetermined duration, or other terms of use depending on the needs of the data.

Policy Protections

Contributors to and users of the Odum Institute Data Archive must agree to the UNC Dataverse Terms of Use policy which describes allowable and limitations on uses of the Odum Institute Data Archive services. This policy, which has been vetted and approved by the University of North Carolina at Chapel Hill Office of University Counsel, binds users to all applicable local, state, national, and international laws and regulations governing the handling of confidential data. Prior to submitting data to the Odum Institute Data Archive, users must confirm that they have read, understood, and agreed to the Terms of Use.

Technological Protections

The technological systems that support the Odum Institute Data Archive incorporate measures to ensure that data are stored securely with safeguards in place to protect the integrity of the data

and to prevent corruption or loss. Odum Institute Data Archive systems include the following technological protections:

- System Security. System security is achieved by employing several techniques that include secure private networks for administration, automated vulnerability scans, encryption for logins, and automated intrusion detection and monitoring.
- Diversified Backup System. A combination of full and incremental backups is performed on all content on a regularly scheduled basis. Backup copies of data files are distributed among local storage sites as well as geographically distributed sites.
- Data Migration. An annual review of Archive systems and content is conducted to determine the necessity of hardware and software migration. Migration decisions are informed by the requirements of the designated user community for content access and use. Criteria for migration also include longevity and viability of new media, and susceptibility to physical damage. Processes are in place to protect against the modification of original content during migration.

Guidelines Review

The Odum Institute Data Archive Data Security Guidelines are subject to three-year review. The current guidelines were approved and issued on May 1, 2017.