Policy:
Adequate research data storage procedures are an essential element of good science practices in the responsible conduct of research. The University Research Council, in February, 2001, approved a set of “best practices” to assure that research data are appropriately recorded, archived for a reasonable period of time, and available for review under appropriate circumstances. This document is available on the VP for Research website at http://www.msu.edu/unit/vprgs/research_data.htm.

Michigan State University’s responsibilities in this regard include, but are not limited to:

- Complying with terms of sponsored project agreements
- Ensuring the appropriate use of animals, human subjects, recombinant DNA, etiological agents, radioactive materials, and the like
- Protecting the rights of faculty, students, postdoctoral scholars, and staff, including but not limited to, their rights to access data from research in which they participated
- Securing intellectual property rights
- Facilitating the investigation of charges, such as misconduct in research and financial conflict of interest
- Responding to legal actions involving the University related to research carried out under its auspices.

Principal Investigators (PIs) of research projects are expected to develop, record, implement, and monitor formal procedures to assure the adequacy of data storage as consistent with applicable federal and University guidelines for research. Per MSU policy (available at http://www.msu.edu/unit/vprgs/research_data.htm), the PI is the custodian of the primary data unless agreed upon otherwise in writing, and is responsible for collecting, managing, and retaining the research data.

I. DEFINITION OF DATA AND RETENTION (STORAGE) OF DATA

Research data (per MSU policy, Research Data: Management, Control and Access; available on the VP for Research website, http://www.msu.edu/unit/vprgs/research_data.htm, “… are defined as the recorded information, regardless of the form of the media on which it may be recorded, necessary to support or validate research findings. Included in the definition of research data are laboratory notebooks, as well as x-ray film, photographs, negatives and slides, print outs, video and audio tape, computers and computer data storage devices, and synthetic compounds, organisms, cell lines, viruses, cell products, cloned coordinates, plants, animals and spectroscope data, however recorded or preserved.

Data storage refers to how research data are retained. Data storage procedures include consideration of the specific ways in which data are stored in order to:

- Retain the integrity (intactness) and security of the data from loss;
- Preserve/assure the confidentiality/de-identification of data as appropriate; and,
- Comply with applicable MSU and federal standards for length of data storage. Data for research conducted as a faculty member or student at MSU is legally owned by MSU.
II. THE PROCESS OF DATA STORAGE

A. External Processes

1. IRB Approval

Permission must be obtained from the appropriate MSU IRB for each key element of the data storage procedures, i.e., Social Science, Behavioral, Education IRB (SIRB) or the Biomedical, Health Sciences IRB (BIRB). The contemporary standard for IRB review is a well-specified, explicit plan for data storage that describes in full where the data will be stored. Any modification of the approved procedures as included in the IRB application requires IRB review, and must therefore be submitted as a revision to the existing approved procedures. The proposed modification to the procedures may not be implemented until IRB review and approval of the change has occurred (failure to do so meets the definition of non-compliance in the Human Research Protection Handbook, available at [http://www.hr.msu.edu/documents/facacadhandbooks/facultyhandbook/protection.htm](http://www.hr.msu.edu/documents/facacadhandbooks/facultyhandbook/protection.htm). Additionally, IRB training requirements by study personnel with access to human subject data must be observed. See CON policy on IRB training requirements.

2. HIPPA Compliance

All HIPPA standards for data privacy, storage and data sharing must be observed.

B. Internal Processes

1. Written Data Storage Procedures

Prior to beginning data collection, the PI and research team should develop a written set of procedures for data storage:

- The written procedures should be written at a sufficient level of detail and clarity that an outside auditor or other researcher could independently verify the specific steps that are used to store the data (see section on Auditing Considerations). These procedures should include the information about data storage procedures that was included in the IRB application for the project, which has been reviewed and approved by UCRISHS, and the funding agency (as appropriate). These should be a formal part of the study procedures manual.
- All staff working with the data for the project should be formally training in the project data storage procedures to be followed, and a written record of the training program completion should be kept on file for each staff member.
- The procedures manual and training of staff in any revised procedures should always be kept completely current at all times and documented as appropriate. All staff should be aware of the location of the procedures manual.
- At least one back up copy of the procedures manual should be retained. The researcher should retain several copies of critical data and address any problems for generating copies in the project procedures manual.

2. Considerations and Procedures for Data Backup

The researcher should propose a specific plan for data backup as part of the IRB application. The same plan should be incorporated into the written procedures manual for the project.

All types of media are prone to deterioration and breakage over time, while electronic media may become obsolete in a relatively short time frame. Therefore, backup plans should take
these factors into account in order to prevent inadvertent loss of data. The table below includes some general considerations for data backup using different types of media. The specific plan for storage and adequate backup will vary depending upon the type of project, and individual needs, but an adequate data storage and backup plan should incorporate backup of data using one or more of the relatively more reliable long term backup systems, as well as use of two or more types of media. For example, a researcher might plan to store data in three forms: computer fixed drive, CD, and computer servers.

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Storage Considerations</th>
<th>Relevant Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper (surveys, transcripts)</td>
<td>Acceptable in short term, but very prone to deterioration over time. Paper copies are not adequate for long-term data storage.</td>
<td>The College has scanners that can be used to convert paper materials to electronic media.</td>
</tr>
<tr>
<td>Audio or video tapes</td>
<td>Acceptable in the short term, but very prone to breakage and obsolescence over time. In addition, there is the risk of accidental tape erasure. Tapes are not adequate for long-term data storage.</td>
<td>Consideration should be given to converting these materials to computerized forms.</td>
</tr>
<tr>
<td>Removable disks (3.5”, Zip, CD, portable plug-in drives)</td>
<td>Prone to breakage and obsolescence over time. Removable disks of various sorts that are fully portable carry the highest risk of inadvertent breakage/damage due to dropping and other misuse. Removable disks are not sufficient as the sole means of data storage, for either short term or long term storage.</td>
<td>If the faculty member does not have access to a rewritable CD drive (CD burner), Health Information Technology staff can copy data onto CDs upon request. CDs are a current state-of-the-art removable disk storage system.</td>
</tr>
<tr>
<td>Computer fixed drive</td>
<td>Prone to breakage and obsolescence over time. Computer fixed drives may malfunction and be fully unusable with little or no prior warning. Not adequate as the sole means of data storage, for either short-term or long-term storage.</td>
<td>Consideration should be given to storing data via multiple types of media.</td>
</tr>
<tr>
<td>HIT servers</td>
<td>Prone to unannounced “down time” due to systems problems. Less prone to obsolescence over time and not as vulnerable to researcher or individual computer breakage.</td>
<td>Health Information Technology staff can arrange for private storage of data in a secured folder on the HIT servers. The researcher can copy to the files stored on a computer server, once the secured folder has been set up.</td>
</tr>
</tbody>
</table>

3. **Frequency of Data Backup**

How often data are backed up varies to some extent with the specific data and the work being done with the data. In general, the more often the data are edited, the more often the data should be backed up. For example, when relatively large amounts of data are being added to a file, it is not excessive to back up the data file after the entry of each record/case. If the data are very critical and even a temporary loss cannot be afforded, it is prudent to back up the data even more frequently. Backups should occur manually for assurance that
planned backups are occurring successfully, even if the computer program has been set to automatic backup.

C. **Access to Data**

The University is accountable for the proper maintenance and availability of primary research data created or collected by University personnel. The following individuals and/or groups may need or be legally entitled to review primary research data well after publication or dissemination of results.

- Sponsors of University research, federal and state oversight agencies, or journals and other colleagues in the field.
- Researchers involved in group investigations have rights to access data gathered by all members of the group.
- The University may be required to review internally the adequacy and integrating of data if findings of University research are called into question, or if violation so of research regulations, e.g., those protecting human subjects of research are alleged.

D. **Auditing Considerations**

University auditors and/or representatives of the funding agency may review research project procedures, including data storage and management procedures at any time. Audits are of two general types: 1) routine/random; and, 2) for-cause, when there is a credible concern or complaint about the research project procedures. The goals of audits are to: 1) monitor research compliance with study procedures, 2) identify deviations from approved procedures; and/or, 3) refer documented violations of approved procedures for further action under University and applicable federal Non-Compliance standards.

E. **Long Term Retention of Data**

The University must retain data in sufficient detail and for an adequate period of time to enable appropriate responses to questions about accuracy, authenticity, primacy and to assure compliance with laws and regulations governing the conduct of the research.

Long term data storage plans need to incorporate considerations of possible faculty or student relocation from MSU. Because MSU owns data from research conducted as faculty member or student at MSU, faculty/students who relocate from MSU must negotiate a revised data storage plan with the MSU IRB. In most instances, with appropriate MSU review/approval, it is permissible for a copy of the data to be taken with the faculty/student to a new institution. In the instance when the PI is still at MSU, a co-investigator or student may take a copy of the data, and the PI will retain the original data at MSU. The Vice President for Research Studies must provide written specific permission for the faculty/student to take data to a new institution.

**Guidelines for duration of retention for funded projects:**

Research data must be archived for not less than three years after the submission of the final project report or publication, whichever occurs last, with original data retained wherever possible. This should include prudent provision of off-site back up of electronic and hard copy data. In addition, any of the following circumstances may justify longer periods of retention:

- Data must be kept for as long as the sponsor specifies in the award agreements.
- Data must be kept for as long as may be necessary to protect any intellectual property resulting from the work.
Data must be kept for 7 years after the last publication or until the faculty retires, whichever is longer.

If any charges regarding the research arise, such as allegations of misconduct in research or financial conflict of interest, data must be retained until such charges are fully resolved.

If a student is involved, data must be retained at least until the degree is awarded or it is clear that the student has abandoned the work.

In most instances, the records will normally be retained in the unit where they were produced. For most projects, the minimum time frame will be 5-7 years. However, many researchers will choose to store research materials indefinitely for projects in which ongoing secondary data analysis is occurring/may feasibly occur.

Incentives paid to research subjects are to be retained for 7 years following payment.

Account ledgers and other administrative paperwork retained in the Research Office are to be retained for 7 years after the final ledger.

Guidelines for duration of retention for non-funded projects:

Copies of unfunded grants are stored in CON for 1 year and then returned to the Principal Investigator. (Note: CGA retains copies of unfunded proposals for 3 years after notification that the proposal/application was not funded.

Guides for destruction of data:

Beyond the period of retention specified here, the destruction of the research record is at the discretion of the PI and his or her department or laboratory. The PI should make a permanent record describing the destroyed data and the destruction date.

F. Ownership of the Data

The University’s claim to ownership and stewardship of the scientific records for projects conducted at the University, under the auspices of the University, or with University resources is based on both regulation (OMB Circular A-110, Sec. 53; 42CFR, Part 50, Subpart A) and sound management principles.

G. Hazardous Waste Storage and Disposal Procedures

Researchers who are dealing with any hazardous materials such as bio-waste, infectious agents, or environmental contaminants, should be familiar with the MSU procedures for hazardous waste storage and disposal. The MSU Office of Radiation, Chemical & Biological Safety (ORCBS) home page may be accessed for information about materials storage safety, available at http://www.orcbs.msu.edu. The MSU hazardous waste disposal policy can be found on line at http://www.orcbs.msu.edu/waste/programs_guidelines/programs_guidelines.htm.