Michigan Education Research Institute Application Guide

Application Overview

The research application is an online form.

Once you start the application, it will automatically save. You may resume the application only from the same IP address within a week of starting.

If more than 7 days pass since starting your application, you should contact meri@miedresearch.org to re-open your application.

Application Requirements

To request confidential data for a new research project, you are required to submit:
1. A completed MERI Research Application Form, including completed data confidentiality and security agreement form(s) and FERPA training certificates for each study team member listed on the project.
2. An IRB approval letter from your institution.
3. If applicable, any letters of support for merging additional data sets to education records.

Please ensure that your application meets the following criteria:

- Each section of the application is completed, with the required forms and supporting documents uploaded. Incomplete forms will result in a return of the application and potential delays in the review.
- Clearly identifies the FERPA exception category, and provides sufficient justification for claiming the exception.
- Clearly identifies why individual-level confidential data is needed instead of publicly available, aggregate data.
- Includes a list of requested data elements, the corresponding data source, years needed, and justification for the data
- Demonstrates a direct relationship between the data elements requested and the research questions posed.
- Is written in terms that may be understood by non-experts. Please do not assume anything is implied, fully explain all requests and justifications. The IRB is comprised of individuals from a range of disciplines who may not be familiar with various aspects of your request.

Please especially note that Researchers who are granted access to confidential Michigan educational records will be responsible for the information obtained, must use it appropriately, and only for authorized purposes. Please see the Data Security section for the expectations that must be met to ensure that all confidential data are appropriately protected.

FERPA Regulations

The dissemination of confidential student level data that may include personally identifiable information (PII) is protected under the Family Educational Rights and Privacy Act (FERPA).

In the event that a research project requires individual student level data FERPA exceptions may be made under certain circumstances.

The FERPA exceptions include the following:

- Auditing or evaluating a Federal or State-supported education program
- Enforcing or complying with Federal legal requirements related to educational programs
- Developing, validating, or administering predictive tests for or on behalf of an educational agency
- Administering student aid programs for or on behalf of an educational agency
- Studies for or on behalf of an education agency, focused on improving instruction

Data requests that include only aggregate data or individual-level staffing data do not have to meet a FERPA exception.

For further explanation of the exceptions listed above please see the following information provided by the US Department of Education:

- Privacy Technical Assistance Center (PTAC) Exceptions Document
- Overview of the Protection of Human Subjects in Research

- If your institution does not provide FERPA training go to the link below, enroll in, and complete the free FERPA course listed on the page. It should take no longer than 1 hour to complete.
  http://www.learnport.org/Compliance-Courses/FERPA-HIPAA

Data Security Checklist

The MERI Research Application requires a formulated data security plan. Use this section to understand the requirements and expectations for protecting the confidential data and enforcing systems for data storage and access.

The list below is comprehensive but not exhaustive. It is the responsibility of each researcher to review institution and Research Collaborative policies and standards for complete guidance on FERPA compliance related to your study specific situation. Additional guidance may be found through the US Department of Education's Privacy Technical Assistance Center (PTAC) http://ptac.ed.gov/

Data Management Plan

Every research project should include a data management plan detailing the following:

Identify all data to be utilized in the study:

- What format will the data come in (csv, txt, etc.)?
- Will the data need to be reformatted for analyses?
- What type of variables are included (numerical, image, text, etc.)?
- What is the classification of each variable (publically available aggregate vs. personally identifiable information [PII])?

What steps are being taken to ensure data remains secure at all times?

- Secure Servers
- Encryption
- Password protection
- Restricted access

If the data will be disseminated:

- What steps will be taken to ensure reporting maintains the anonymity of those included in the data?
- What steps will be taken when reporting involves small numbers of individuals?

Once a project has reached its completion:

- What methods will be taken to dispose of the data? Who is responsible for managing the storage, access, and destruction of the data? Is there a documented procedure for reporting and monitoring each step of the data management process?

Electronic/Device Security

All data stored electronically should be kept on:

- Secure servers maintained by trained systems administration staff
- Encrypted devices (e.g., thumb drives, externals, laptops) with up-to-date endpoint, anti-virus, anti-spyware protection

WARNING: Do not copy confidential data to individual workstations or personal devices.

Physical Security
Make every effort to remove PII from hard copy materials. In the event that PII must appear on hard copy materials, these documents must be:

- Kept in locked cabinets
- Transferred off premise in a secure manner (e.g., locked containers)
- Accessed only by study team members listed on the Research Collaborative IRB application
- Shredded and disposed of through FERPA compliant methods once no longer needed

Machines storing PII data must also have physical security measures:

- All machines must be kept in restricted access, locked rooms.
- Devices that are removable (e.g., thumb drives, DVDs, laptops) must be kept in locked storage within restricted access areas when not utilized.
- All devices must include security programs (encryption, password protection, locking the device after a given length of inactivity).

Access to Data

- Only those staff listed on the Research Collaborative IRB application may have access to the data in any format.
- Access to data is only for those research aims detailed in the Research Collaborative IRB application.
- Transfer of data must be done through secure file transfer and may not be sent to email accounts that are not secure (e.g., Gmail, Yahoo, Hotmail, Comcast).

Managing an Approved Research Project

Once your project is approved, please keep the following guidelines in mind:

- The data are a loan.
- You are not permitted to share confidential, identifiable data with any individual beyond those study team members listed within the application.
- Using the data for any other purpose or research besides the specific research approved by the Committee is not permitted.
- Researchers should not make or allow any unauthorized use of information provided/generated.
- Researchers should not use the results of information provided/generated in an effort to determine the identity of any individual for whom data is included.
- Researchers should not publish reports with a cell size of less than 10. Reports must mask/suppress the data in these cells so that results are not revealed.
- Researchers are required to submit any updated IRB documentation, including continuing reviews for multi-year projects.

- Researchers are required to destroy unit record data that have been provided from the Committee pursuant to a formal agreement within the time limitations defined in the agreement and provide certification to the Committee staff that such records have been destroyed.
- At least 30 days prior to publication/release, provide any documents generated as a result of using data received from the Committee for review and verification that the intended purpose. Additionally, the applicant must include the Committee-provided disclaimer regarding the data and findings
    - The 30 day submission is prior to initiating a dissemination process, meaning prior to submitting a report, manuscript, presentation to a given entity (conference, journal, etc.). Though not typically requested, in the event that the Committee requests revisions to any reports, manuscripts, presentations, etc. designated for publication/release, the applicant(s) must comply with the request and provide proof of the compliance.
    - Research results must include the following disclaimer: "This research result used data collected and maintained by the Michigan Education Research Institute (MERI). Results, information and opinions solely represent the analysis, information and opinions of the author(s) and are not endorsed by – or reflect the views or positions of – grantors, MERI partners or any employee thereof."