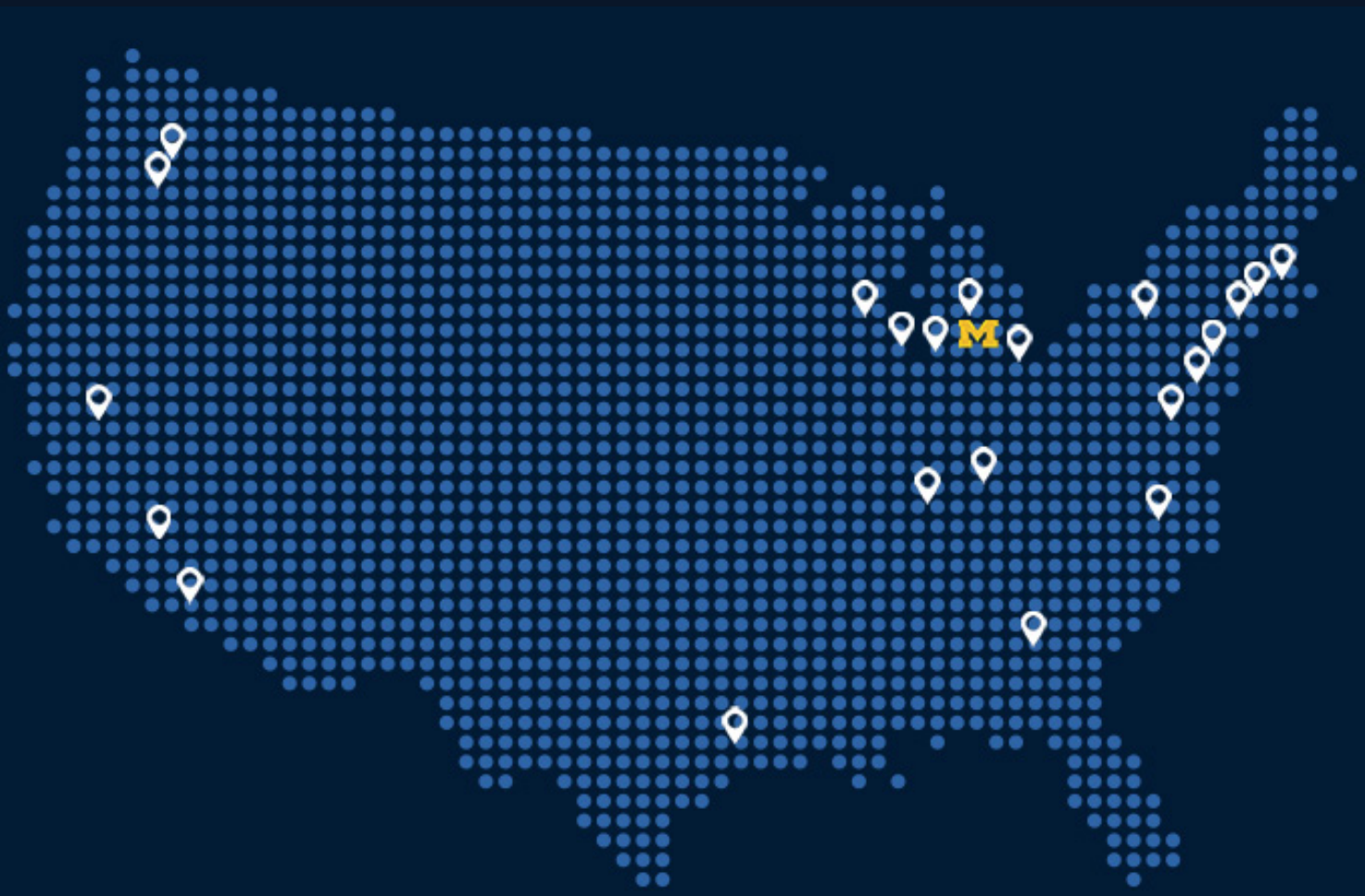

# Michigan Education Research Institute Application Guide

MICHIGAN EDUCATION DATA CENTER
UNIVERSITY OF MICHIGAN

# Contents

# Application Overview

The research application is an online form accessed after you have created an account in Survey Monkey Apply. Once you start the application, you are able to save sections and return at a later time. You are also able to add collaborators to your application. To prepare for completing the application, we suggest clicking through the application, and making sure that you have the following steps completed:

- Review FERPA exceptions and complete FERPA training.
- Ask all members of your research team who will be included as part of this application to complete FERPA training.
- Obtain signed confidentiality and security forms for all research team members included in the application.
- Review application resources provided in this guide.

# Application Requirements

To request confidential data for a new research project, you are required to submit:

1. A completed MERI Research Application, including completed data confidentiality and security agreement form(s) and FERPA training certificate(s) for each study team member listed on the project.
2. An IRB approval letter from the institution where the data will be stored and where the PI has an affiliation.
3. If applicable, any letters of support for merging additional data sets to education records.
4. Name and contact information from IT professional who can confirm that the data protocols are followed and certify data destruction at the end of the study.

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 Review Team is composed 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. See the Data Security Section for the expectations that must be met to ensure that all confidential data are appropriately protected.

# Researcher Eligibility

- MEDC can release data to researchers at an institution of higher education or a non-profit research institution in the United States.
- Researchers requesting data must have their primary affiliation with an eligible U.S.-based institution, or be a currently enrolled student in a doctoral program at an eligible institution.
- Data can only be delivered to the institution where the primary IRB is housed.
- Additional guidelines related to PhD students and postdoctoral fellows are available on the MEDC website.

# FERPA Regulations

The dissemination of confidential student level data is protected under the Family Educational Rights and Privacy Act (FERPA). FERPA exceptions may be made for research projects that require individual student level data. The FERPA exceptions include the following:

- Auditing or evaluating a Federal or State-supported education program Updated June 2023
- 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

We are unable to provide aggregate data at this time. 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 one of the links below, enroll in, and complete the FERPA course listed on the page. It should take no longer than 1 hour to complete.

https://michiganvirtual.org/course/ferpa-family-educational-rights-and-privacy-act/
https://studentprivacy.ed.gov/content/online-training-modules

# 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 institutional and MERI 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): https://studentprivacy.ed.gov/

**Data Management Plan**
Data made available through the Michigan Education Research Institute describe Michigan's children. It is critical that researchers keep data security at the forefront during every stage. Before submitting a research application, researchers should review these guidelines and work with their institution's IT and data security experts to make sure best practices are followed.

- In most cases, the use of cloud storage (e.g., Box, Sharepoint, Dropbox) or local computers will not be approved for data storage. Talk with your institution's IT staff and ask for secured network storage.
- Data must be stored within the United States.
- Describe how account management will be used to ensure only approved users have access to the data. Group-based policies (vs. allowing access on a one-off basis) are preferred. Your institution should have a role in issuing accounts that requires personal information (e.g., date of birth, address) to confirm identity.
- How often will data access be reviewed and updated? Describe how you plan to access and analyze the data. We recommend only using machines or remote desktops that are monitored by your institution's IT staff.
- How will you access data from off-campus? Whatever the answer, it should include the use of a VPN or other means to ensure end-to-end encryption of data.

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

What steps are being taken to ensure data remains secure at all times?
- Secure servers, not stored on the Cloud
- 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 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 identifiers from hard copy materials. In the event that any identifiable information 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 MERI application and IRB
- Shredded and disposed of through FERPA compliant methods once no longer needed

Machines storing identifiable 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 MERI research application and the study IRB application may have access to the data in any format.
- Access to data is only for those research aims detailed in the MERI 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 project 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 MERI 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 MERI pursuant to a formal agreement within the time limitations defined in the agreement and provide certification 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 MERI for review and verification that the intended purpose. Additionally, the applicant must include the required 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 Review Team 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 structured and maintained by the MERI-Michigan Education Data Center (MEDC). MEDC data is modified for analysis purposes using rules governed by MEDC and are not identical to those data collected and maintained by the Michigan Department of Education (MDE) and/or Michigan's Center for Educational Performance and Information (CEPI). 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, MDE and CEPI or any employee thereof"*