CENTER FOR EDUCATIONAL PERFORMANCE AND INFORMATION

PRIVACY AND SECURITY POLICY
Policies and procedures used by CEPI to safeguard education data

Last Updated 11/1/2021

OVERVIEW

Educators, students, parents and policymakers need sound, actionable data to make informed decisions to improve educational opportunities and outcomes. Data help empower parents and the public to hold schools accountable for performance; help educators personalize learning and create dynamic, engaging classrooms; and help ensure states and schools purpose tax dollars toward effective programs and services.

The Center for Educational Performance and Information ensures that effective systems exist to nurture and support these important education data uses and other data-informed strategies to improve education for all students in Michigan.

At the same time, CEPI makes certain that data's incredible educational value is balanced with powerful safeguards that ensure the privacy and security of personally identifiable information (PII). Protecting student privacy is an important responsibility that CEPI takes seriously and requires the same level of diligence from all education data stakeholders and users.

This document addresses the valid public concerns about appropriate access to, and use of, student data; the potential permanence of sensitive, personal records; and other related data privacy and security issues.

This document addresses the important challenges of balancing the educational advantages associated with effective data connections and use with strong privacy protections for PII across the education continuum (P-20) and into the workforce (P-20W).

This document addresses CEPI's education data privacy, access and security as comprehensively as possible, drawing from federal and state laws, terms of use policies, missions and best practices.

This document avoids presenting a one-size-fits-all solution, recognizing the specific context of how data can be used to empower stakeholders about the state of education in Michigan. Access to confidential data is always purposeful, governed by laws, regulated and provided to authorized individuals who work to improve teaching and learning in Michigan, and is tailored to each authorized individual's specific data needs. CEPI's privacy policies are supported with significant investment in training.

This document outlines the strong and comprehensive policies governing education data collection, storage, sharing and analysis to ensure appropriate and effective safeguards for PII, while supporting CEPI's quest to establish a robust, actionable longitudinal data system that addresses today's educational needs while preparing for future needs.

CEPI is chiefly responsible for coordinating the collection, management and reporting of all education data required by state and federal law for preschool, elementary, secondary and postsecondary education (PK-20). CEPI securely stores these data, which can now be joined together, in a common data structure called a longitudinal data system. CEPI adheres to the measures put in place by the state of Michigan to protect records from loss, theft, vandalism, illegal access and corruption.

Whenever possible, aggregate and de-identified data are released instead of PII. All data sharing requests are governed by rigorous approval criteria and requirements to ensure compliance with all laws governing the data. Supplementing the laws are CEPI's policies, overseen by its Chief Privacy Officer, stemming from the core values that protecting students' privacy and data security is critically important and shall always be governed by the Family Educational Rights and Privacy Act (FERPA). Data governance structures are further used to establish and maintain checks and balances of safeguards that are implemented.

WHO WE ARE

CEPI, a division of the State Budget Office in the Department of Technology, Management & Budget, was established under state law (State School Aid Act of 1979 388.1694a). CEPI is chiefly responsible for coordinating the collection, management and reporting of all education data required by state and federal law for PK-20, in a manner that reduces the administrative burden on reporting entities, complies with federal and state privacy laws, and provides data and reports to state and local policymakers and the residents of this state (including parents and other residents/taxpayers and stakeholders in the state).

CEPI is also responsible for the development and implementation of a comprehensive P-20 longitudinal data reporting system and the collection of data necessary to implement the system.

CEPI collects educational data from Michigan's preschools, elementary schools, secondary schools and postsecondary institutions. CEPI collects these data using various web-based applications it maintains with DTMB.

CEPI collects educational data for the following reasons:

- **Funding.** School aid dollars are paid out based on the number of students enrolled in a school, and many federally funded programs are based on the number of students who meet certain eligibility criteria. Roughly $12 billion is paid out annually to schools, based mostly on the data we collect.
- **Accountability.** Are our students learning? Are our schools meeting the educational needs of all students equally?
- **Transparency.** How are our education tax dollars being used?
- **Inform efforts to improve student success.** What policies and programs are most helpful in preparing our students for college and successful careers?

DATA COLLECTION AND USE

CEPI facilitates and streamlines the data collections using a set of secure web-based applications. Only CEPI staff who assist school users with uploading data have secure access to these applications. Schools submit data using such tools as the Michigan Student Data System, Registry of Education Personnel, Financial Information Database, and others. The CEPI website has details about each of these collections.

Only CEPI staff who assist school users with uploading data, or those contracted by the state of Michigan to perform data custodial tasks have secure access to these applications. MDE staff who require the data for decision making have limited access to some parts of the applications as well.

CEPI keeps tight control over who gets secure access to the applications and what user role is required to perform critical job functions. Access to a secure application is only granted based on FERPA-compliant justification, with signatures from the staff member and office director (or other legally authorized representative). Requests are reviewed by both MDE and CEPI personnel with a final sign-off from CEPI's Chief Privacy Officer. Logins, unique passwords, inactivity timeouts, and audit trails are used to further control and protect access. When a person no longer performs critical functions, access is immediately removed. An annual review of access rights is also performed.

The collection applications include demographic data like gender and race, program participation data (e.g., English language learner, special education, migrant or homeless) and attendance. School information such as finances, crime and safety, and directory information is collected. Information about educators such as demographics, teaching credentials and the courses taught is also collected.

In addition, student and teacher personally identifiable information is collected with unique identifier codes to safeguard privacy and ensure data are accurately collected for each individual. PII is any sensitive or non-sensitive data that, alone or in combination with other information, could potentially identify a specific individual. Examples include name, address, date and place of birth. CEPI collects PII to ensure accurate collection of data.

CEPI classifies PII as highly confidential and puts additional security controls on these data. Access to PII requires additional justification, and is restricted to those performing certain

critical functions. When a person no longer performs those critical functions, access is immediately removed. An annual review of PII access rights is also performed.

CEPI assigns and collects a unique/personnel identifier code for all students and educators. This enables names and dates of birth, for example, to be removed from the stored data to safeguard privacy.

All applications and the data collected within them are classified using the state of Michigan Data Classification Standards. As such, the proper security controls are placed onto these data by DTMB and reviewed annually.

Details about the specific data elements collected can be found on the CEPI web pages shown below:

- PK-12th grade
- Postsecondary
- Personnel and staffing information
- School safety practices and incidents of crime
- School directory information
- School expenditures and revenues

These data are required for state and federal reporting purposes such as:

- State aid payments.
- United States Department of Education Consolidated State Performance Report.
- Every Student Succeeds Act, Individuals with Disabilities Education Act, Perkins (Vocational Training).
- Michigan Department of Education's accreditation plan.
- MDE's Educator Preparation Institution oversight and management.

It is important to know the data CEPI does NOT collect:

- Data that don't meet requirements of state or federal law.
- A student's or parent or guardian's beliefs or practices on issues such as sex, family life, morality or religion.
- Political, voting, family financial, biometric or medical records, including information on a students' psychological or emotional state.

To see details about the collections, the quality of the data and their purposes, go to CEPI's How Your Data Are Used web page.

To see how CEPI publicly reports these data, go to MI School Data.

To see examples on how the data are used for auditing or evaluating Michigan education policies, go to MDE and CEPI's research partnership website with the University of Michigan and Michigan State University, called the Michigan Education Research Institute.

CHOICE AND CONSENT

The student and educator records CEPI receives for audit, evaluation, or compliance purposes are required under the State School Aid Act of 1979 and cannot be opted out of. Under this Act, CEPI is chiefly responsible for coordinating the collection, management and reporting of all education data required by state and federal law. To accomplish this, all students and educators in this state must be reported to CEPI. Failure to report these data

would jeopardize school aid funding and prevent students from receiving necessary programs and services. The State School Aid Act of 1979 is cited in the CEPI's collection manuals.

FERPA permits CEPI to redisclose PII from education records without parent/student consent under limited circumstances, commonly known as exceptions. See § 99.31 for the full list of exceptions to the consent requirement in FERPA, which include:

1) an audit or evaluation of Federal or State supported education programs
2) the enforcement of or compliance with Federal legal requirements relating to such programs
3) studies
4) subpoenas
5) when there is a health or safety emergency.

PII DATA QUALITY

Ensuring that accurate data is collected for the correct individual means PII must be accurate. Not only does CEPI strive for data quality assurance, a driving principle behind data collection and use is to "collect once and use many times." This means the data must be accurate at the source. PII can be updated or corrected in the secure electronic collection applications by the data uploaders. Authorized users may identify errors through either CEPI system checks, district system checks or data quality feedback provided to districts by CEPI. This process is explained in the application data collection manuals.

MICHIGAN STATEWIDE LONGITUDINAL DATA SYSTEM

CEPI stores year-to-year data in a common data structure called a longitudinal data system, which joins and securely stores data from multiple sources. CEPI is charged by the state legislature with securely creating, maintaining, and enhancing Michigan's Statewide Longitudinal Data System.

Put simply, a longitudinal data system is a data system that:

1. Stores and maintains detailed, high quality, student- and staff-level data and aggregate data
2. Links these data across entities and over time, providing a picture of academic and performance history for each student, educator or entity
3. Makes these data accessible, at appropriate levels of detail, through reporting and analysis tools

The MSLDS does not *collect* data. Rather, the MSLDS lets us *connect* data in powerful ways—grade to grade, school to school, level to level. It lets us connect seemingly disparate data like school finance, test scores, teacher credentials, student gender and race, courses taken and grades earned, school graduation rates, college enrollment, school lunch eligibility, career and technical education programs, special education and gifted program participation. These connections, which span from early childhood into the workforce, help ensure the state's education system is meeting the needs of *all* Michigan students, and they help evaluators see which policies and programs work.

Besides building, maintaining, and enhancing the MSLDS, CEPI is dedicated to making education data available to the public, education community, policymakers, and researchers

in ways that support sound education decisions while safeguarding student privacy. In all cases, FERPA guides whether, how, with whom, and when we share the data. If data is needed for public accountability and transparency, to inform education policy or to comply with a required law, we release the least amount of detailed information possible.

CEPI has very deliberately made the decision to ensure names are not stored in the MSLDS. Instead, a unique identification code is used to prevent being able to identify an individual student and a personnel identification code is used to prevent being able to identify an individual school staff member.

The MSLDS is not something anyone can just log into or access. The only people with access are those employed or contracted by the state of Michigan who are tasked with loading data into the MSLDS, performing data custodial tasks, and extracting the data to create reports for important education data uses. MDE staff members who require the data for decision making have limited access to some parts of the system as well.

Even for state staff, CEPI keeps tight control on who gets what information, how they receive it, and under what terms and conditions. Access to the MSLDS, like the secure electronic collection applications, is only granted based on justification that is FERPA compliant, with signatures from the requestor and office director (or other legally authorized representative). Reviews of requests are conducted by both MDE and CEPI personnel with a final sign-off from CEPI's Chief Privacy Officer. Logins, unique passwords, inactivity timeouts, and audit trails are used to further control and protect access. When a person no longer performs critical functions, access is immediately removed. An annual review of access rights is also performed.

DATA SHARING WITH OTHER STATE AGENCIES

CEPI shares data with other state agencies. Examples where we receive data *from* other state program areas are:

- Michigan Department of Health and Human Services. By matching student enrollment records against DHHS records of families receiving public assistance, we can let schools know which students are automatically eligible for free or reduced-price meals. This saves schools, families and agencies from cumbersome paperwork. It also ensures that kids are fed and ready to learn.
- MDE. MDE stores its assessment and accountability data in the MSLDS along with data from its Career and Technical Education Information System and the Migrant Education Data System.

Examples where we provide limited data *to* other state program areas are:

- MDE. MDE staff evaluates Michigan's education policies and programs, such as Special Education and homeless programs.
- Michigan Department of Treasury. Treasury receives data on postsecondary progression and completion in order to evaluate the performance of state scholarship and grants programs.
- Talent Investment Agency-Workforce Development. To truly understand if Michigan students are career and college ready, and which policies lead to greatest student success, we need to connect with workforce data. Are they unemployed or gainfully employed? Are our career and technical skills programs meeting employer needs and in line with employment forecasts?

Before any data are exchanged, a formal data sharing agreement or memorandum of understanding is established to ensure compliance with all laws governing the data. Only the minimal data that are required for the program evaluation or audit are shared. If individual-level data must be shared, we remove PII and exchange using only identification codes, if possible.

POLICIES

- CEPI takes protecting students' privacy and data security seriously and requires that same level of diligence of all stakeholders and users.
- CEPI will work to ensure that those with education data access understand their ethical and legal obligation to keep records confidential.
- Release of PII will always be governed FERPA.
- Education data will be safeguarded, and privacy will be honored, respected and protected.
- Access to confidential data will always be purposeful, governed by laws, regulated and provided to authorized individuals with a legitimate educational need who work to improve teaching and learning in Michigan.
- Student information is to only be used by appropriate educational authorities and then, only to serve the best interests of the student.
- PII will only be released to authorized representatives who have received clearance to access the data for a legitimate need to support their professional roles.
- Employees who have student data access will undergo data privacy and security training.
- CEPI will not release any data that identify the names of individual students to the public.
- Role-based secured levels of data access will be enforced and monitored.
- All users no longer needing access to the web-based collection applications or the MSLDS will be removed. CEPI will review user accounts annually.
- All data sharing requests will be governed by rigorous approval criteria and requirements.
- CEPI's data retention and disposal schedule will be followed.
- Data governance structures will be utilized to establish and maintain checks and balances of safeguards that are implemented.
- CEPI will adhere to the measures put in place by the state of Michigan to protect records from loss, theft, vandalism, illegal access and corruption.
- CEPI data are hosted on a secure platform that provides the highest level of security along with backup and disaster recovery capability.
- CEPI uses automatic encryption and Secure Socket Layer (SSL) techniques for data transmissions.
- A designated CEPI Chief Privacy Officer will oversee the privacy and security policies and practices.
- The CEPI Chief Privacy Officer will monitor and update the Privacy and Security Policy annually.
- CEPI may release directory information (e.g., student's name, address, date of birth, dates of attendance, district of enrollment) as requested by human services or law enforcement representatives in accordance with FERPA, which allows for such release without parental consent when it is necessary to protect the health or safety of the student or other individuals.
- Concerns about security breaches must be reported immediately to the CEPI Executive Director and Chief Privacy Officer.

- CEPI does not share or sell any individual level student data with any person or organization seeking to promote their products or services.

PROCESS FOR MAINTAINING THE DATA PRIVACY AND SECURITY POLICY

In conjunction with the U.S. Department of Education's Student Privacy Policy Office, CEPI annually monitors changes in state and federal regulations that are related to data collection and reporting, and updates procedures to address any new requirements and best practices. For instance, in January 2012, FERPA was reauthorized to include additional clarity around and support for the development and use of statewide longitudinal data systems. CEPI's policies and procedures have been reviewed by CEPI's Executive Director and Chief Privacy Officer to ensure that they fully align with these revised federal regulations.

STAFF TRAINING

To minimize the risk of human error and misuse of information, CEPI provides a range of training and awareness lessons for all staff using educational data. Topics range from new laws or modifications to laws as they come into effect, annual policy reviews, refresher trainings, and Q&A sessions. New CEPI employees receive general FERPA training as well as training tailored to their job roles; read and review a series of CEPI, state, and federal confidentiality policies; read and review a series of state IT and information security policies; and sign a security agreement stating they are aware of and will follow all rules related to working with sensitive data. All employees participate in annual FERPA refresher trainings. In addition, ongoing security awareness lessons explain ever-evolving technology threats, along with tactics that help prevent security risks.

DATA RETENTION AND DISPOSAL

The PII that CEPI collects is maintained according to the retention and disposal schedules outlined by Michigan's Records Management Manual. For information defined as "Student Permanent Record" (e.g., demographics, enrollment and academic performance data), CEPI archives this PII and protects it with appropriate technical, physical, and administrative safeguards in accordance with FERPA. For "non-permanent" student information (e.g., audit work papers), CEPI deletes or destroys this information upon expiration of the retention period outlined in the manual.

INTERNAL USE OF DATA

PII from student and educator records that CEPI receives for audit, evaluation, or compliance purposes is not available to all CEPI employees. This information is only available to employees and contract partners who have a reasonable and appropriate need for access to the information in order to maintain the records or to assist in conducting evaluation, audit, or compliance functions.

BREACHES IN SECURITY

Concerns about security breaches must be reported immediately to the CEPI Executive Director and Chief Privacy Officer. If the CEPI Executive Director and Chief Privacy Officer, in collaboration with appropriate members of the department's executive team, determines that one or more employees or contracted partners have substantially failed to comply with the security and privacy policies, appropriate consequences will be identified, which may include termination of employment or a contract and further legal action.

As pursuant of §99.67 of the FERPA regulations, if the USED issues a final agency decision that a third party has redisclosed PII from educational records in violation of FERPA, or has failed to provide the notification required under §99.31(a)(9)(ii) pursuant to §99.33(b)(2) of the FERPA regulations, the state will adhere to the FERPA guidance to not allow the third party or individual team members, as appropriate, access to PII from educational records for at least five years.

USE OF AGGREGATE DATA

Aggregate data is information about groups of students without any identifying information. This is the most common data available to stakeholders (e.g., a report showing the average SAT scores of all Michigan students).

CEPI applies data disclosure avoidance techniques, such as cell suppression, to help prevent situations in which narrowly defined populations produce cell sizes small enough to potentially permit the identification of individuals. Data suppression rules are applied to sensitive data when report settings would yield fewer than 10 students in a given group. Complementary groups may also be suppressed. In some cases, values less than 10 may be shown when there is no risk of identifying individual students.

DISCLOSURE OF DE-IDENTIFIED STUDENT DATA

- **UIC.** A Unique Identification Code, assigned to each student when they begin public school, is used to collect, store, connect, and share student data in a de-identified way. This supports powerful analysis without identifying any student. The UIC lets us follow students through various transition points in their educational lifecycles, including transfers across schools and into college.
- **RIC.** For further protection of individual level data during research for audit and evaluation purposes, a research identification code is used in place of the UIC. This code cannot be matched back to PII without a crosswalk to the UIC, which is heavily protected and secured.

CEPI may disclose de-identified student data to researchers who are auditing or evaluating Michigan education policies. They must follow the process outlined by the MERI Review Committee, which considers and reviews all requests to conduct research using Michigan student or school system data collected by CEPI and MDE. Potential users such as doctoral and master's degree candidates, university faculty, independent researchers, and private and public agencies must submit proposals before receiving data and conducting and publishing their research.

For every data request, the Review Committee defaults to the guidance that if student-level data is requested, the data shared should be de-identified. To accomplish this, the RIC is attached to each education record in a way that prevents any student's identity from being identified.

Those requesting data must meet all the Review Committee's criteria prior to obtaining any de-identified student-level data. One of these criteria is that the researchers have completed training on the ethical and professional standards for protecting human research participants that are either the same as, or equivalent to, the training that CEPI employees complete. To further ensure data privacy and security, staff members from CEPI and/or MDE provide the necessary data to the researchers; researchers do not have direct access to the data.

DISCLOSURE OF PII

In compliance with FERPA, CEPI does not disclose PII from student records unless the disclosure is for one of the limited purposes outlined in FERPA, 34 CFR § 99.31, including the following.

- **Student Transfer and Enrollment**. Student information may be disclosed to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer.
- **Educational Studies**. Student information may be disclosed to organizations conducting studies for, or on behalf of, CEPI and MDE to:

    1) develop, validate, or administer predictive tests
    2) administer student aid programs, or
    3) improve instruction

    Disclosures for the purposes of such studies must ensure that the study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information, the information is destroyed when no longer needed for the purposes for which the study was conducted, and CEPI enters into a written agreement meeting the requirements below.

- **Audits or Compliance Activities**. Student information may be disclosed to authorized representatives in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of, or compliance with, federal legal requirements that relate to those programs. The authorized representative must:
    1) use PII only to carry out an audit or evaluation of federal- or state-supported education programs, or for the enforcement of or compliance with federal legal requirements related to these programs
    2) protect the PII from further disclosures or other uses, in accordance with FERPA
    3) destroy the PII in accordance with FERPA, and
    4) enter into a written agreement with CEPI meeting the requirements below.

REQUIREMENTS FOR DATA SHARING AGREEMENTS TO DISCLOSE PII FOR STUDIES

Prior to sharing PII for purposes of educational studies, CEPI must enter into a written agreement or contract that meets the following requirements:

- Designates the individual or entity that will serve as the authorized representative. If an entity is designated, the agreement must specify the individuals directly responsible for managing the data in question.
- Specifies the purpose, scope and duration of the study and the information to be disclosed. This description must include the research methodology and why disclosure of PII from education records is necessary to accomplish the research. Note: CEPI will not disclose all the PII from its education records; rather, it will determine only the specific elements the authorized representative needs and disclose only those.
- Requires the authorized representative to use PII only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure. Approval to use the PII from the education records for one study, audit, or evaluation does not confer approval to use it for another.
- Requires the authorized representative to conduct the study in a manner that does not permit the personal identification of parents and students by anyone other than representatives of the organization with legitimate interests. The agreement must require the authorized representative to conduct the study to not identify students or their parents. This typically means that the authorized representative should allow internal access to PII from education records only to individuals with a need to know for the purposes of the study, and that the authorized representative must take steps to maintain the confidentiality of the PII at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques.
- Affirms that the authorized representative may only publish results in a way that protects the privacy and confidentiality of the individuals involved. For example, when publishing tables, cell suppression and other methods of disclosure avoidance must be used so that students cannot be identified through small numbers displayed in table cells.
- Requires the authorized representative to destroy the PII from the education records when the information is no longer needed for the purpose specified and must be clear about how the education records will be destroyed. The agreement must identify a specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit. The agreement shall also require the authorized representative to provide written confirmation to CEPI when the education records have been destroyed, per the terms of the contract.
- Documents appropriate technical, physical, and administrative safeguards to protect PII data at rest and in transit. Examples of this include secure-file transfer protocols and hypertext transfer protocol over secure socket layer.
- The agreement establishes policies and procedures to protect PII from further disclosure and unauthorized use, including limiting use of PII to only the authorized representatives with legitimate interests in the research or study.
- Includes a plan for how to respond to any breach in security, including the requirement that any breach in security must be reported immediately to CEPI.

REQUIREMENTS FOR DISCLOSING PII FOR AUDITS, EVALUATION OR COMPLIANCE MONITORING

Written agreements for audits, evaluation or compliance monitoring are like, but slightly different than, agreements for research and studies. These written agreements or contracts must include the following:

- Designates the individual or entity that will serve as the authorized representative. If an entity is designated, the agreement must specify the individuals directly responsible for managing the data in question.
- Specifies the purpose for which the PII from education records is being disclosed and state specifically that the disclosure is in furtherance of an audit, evaluation, or enforcement or compliance activity. The agreement must specify the student information to be disclosed and must include a description of how the student data will be used. The agreement must describe the methodology and why disclosure of PII is necessary to carry out the audit, evaluation, or enforcement or compliance activity.
- Requires the authorized representative to use PII only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure.
- Requires the authorized representative to destroy the PII from the education records when the information is no longer needed for the purpose specified and must be clear about how the education records will be destroyed. The agreement must identify a specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit.
- The agreement shall require the authorized representative to provide written confirmation to CEPI when the education records have been destroyed, per the terms of the agreement.
- Documents appropriate technical, physical, and administrative safeguards to protect PII data at rest and in transit. Examples of this include SFTP and HTTPS.
- The agreement establishes policies and procedures to protect PII from further disclosure and unauthorized use, including limiting use of PII to only the authorized representatives with a legitimate interest in the audit, evaluation, or enforcement or compliance activity.
- Includes a plan for how to respond to any breach in security, including the requirement that any breach in security must be reported immediately to CEPI.

REQUIREMENTS FOR DISCLOSURE OF PII TO EDUCATORS

Michigan's official portal at MI School Data is where educators can go to access education data on their students to help make informed decisions that can lead to improved student success. Before educators can view PII, the following privacy procedures are in place:

- Those in the education community who have a legitimate educational interest may be granted access to their education agency's data.
- Access is granted by the school, district or intermediate school district's leadership, who ensures that the user agrees to comply with proper privacy and security protocols.
- A Secure Report Use Policy is also consented to and accepted as users navigate through various reports. This agreement must be agreed to annually.

MONITORING IMPLEMENTATION OF DATA SHARING AGREEMENTS

In addition to all the precautions addressed above, any data sharing agreement or contract shall also include the following assurance to protect PII from further disclosure and unauthorized use:

- CEPI shall verify that the authorized representative has a sound data security program to protect data at rest and in transmission. This may be addressed through language in the data sharing agreement that states what data security provisions are required, including requirements related to encryption, where the data can be hosted, transmission methodologies, and provisions to prevent unauthorized access. CEPI shall maintain the right to physically inspect the authorized representative's premises or technology used to transmit or maintain data.

CONSEQUENCES FOR FAILURE TO COMPLY WITH DATA SHARING AGREEMENTS

As required by FERPA, if an authorized representative who receives data to perform evaluations, audits, or compliance activities improperly discloses the data, CEPI shall deny that representative further access PII for at least five years.

GOVERNANCE STRUCTURES

CEPI is highly vested in establishing and maintaining checks and balances of privacy and security safeguards. Key governance structures that help accomplish this include:

- **Chief Privacy Officer.** CEPI's Chief Privacy Officer and a staff member are dedicated to privacy compliance and monitoring. Among their delegated authority to enforce the privacy and security policies, their activities include the following:
    - Meet regularly about privacy maintenance and to discuss the tailored needs of data access for specific purposes.
    - Ensure CEPI's data collections, MSLDS implementation and reporting tasks adhere to privacy policies.
    - Maintain familiarity with federal and state privacy laws and regulations, including FERPA, Children's Internet Protection Act, Children's Online Privacy Protection Act, Freedom of Information Act, and related federal and state laws.
    - Serve on the DTMB Information Management Committee, maintaining awareness of current privacy and security and issues within DTMB.
    - Plan and conduct employee training on FERPA and state, department and office privacy and security policies.
    - Update the Privacy and Security Policy annually.

- **P-20 Advisory Council.** The MSLDS has a governance board, the P-20 Advisory Council, whose members are appointed by the State Budget Office Director and who are experienced data leaders committed to protecting PII and helping to ensure a strong and coordinated system of protections statewide. The Council recommends policy items and implications for various MSLDS data items being used for longitudinal analysis; helps establish model data-sharing agreements and memorandums of understanding; and recommends research questions to be addressed via the MSLDS. This is all accomplished with the overarching priority of ensuring the privacy of individual student data is upheld to the highest standards. CEPI's Chief Privacy Officer is an active participant on the Council, to ensure these important privacy, access and security issues receive appropriate attention.

- **Research Collaborative.** Michigan's state-level research collaborative assembles researchers from across the state and the Midwest region to collaborate on and

contribute to the development of a research agenda targeting needs recommended by the P-20 Advisory Council. This group enables the organization of a broad research capacity to address state education policy questions in a coherent fashion. The Research Collaborative oversees several key data tasks: (1) work with the P-20 Advisory Council to set and prioritize a state research agenda; (2) ensure that student, school and system performance are measured meaningfully; (3) build the technical and human capacity to use the data effectively in local education agencies, by research audiences and centrally; (4) review research proposals requiring state data, regardless of funding source; (5) establish guidelines and standards for proposal submission with data requests; and (6) make appropriate research results available to the public through the state's education data portal. CEPI's Chief Privacy Officer is a co-chair on this committee.

TRANSPARENCY AND PUBLIC AWARENESS

CEPI takes great effort to educate the public about the privacy and security measures taken at CEPI to protect the data collected, connected and used. These efforts help to ensure that stakeholders are aware of our policies and procedures so we can all work together toward the goal of ensuring data's incredible educational value is balanced with powerful safeguards that ensure privacy and security.

- Privacy and security policy and procedure materials (e.g., this document and a Frequently Asked Questions document) are posted on the CEPI and the MI School Data websites.
- Terms of Use/Secure Report Use Policies are available on the MI School Data website for all users so everyone can understand the steps taken to keep data private and secure when accessed and used by authorized users with secure logins.
- When new legislation or updated guidance is released at the federal or state level regarding data privacy and security, CEPI makes this information available on the CEPI and MI School Data websites, with information on how CEPI is implementing these changes.
- CEPI relies on our workgroups and partnerships to help disseminate both current and new privacy and security policies and procedures directly to member user groups.

FERPA REQUESTS TO VIEW EDUCATIONAL RECORDS

Under FERPA § 99.10, parents and students may request to inspect and review a student's education records. A FERPA request requires verification of the requester's identity with the school, and the requestor will generally need to come to Lansing to review the records in person, after additional identity verification at CEPI.

QUESTIONS

Questions or concerns regarding these policies should be directed to CEPI's Customer Support Center at cepi@michigan.gov or 517-335-0505 x3. Or, write CEPI's Chief Privacy Officer at:

Michigan Library and Historical Center
702 West Kalamazoo Street, 3rd Floor
Lansing, Michigan 48915