OPI Data Security

December 2014

Agenda

- Introductions
- OPI's Policy
- School District Responsibilities
- Built-in Security features of AIM
- Recommendations on Controlling Access to Data

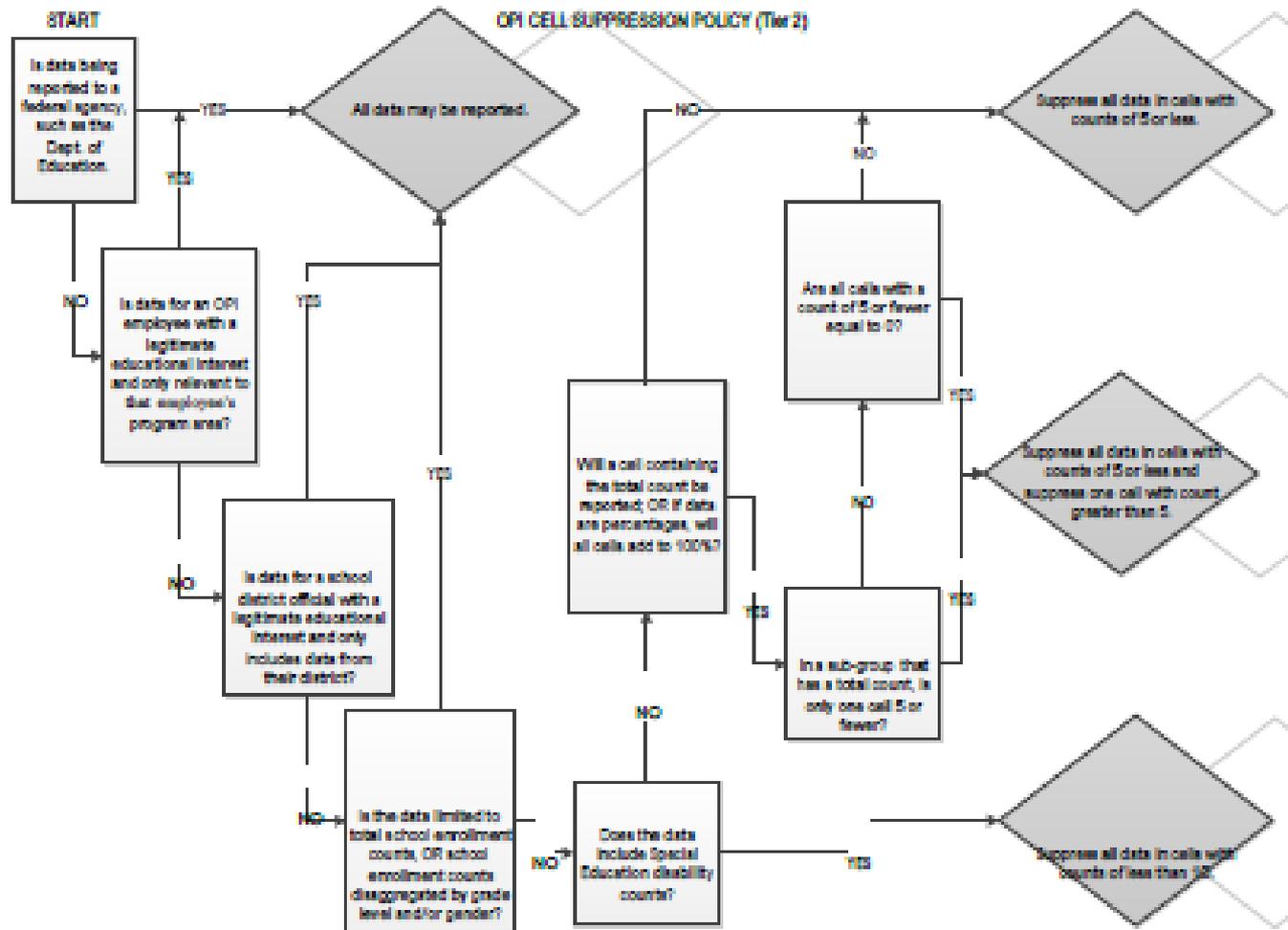# OPI Student Records Confidentiality Policy

This policy is to enforce the procedures and responsibilities governing the access, use and dissemination of confidential, sensitive and/or restricted data by the OPI.

Violation of the OPI Student Records Confidentiality Policy by and OPI employee may result in a formal disciplinary action, up to and including termination, denial of access to sensitive data and revocation of network access privileges.

OPI Student Records Confidentiality Policy cont....

- Definitions

- Cell Suppression

- Data Tiers

- Obtaining Access

- Responsibility for Process

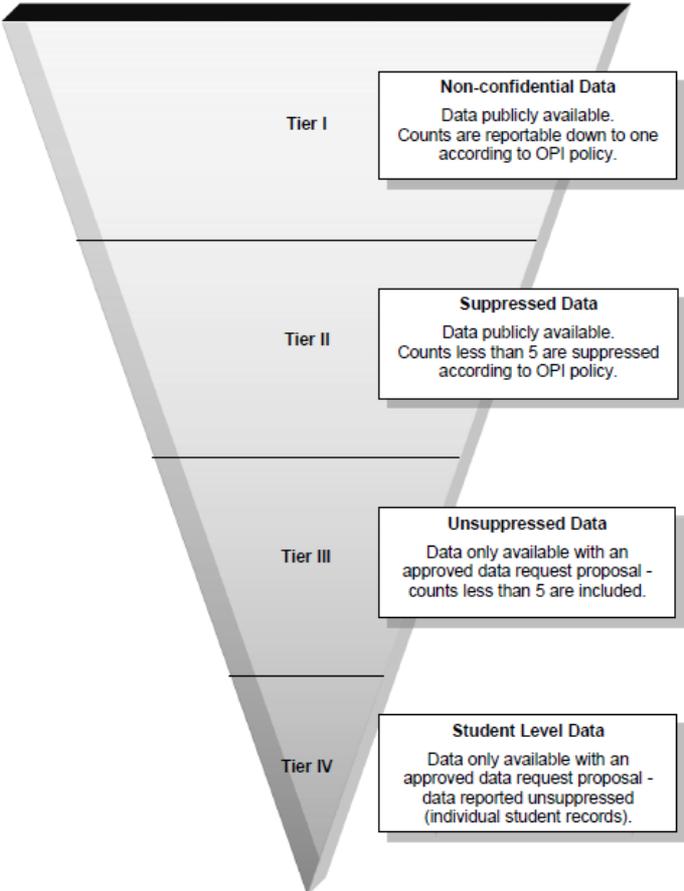- Process for Handling Data requests

Cell Suppression

Data Tiers

Obtaining Access

OPI Staff

- Access to PII shall be granted only to personnel who are authorized by the OPI on a need-to-know basis in the performance of their duties. Access to confidential information carries with it the responsibility to protect the data from further disclosure.

- OPI staff who have a need to access PII in AIM must complete and submit an OPI Employee AIM Access Request Form (Attachment A) and the OPI Confidentiality Agreement (Attachment B) to the OPI Security Officer. The division administrator of the person requesting access to confidential information must sign the form which indicates the person needs access to this information in the performance of his or her assigned duties and responsibilities.

- OPI staff who do not need access to AIM but who need to use PII in the course of their job duties must sign the OPI Confidentiality Agreement (Attachment B).

Responsibility for Process

Protecting Student Data

All agency employees, agents of the OPI, researchers, and other entities with access to confidential student PII are responsible for protecting the data. Measures to protect confidential data include:

- protect visibility of reports and computer monitor when displaying and working with confidential information;

- lock or shutdown workstations when left unattended for any amount of time;

- store electronic data in a password protected, secure location only accessible by the authorized entity;

- protect physical data (including hard copies of reports, storage media, notes, backups) from unauthorized persons and lock up when not in use;

- change data to guarantee anonymity and omit or mask counts less than five if reports containing any confidential student information are used in meetings or presentations, or presented to anyone without authorized access to the information;

- shred paper reports and destroy electronic files (in accordance with the Montana Secretary of State, Local Government Retention and Disposition Schedule) when no longer needed;

- do not fax PII;

- stamp or otherwise mark all reports, CDs, or any other media containing PII (including protective envelopes) as "confidential" prior to being released outside the agency; and

- encrypt email containing PII, or use the file transfer process set up in E-Pass. (Instruction for using E-Pass can be found at https://app.mt.gov/epass/Authn/selectIDP.html.)

Handling Data Requests

Non-OPI staff

- Agent of the OPI - Data collection and analysis for the purpose of fulfilling the objectives of a contract with an agent of the OPI may not be released to any third party, including Contractor's employees, for any other purpose, without written permission of the OPI.

- The agency staff person responsible for contracting with an agent of the OPI to provide a service involving confidential data is also responsible for securing a FERPA Memorandum of Agreement (MOA) with the agent of the OPI to ensure strict confidentiality of the confidential data or PII.

- When an agent of the OPI contracts with another entity (third party) to provide a service involving confidential data, these entities are considered agents for data access purposes. The agency staff person responsible for contracting with an agent of the OPI, must ensure that the third party also enters a FERPA MOA and complies with the same conditions applicable to any agent of the OPI.

School District Responsibilities

Many School Districts have adopted their own policies and procedures

- Examples are Helena and Lewistown School Districts
- US Department of Education has many resources available on State Longitudinal Data Systems & Student Privacy protections under FERPA and State Data Systems & FERPA

Related Policies

- Family Educational Rights and Privacy Act (FERPA) 34 CFR, Part 99
- Release of Information to the Public under the Public Information Act (MCA 2-6-102)
- Montana School Accreditation Standards and Procedures Manual
- Montana Secretary of State Local Government Retention and Disposition Schedule
- Public Law 103-448, Section 9 and 108

Built-In Security Features of the Montana Edition of AIM

- Access Log

- Strong Passwords

- Hide Passwords

- Role Based Access

Access to Data

- Authorized Personnel Only

- Confidentiality Agreement

- Do NOT share passwords

- Protect visibility of reports

- Lock or shutdown workstations

- Shred paper reports

- Encrypt email

- Do not store on removal storage media

- Prepare aggregate reports

- Store paper reports in locked cabinet

- Implement Policies and Procedures

Montana
Office of Public Instruction
Denise Juneau, State Superintendent

opi.mt.gov

AIM Security Presentations

OPI Student Records Confidentiality & Security

http://opi.mt.gov/Streamer/ConfidentialityPolicy/Index.html

School District Responsibilities and Features of AIM

http://connect.opi.mt.gov/p79324089/

Technology and Infrastructure of AIM

http://connect.opi.mt.gov/p74493606/

Montana
Office of Public Instruction
Denise Juneau, State Superintendent
opi.mt.gov

Questions???

- Local School District

- Measurement & Accountability Division
  - Jamey Ereth – 444-4409
  - Sue Mohr – 444-0793

- OPI AIM website – http://opi.mt.gov/AIM