UDS Data Access and Management Policy

Background

The Oklahoma State Regents for Higher Education (OSRHE) manage a unit record database containing public and private higher education institutional data submissions that are used by OSRHE for state and federal reporting, policy analysis, and decision-making.

The Unitized Data System (UDS) contains the following records:

1. S: Student Record,
2. E/M: Enrollment Record,
3. L: Prior Learning Assessment,
4. D: Degrees Conferred,
5. F/X: Financial Aid,
6. P: Professional Staff, and
7. B/R: Facilities Inventory

While each of the records are collected and stored separately, the usefulness of the entire UDS is in the ability to connect data across files to generate complex data sets. These files also can be integrated with other data sets, such as K-12 and employment information.

The System Analysis and Reporting (STAR) division of OSRHE protects the UDS in accordance with the Family Educational Rights and Privacy Act (FERPA). Because the UDS data system contains individual data on students and staff, this policy is subject to both confidentiality and privacy procedures.

Purpose

This policy establishes the principles governing access to and the dissemination of information gathered and maintained through OSRHE's UDS.

Definitions

Confidentiality consists of how personally identifiable information collected by an authorized agency is protected when consent by the individual is required. FERPA guards the confidentiality and access to certain educational records, but not to personal data. To protect confidentiality and privacy of individual records, the individual record is subject to restricted access defined in this policy.

Directory information consists of information contained in an educational record that would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to, the students' date of birth, field of study, dates of attendance, and degrees and awards received.

Educational records are those UDS records directly related to a student and maintained by an educational agency or institution.

Legitimate educational interest, for the purposes of this policy, is an endeavor meant to further the understanding of educational practices, methods, and/or theory that is expected to be analyzed through formal, accepted research practices and the result of which, consistent with FERPA, will be disseminated in such a manner as to benefit the educational community and/or public in general.

Personally identifiable information (PII) consists of information that can be used to distinguish or trace an individual's identity, alone or when combined with other personal or identifying information, which is linked or linkable to a specific individual.

Privacy is the right of individuals to exercise control over the collection, use, and disclosure of personal information.

Research is a formal investigation designed to develop or contribute to generalized knowledge.

Scope and Applicability

This policy shall apply to all data and information products created, collected, and maintained by or for OSRHE's UDS data system, whether in electronic, paper, or other format. When access to information, as it is collected or maintained, is restricted by federal or state laws for confidentiality, privacy, or other authorized purpose, the information shall be processed (e.g., aggregated, summarized, or characterized) as appropriate to provide access while meeting the requirements for restriction. This policy will adhere to restrictions on thee releases of confidential information identified in FERPA, 20 U.S.C. 1232g and its implementing regulations found in Title 34 C.F.R. Part 99, which established restrictions and penalties for the improper release of information contained within a student record.

Policy

Data collected and maintained in OSRHE's UDS data system shall be managed in a manner which will promote access to and dissemination of information that improves the education-related decisions of parents, teachers, administrators, policymakers, educational stakeholders, and the general public.

This policy is designed to keep our data private, trusted, and accessible.

1. **Security** includes the measures in place to ensure that records are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. Since the data are stored on computers, it is essential that there be a high level of protection that provides confidentiality, integrity and availability commensurate with the level of risk and magnitude of harm.

2. **Access** to data is restricted by OSRHE and significantly limits who can view the data and for what purposes. There are four access, each of which is consistent with a specific educational purpose as defined in Section 99.2 of the FERPA regulations.

3. **Disclosure** in summary reports is designed to protect individual data. In cases where populations include only a few individuals, no group smaller than six individuals is reported.

Access Level

To protect confidentiality and privacy, Access Levels are assigned to maximize public usage without risking disclosure of PII.

Level 1 allows authorized OSRHE staff to read and write to all records and fields in the database. This access level is only permitted to a minimum number of authorized staff members who operate or manage the UDS data system or are responsible for maintaining the accuracy and security in the performance of their duties.

Level 2 allows researchers, education groups, and other parties who express legitimate educational interests to have read-only access to all records and fields in the database. This access is granted for the purpose of furthering the understanding of educational practices, methods, or theory through acceptable research practices. These users are not permitted to modify any data and must adhere to all applicable data use agreements and confidentiality standards.

Level 3 allows researchers and professionals who express legitimate educational interests to have read-only access to some records and fields of the database. (The most sensitive data elements, such as names, social security numbers, and other PII, are excluded from access at this level.) Access is primarily granted for purposes like audits, operations, accreditation, and reporting to state and federal government agencies. Authorization is granted solely to support the advancement of knowledge about Oklahoma education and not for commercial use. Researchers must submit a restricted access request form detailing the purpose of the research and the measures that will be taken to ensure data confidentiality and security.

Level 4 allows state government agencies other than OSRHE, as well as state legislators, legislative aides, and members of the executive branch, to have read-only access (excluding all PII and access to individual student or staff records). Authorized users at this level may perform limited data mining of core data sets to generate aggregated reports containing averages or totals related to groups of students or professionals. Because some queries may involve small populations, OSRHE will block any aggregated results where five or fewer students or educational personnel might be disclosed, in order to protect individual privacy, unless otherwise permitted by exception under FERPA[1].

OSRHE provides public-facing dashboards and static reports that include State System aggregate data that align with Level 4 access (e.g., enrollment metrics, degrees conferred, etc.).

Request for Data Access

Pursuant to this policy, researchers, education groups, and other parties who express legitimate educational interests in data, as defined by this policy and consistent with FERPA, may submit requests for access to OSRHE's UDS data system. In reviewing requests for data, consideration is given to access permitted by statute, federal law, privacy concerns, security procedures, availability of staff to monitor the data release, and the perceived benefits of the research. Entities seeking access to OSRHE's UDS data system are required to submit a Data Request Form stating how the data will be used and a description of the data needed. Release of data is subject to approval by and at the discretion of the Chancellor or designee.

Upon request of individuals under Section 552a(f)(1) of the Privacy Act of 1974 or Section 99.20 of FERPA to gain access to their records contained in OSRHE's UDS data system, OSRHE will provide a copy of all or any portion in a comprehensible form and will consider requests to amend the records.

Processing Request

Completed requests will be reviewed and a response provided in an appropriate manner. In the event a request is rejected, specific reasons shall be given and if appropriate, may include information concerning possible alternatives. Requests may be rejected if information on the application form is incomplete.

---

[1] School Official (34 CFR 99.31(a)(1) and 34 CFR 99.33(a)): An Educational Agency or Institution may disclose student PII to a school official if that school official has a legitimate educational interest in the student PII.

Disclosure of Data

Private or confidential data on an individual shall not be created, collected, stored, used, maintained, or disseminated by OSRHE in violation of federal or state law and shall not be used for any purposes other than those stated. If OSRHE enters into a contract with a private person or third party to perform any OSRHE function, that agreement shall require that the data be protected in the same fashion.

Under this policy, no private or confidential data will be released except under the following circumstances as stated in Section 99 of the FERPA regulations:

1. To staff of the higher education institutions who have released the data to State Regents when the determination has been made that there are legitimate educational interests, under Section 99.36(b)(2).

2. To comply with a subpoena or court order, under Section 99.31(a)(9)(A).

3. To honor a request from a judicial order, or an authorized law enforcement unit, or lawfully issued subpoena, under Section 99.31(a)(9)(i). A law enforcement unit refers to all state and local prosecution authorities, all state and local law enforcement agencies, the Department of Corrections, and probation officers who are part of the Judiciary.

4. To educational officials in connection with an audit or evaluation of a federal or state supported education program, under Section 99.32(c)(3).

5. To appropriate parties in connection with an emergency if such knowledge is necessary to protect the health and safety of the student or other individuals, under Section 99.36(a). In cases of health or safety emergency, the request for release must first be directed to the school district that owns the data. The Director, under Section 99.36(a), may also convene a committee to evaluate the request and determine whether or not the person who would receive the information is in a position to deal with the emergency and the extent to which time is of the essence.

6. To research proposals approved by the Chancellor or designee, when a requestor demonstrates a clear legitimate educational interest, provided that PII if discovered is not disclosed to anyone other than the initiator of the request. At the discretion of the Chancellor or designee, any request may be denied.

Data will be disclosed only on the conditions that (1) the party of whom the data are released does not disclose the information to any third party, (2) the data are protected in a manner that does not permit the personal identification of the individual, (3) the data are used solely for the purpose intended, and (4) the data are destroyed when no longer needed for the purposes under which the disclosure was granted.

If it is determined that PII was disclosed in violation of this policy, directly or indirectly, the violation will be reported in accordance with FERPA to the appropriate federal and state enforcement agencies.

OSRHE will account for all disclosures. This includes the date, nature, and purpose of the disclosure, and to whom the disclosure was made. Data access provisions may change at the discretion of OSRHE or if mandated by federal statute, state law, or administrative rules.

Requirements for Security, Privacy, and Confidentiality

Commercial use of data obtained under such a request is prohibited. Recipients **do not** obtain ownership of the data. Such data may not be shared o distributed, and all copies must be destroyed when the researcher completes the analysis or report. Data, copies of data, and all reports must be maintained in a secure environment to prevent unauthorized access. A secure environment includes any electronic media, personal computer, server, or network on which the data reside. Compliance with these security requirements may be monitored by unannounced, unscheduled inspections of the data user's work site by OSRHE staff or designated representatives.

All users of the requested data must submit the Data Request Form that explains how the data are to be stored, used, maintained, and disseminated. When the Chancellor or his designee approves the research proposal request pursuant to this policy, the requestor may be required to forward a copy of any analysis or reports created with OSRHE's UDS data system to the STAR division of OSRHE.