Sharing of Education Data

Data Security Briefing Paper
April 1, 2013

Commitment to Protection

The North Carolina Department of Public Instruction (NCDPI) is committed to protecting all confidential student information for which it is responsible. The Personally Identifiable Information (PII), or private information, collected and used by NCDPI is required and necessary in order to comply with federal or state laws or for other legitimate purposes. NCDPI's data security measures are aligned with both federal and state laws.

Relevant Laws

The Family Educational Rights and Privacy Act (FERPA) [20 U.S.C. § 1232g; 34 CFR Part 99] is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education and restricts the release of private information without the consent of the parent or eligible student.

The Identity Theft Protection Act of 2005 (SL 2005-414/SB 1048), was passed by the General Assembly and imposes certain obligations on state agencies concerning the collection, use and dissemination of Social Security Numbers (SSNs) and other PII.

Internal Use of Private Data

Since the Identity Theft Protection Act restricts the use of SSNs by state government unless "authorized by law to do so or unless the collection of a SSN is otherwise imperative for the performance of the agency's duties and responsibilities by law" [§ 132-1.8.(b)(1)], systems that use SSNs have been steadily eliminated from the NCDPI information system portfolio or modified to exclude SSNs. New systems added to the portfolio are only permitted to capture or retain SSNs by exception.

To minimize the need for the use of SSNs, NCDPI implemented a Unique ID (UID) system for students and staff as part of the NC CEDARS project to create a K-12 statewide longitudinal data system for education data. This system matches individual students and staff and assigns UIDs that are used for data cross-referencing between information systems. As this system was put in place over the past three years, other systems have shifted to using the UIDs for students and staff and dropped their dependence on SSNs as a cross-reference key.

In addition to reducing the use and collection of SSNs, NCDPI has taken other steps to ensure the security of private data when it is used by agency staff. All NCDPI staff members are required to sign a confidentiality agreement annually that is witnessed by their Division Director. The Information Security Officer conducts periodic information security briefings for all staff, which cover the legal

and policy aspects of handling PII. Attendance at one of these briefings annually is mandatory for all employees.

External Use of Private Data

To answer questions about student achievement level and program effectiveness, NCDPI is often asked to provide student level data. Whenever possible, NCDPI refers data requesters to the North Carolina Education Research Data Center (NCERDC), which provides de-identified data sets. When data including PII are required, such as for the Race to the Top (RttT) evaluation, all data releases must be approved by the State Superintendent or her designee. Only requests from researchers conducting studies for, or on behalf of, the students of North Carolina and who have partnered with an internal NCDPI sponsor are approved.

If the data request is approved for PII about individuals, all requesters must adhere to the following requirements:

- Requester is responsible for the information obtained—for using it appropriately, and only for authorized purposes.
- Requester must not use the data for any other purpose or research other than the specific purpose stated in the request.
- Requester must agree to comply with the provisions of the Family Education Rights & Privacy Act (FERPA).
- The NCDPI Standard confidentiality agreement is required for all personnel who have access to the requested data.
- If the requester deliberately or accidentally misuses the obtained information, the requester may lose access to data, and/or face dismissal or prosecution under the scope of all applicable federal and state laws.
- The requester may not share data and information provided by NCDPI with any other entity without prior written approval from NCDPI.
- Data from NCDPI must not be taken outside the United States.
- A Memorandum of Agreement (MOA) between NCDPI and any organization or individuals conducting educational research is required for the release of any PII about individuals. Results will not be displayed or distributed in a breakdown by student group where the number of students in the group is too small (fewer than five). In any group where the percentage of students is greater than 95% or less than 5%, the actual values may not be displayed because of federal privacy regulations (FERPA).
- At the close of the research, the data requester must verify, in writing, that the data set from NCDPI has been destroyed.

References

The Data Management Group (DMG) is the official data management oversight body of NCDPI. The DMG is charged with the responsibility and authority to set policy and resolve issues concerning agency data collection, management, security and use. For more information visit the DMG webpage: http://www.ncpublicschools.org/data/management/

Additional information about FERPA may be found at the U.S Department of Education webpage: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html