Commonly Cited Privacy and Data Security Resources

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of longitudinal data systems. More PTAC information is available on http://ed.gov/ptac.

Purpose

The recent increase in demand for high quality education data calls for greater transparency about the ways these data are collected, processed, stored, and used. Increased scrutiny of education data management practices and concerns about privacy and confidentiality have prompted the U.S. Department of Education (ED) to provide educational agencies and institutions with additional privacy and data security guidance. This paper aims to assist educational organizations by providing a set of useful resources on best practices in privacy and data security.

Resources are organized into two categories: 1) ED Resources on Privacy and Data Security and 2) External Data Security Best Practices Resources. The ED resources section provides a brief overview of the various offices within the Department involved in privacy protection, including their roles and missions. The overview describes the types of issues these offices oversee and provides links to specific resources on their websites. The External resources section lists government and private sector institutions highly regarded for their expertise in the areas of computer technology, data protection, and security. These organizations provide a wealth of information on best data security practices, which can be particularly useful to managers and technical teams responsible for implementing data security strategies and capabilities.

U.S. Department of Education Resources on Privacy and Data Security

Privacy Laws

FERPA: The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, is a federal law that protects the privacy of student education records. FERPA regulations, 34 CFR Part 99, make student education records confidential and provide parents and eligible students with certain rights for inspection and correction. FERPA applies to all schools and educational agencies that receive funds

under an applicable program of ED.

- U.S. Department of Education FERPA Website
  http://www.ed.gov/policy/gen/guid/fpco/ferpa/
- FERPA Regulations
  http://www.ed.gov/policy/gen/reg/ferpa/
- U.S. Department of Education FERPA Final Rule (December, 2011)
  http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf
- FERPA Frequently Asked Questions
  http://www.ed.gov/policy/gen/guid/fpco/faq.html
- FERPA Guidance on Emergency Management
  http://www.ed.gov/policy/gen/guid/fpco/ferpa/safeschools/
- Eligibility Manual for School Meals
  http://www.fns.usda.gov/cnd/guidance/EliMan.pdf
- Balancing Student Privacy and School Safety: A Guide to FERPA for Elementary and Secondary Schools.
  http://www.ed.gov/policy/gen/guid/fpco/brochures/elsec.html

PPRA: The Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. 1232h(a), requires that any material used by students in connection with ED funded surveys, analyses, or evaluations be made available to parents to inspect prior to use. The PPRA, 20 U.S.C. 1232h(b), also requires schools and contractors to acquire written parental consent before a minor student participates in ED funded surveys, analyses, or evaluations on the following subjects:

- political affiliations or beliefs of the student or student's parent;
- mental or psychological problems of the student or student's family;
- sex behavior or attitudes;
- illegal, anti-social, self-incriminating, or demeaning behavior;
- critical appraisals of others with whom respondents have close family relationships;
- legally recognized privileged relationships, such as with lawyers, doctors, or ministers;
- religious practices, affiliations, or beliefs of the student or parents; or
- income, other than as required by law to determine program eligibility.

- U.S. Department of Education PPRA Website
  http://www.ed.gov/policy/gen/guid/fpco/ppra/

Central Privacy Office

In recognition of the explosion of student information and the changing privacy landscape, ED established in 2011 an executive level position for Chief Privacy Officer (CPO) and named its first CPO.. The CPO is responsible for coordinating privacy work across all ED offices, and for providing privacy guidance for ED's programs. The CPO will also be responsible for ED's new initiatives to safeguard

student privacy.

- Announcement of the first Chief Privacy Officer
  http://www.ed.gov/news/press-releases/us-education-department-launches-initiatives-safeguard-student-privacy

FPCO: The mission of the Family Policy Compliance Office (FPCO) includes meeting the needs of the Education Department's primary customers—learners of all ages—by administering two laws that seek to ensure student and parental rights in education: the Family Educational Rights and Privacy Act and the Protection of Pupil Rights Amendment.

FPCO reports to the CPO.

- FPCO Website containing information on the Family Educational Rights and Privacy Act and the Protection of Pupil Rights Amendment
  http://www.ed.gov/policy/gen/guid/fpco/

PTAC: The Privacy Technical Assistance Center (PTAC) is a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC offers technical assistance to state education agencies, local education agencies, and institutions of higher education related to the privacy, security, and confidentiality of student records. It accomplishes its mission through

  - site visits;
  - regional meetings;
  - privacy and security practice presentations;
  - privacy toolkit containing best practice guides and related resources;
  - data security policies, procedures, and architectures reviews;
  - data security audit assistance;
  - frequently asked questions and answers commonly requested by PTAC stakeholders; and
  - help desk support on data privacy and security questions.

- PTAC Website
  http://nces.ed.gov/programs/ptac/
- PTAC Privacy Toolkit
  http://nces.ed.gov/programs/ptac/Toolkit.aspx

Privacy Safeguards Program

ED's privacy safeguards program is an internally focused effort designed to foster the appropriate handling and protection of personal information at ED. This is done through

- coordinating policy development and implementation across ED;
- providing employee outreach and training;
- providing technical guidance to program officials;
- working closely with the Office of the Chief Information Officer to integrate safeguards for data protection and system security; and
- participating in government-wide adoption of best practices.

The Privacy Safeguards Division reports to the Office of the Chief Privacy Officer.

- Privacy Safeguards Program Fact Sheet
  http://www.ed.gov/about/offices/list/om/onboard/docs/pspfactsheet.pdf

Data Security

The Office of the Chief Information Officer (OCIO) advises and assists the Secretary and other senior officers within ED in acquiring information technology and managing and securing information resources. The OCIO helps these leaders to comply with the best practices in the industry and applicable federal laws and regulations, including the Clinger Cohen Act, the Government Paperwork Reduction Act, and the Federal Information Security Management Act. Under the Chief Information Officer, the Chief Information Security Officer (CISO) is responsible for developing and managing security solutions that protect ED's information systems and data. Working with organizations across the Department, and with other federal agencies, the CISO is responsible for developing a security strategy and architecture, developing security policies, and monitoring and assessing security performance.

- Office of the Chief Information Officer Website
  http://www.ed.gov/about/offices/list/ocio/

Restricted Data Licenses

The Institute of Education Sciences (IES) uses Restricted-Use Data Licenses as a mechanism for making confidential data disseminated by the National Center for Education Statistics available to qualified researchers. The goal of this initiative is to maximize the use of statistical information, while protecting confidential information information from disclosure. An on-line application system is available for organizations interested in obtaining restricted-use data. The Electronic Application System facilitates the restricted-use data application process, explains the laws and regulations governing these data, and serves to process users' requests for license amendments. Additional information about the licensing process can be found in the Accessing and Using Restricted-Use Data FAQ , Licensing Procedures FAQ, and IES Restricted-Use Data Procedures Manual. Remaining questions can be answered by sending an email to IESData.Security@ed.gov.

- IES Data Security Office Website
  http://nces.ed.gov/statprog/instruct.asp

Statewide Longitudinal Data Systems Program Support

The Statewide Longitudinal Data Systems (SLDS) Grant Program, as authorized by the Educational Technical Assistance Act of 2002, is designed to aid state education agencies in developing and implementing longitudinal data systems. These systems are intended to enhance the ability of states to efficiently and accurately manage, analyze, and use education data, including individual student records. The data systems developed with funds from these grants should help states, districts, schools, and teachers make data-driven decisions to improve student learning, as well as facilitate research to increase student achievement and close achievement gaps. All states, including non-grantees, have access to a variety of support resources. These support resources are designed to help states with a variety of issues related to longitudinal data systems, including assessment issues, data governance, interoperability, data sharing, teacher-student linkages, external evaluations, and research.

- SLDS Resources Website
  http://nces.ed.gov/Programs/SLDS/resources.asp

National Center for Education Statistics Technical Briefs

Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records
http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011601

This technical brief discusses basic concepts and definitions that establish a common set of terms related to the protection of personally identifiable information, especially in education records in the Statewide Longitudinal Data Systems. The brief also outlines a privacy framework that is tied to Fair Information Practice Principles that have been promulgated in both the United States and international privacy work.

Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records
http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011602

This technical brief focuses on data stewardship, which involves organizational commitment to data management in a way that ensures privacy, confidentiality, and security of personally identifiable information throughout all stages of data lifecycle, from planning and collection to use and dissemination. The brief reviews internal control procedures that should be implemented to protect personally identifiable data, including workforce security, role-based access to student records, and the handling of data breaches. The discussion concludes with a review of accountability and auditing procedures necessary to ensure that data stewardship principles have been successfully implemented.

Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting
http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011603

This technical brief examines what protecting student privacy means in a reporting context. To protect a student's privacy, the student's personally identifiable information must be protected from public

release. When schools, districts, or states publish reports on students' educational progress, they typically release aggregated data–data for groups of students–to prevent disclosure of information about an individual. However, even with aggregation, unintended disclosures of personally identifiable information may occur. Drawing upon the review and analysis of current practices, the brief provides a set of recommended rules for public reporting of percentages and rates used to describe student outcomes to help ensure that intended protections are successful and the utility of the reported data is retained.

External Data Security Best Practices Resources

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is the leading provider of data security standards and information for the federal government. Although the Institute's information is targeted to U.S. federal agencies and departments, guidelines and standards established by NIST are often recognized internationally and used by governments and private sector organizations world-wide. The NIST website and publications provide a wealth of information on best practices in electronic data security and Federal Information Processing Standards.

- NIST Website
  http://csrc.nist.gov/
- Recommended Security Controls for Federal Information Systems and Organizations 800-53
  http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

Department of Homeland Security

The Department of Homeland Security's Computer Emergency Response Team's (DHS US-CERT) website provides a wide variety of free reports and guidelines for both individual users and enterprises. In addition to general information on best practices in computer security, including internet connection, spyware, home network, and web browser security, US-CERT offers a long list of technical documents on highly specialized topics, such as protecting aggregated data. US-CERT also offers a free subscription to the mailing list that alerts organizations and users to the latest internet vulnerabilities and threats.

- DHS US-CERT Website
  http://www.us-cert.gov/

Carnegie-Mellon: The Computer Emergency Response Team

The Computer Emergency Response Team (CERT), located at the Software Engineering Institute of the Carnegie Melon University, is dedicated to training and educating computer security professionals in a

variety of disciplines. CERT's website provides a wealth of free information on a variety of technical topics in information security, including building an incident response capability; software assurance and secure coding; threat and risk assessments; monitoring, detection, and defending against insider threats; and many others.

- Carnegie-Mellon CERT Website
  http://www.cert.org/

National Initiative for Cybersecurity Education

The National Initiative for Cybersecurity Education (NICE), established in 2010, has evolved from the Comprehensive National Cybersecurity Initiative and extends its scope beyond the federal workplace, by including civilians and students in kindergarten through post-graduate school. The goal of NICE is to establish an operational, sustainable, and continually improving computer security education program for the nation to use sound information management practices that will enhance the nation's security.

The purpose of the NICE website is to provide up-to-date information on computer and electronic data security, including expert commentary and advice; links to educational materials and programs at all levels; and learning events and workshops. It also provides opportunities to share best practices in use at state and local levels and across federal agencies, as well as grassroots news and activities.

- NICE Website
  http://csrc.nist.gov/nice/

System Administration, Networking, and Security Institute

Focused primarily on training, the System Administration, Networking, and Security (SANS) Institute is a leader in cultivating computer and electronic data security professionals through internationally recognized certifications. SANS website offers a great variety of free resources on computer technology, networking, and information security. These resources include webcasts, audiocasts, newsletters, examples of policy documentation (e.g., templates of internet and desktop security policy), and the "reading room" with over 1,600 white papers in 70 popular categories, such as the latest internet security threats, database security, backup strategies, data loss prevention, and disaster recovery.

- SANS Institute Website
  http://www.sans.org/