NORTH CAROLINA DEPARTMENT OF PUBLIC INSTRUCTION

Transmitting Private Information Electronically

Best Practices Guide for Communicating Personally Identifiable Information by Email, Fax or Other Electronic Means

Division of Data, Research and Federal Policy

July 29, 2013

School, LEA, and NC Department of Public Instruction (DPI) staff frequently need to share information from individual student records to resolve data issues and answer program area questions. This guide is intended to provide best practices for transmitting individual-level data securely to protect individual privacy and comply with State and Federal Laws.

In compliance with federal law, the NC Department of Public Instruction administers all state-operated educational programs, employment activities and admissions without discrimination because of race, religion, national or ethnic origin, color, age, military service, disability, or gender, except where exemption is appropriate and allowed by law.

Contents

Transmitting Private Information Electronically

Best Practices Guide for Communicating Personally Identifiable Information by Email, Fax or Other Electronic Means

Purpose

School, LEA, and NC Department of Public Instruction (DPI) staff frequently need to share information from individual student records to resolve data issues and answer program area questions. Employees of schools, LEAs, the NC DPI or other education institutions are legally and ethically obliged to safeguard the confidentiality of any private information they access while performing official duties[1]. Private information regarding students and staff should always be transmitted securely. This guide is intended to provide best practices for transmitting individual-level data securely to protect individual privacy and comply with State and Federal Laws.

Relevant Law

FERPA

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.

Definitions

Personally Identifiable Information (PII)

Private information is often referred to as Personally Identifiable Information in the education community. According to the U.S. Office of Management and Budget (OMB), "The term 'personally identifiable information' refers to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

PII includes, but is not limited to:

- The student's name
- The name of the student's parent or other family members
- The address of the student or student's family
- A personal identifier, such as the student's social security number or biometric record

[1] National Forum on Education Statistics. (2006). *Forum Guide to the Privacy of Student Information: A Resource for Schools* (NFES 2006-805). U.S. Department of Education. Washington, DC: National Center for Education Statistics.

- State student number combined with other identifying information
- Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name
- Other information that, alone or in combination, linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty
- Information requested by a person who the education agency or institution reasonably believes knows the identity of the student to whom the education record relates

Education Agency or Institution

The school district, school, or postsecondary institution where the student attends.

Education records[2]

Education records are broadly defined to mean those records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.

Reasonable Person[3]

The standard is – can a "reasonable person in the school community" – someone without personal knowledge of the circumstances – identify the student. Also, PII includes information requested by a person whom the school believes knows the identity of the student

Encrypted

Encrypted data has been put into code so that it cannot be understood without the appropriate decryption equipment.

Secure Methods of Transmitting Data Electronically

According to the State of North Carolina Statewide Information Security Manual[4], "All confidential information shall be encrypted when transmitted across wireless or public networks."

Email privacy, without some security precautions, can be compromised because[5]:

- Email messages are generally not encrypted.
- Email messages have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages.

---

[2] http://www2.ed.gov/policy/gen/guid/ptac/pdf/transcript.pdf
[3] http://www2.ed.gov/policy/gen/guid/ptac/pdf/transcript.pdf
[4] "State of North Carolina Statewide Information Security Manual." *Office of the State Chief Information Officer*. Enterprise Security and Risk Management Office, 20 Apr. 2012. Web. 7 Mar. 2013. <https://www.scio.nc.gov/library/pdf/StatewideInformationSecurityManual/Statewide_Information_Security_Manual_April_20_2012.pdf>.
[5] "Email - Wikipedia, the free encyclopedia." *Wikipedia, the free encyclopedia*. N.p., n.d. Web. 11 Feb. 2013. <http://en.wikipedia.org/wiki/Email#Privacy_concerns>.

- Many Internet Service Providers (ISP) store copies of email messages on their mail servers before they are delivered. The backups of these can remain for up to several months on their server, despite deletion from the mailbox.
- The "Received" field and other information in the email can often identify the sender, preventing anonymous communication.

To protect the confidentiality of individuals from those who do not have access to individual level data, PII should be transmitted using one of the following methods:

- Encrypted Files,
- Password Protected Files, (as long as the password is not contained within the email, file, or on the electronic device containing the data)
- Secure FTP Servers, and
- Emailed files only if encrypted and/or password protected using strong passwords (example: mixed case, special characters)

For those LEAs and schools with full encryption capabilities, transported data and other electronic transporting devices containing DPI data should be encrypted. This requires the recipient of the data to have corresponding decryption capabilities. If compatible encryption is not available to both parties, data should be password protected. The password should be given to the recipient through a different medium, such as a separate e-mail or a phone call, never in notes or documents accompanying the actual data file. In addition, the password should not be transferred via voicemail.

The data should be secured in such a manner that it cannot be identified during the transportation process. The recipient's name, address, and telephone number should be clearly labeled in the body of the email message. While password protection is an adequate means for safeguarding transported data, it is a less desirable method and should only be used if encryption is not available.

Non-secure methods of transmitting data include any combination of data elements that allows individuals to be identified: fax; email without encryption or password protection; and sending IDs paired with any personally identifiable information. In addition, PII should not be shared in a Listserv, on Google Docs or through data-sharing services like Dropbox.

Aggregate Data

While this guide is mainly intended to provide best practices for transmitting private student and staff-level data, it should be noted that care also must be taken with some aggregate-level data. In a small population, it may be possible to identify an individual based on his or her characteristics, even though no name is provided. In that case, the aggregate data should be transmitted using one of the secure methods mentioned above. If the data are intended for publication, data suppression methods such as data masking or data blurring should be used.

Frequently Asked Questions

1. Is a student's Unique Identifier (UID) considered PII?

   A list of UIDs without any other identifying information is not considered PII and may be sent in unsecure email. However, the Reasonable Person standard always applies. If a reasonable person could identify the student based on the information in a document, it should be transported by secure means.

2. Are emails sent from PowerSchool/Home Base secure?

   PowerSchool is configured to work with client email systems, such as; Microsoft Outlook or Outlook Express. Therefore, the same security precautions recommended for other types of email also apply to messages sent from PowerSchool.

3. Is it acceptable to share PII on a restricted-access Listserv?

   No, PII should never be posted to a Listserv.

4. How can PII be securely transmitted to a FAX machine?

   Physical security is essential to preventing unauthorized access to sensitive data. Before sending PII to a Fax machine or printer, the sender should ensure that access to those areas is secure. PII should never be sent to a printer or Fax in a public area.

5. Does the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule apply to an elementary or secondary school?

   Generally, no. In most cases, the HIPAA Privacy Rule does not apply to an elementary or secondary school because the school either: (1) is not a HIPAA covered entity or (2) is a HIPAA covered entity but maintains health information only on students in records that are by definition "education records" under FERPA and, therefore, is not subject to the HIPAA Privacy Rule. However, at the elementary or secondary level, a student's health records, including immunization records, maintained by an educational agency or institution subject to FERPA, as well as records maintained by a school nurse, are "education records" subject to FERPA.[6]

Additional References

- Joint Guidance on the Application of the *Family Education Rights and Privacy Act (FERPA)* And the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* To Student Health Records. http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hippa-guidance.pdf

[6] "Joint Guidance on the Application of FERPA and HIPAA." *U.S. Department of Education*. N.p., n.d. Web. 8 Mar. 2013. <www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hippa-guidance.pdf>.

- State Statutes
    - §116E-5. - North Carolina Longitudinal Data System.
    - §116-229.1. – Disclosure of student data and records by private colleges and universities.
    - §115C-566.1. – Disclosure of student data and records by nonpublic schools.
    - §115C-401.1. – Prohibition on the disclosure of information about students.
    - §132-1.1.(f) – Confidential communications by legal consul to public board or agency; State tax information; public enterprise billing information; Address Confidentiality Program information.

Contact Information

For questions about this guide, please contact Diane Dulaney (diane.dulaney@dpi.nc.gov or 919-807-3690) at the NC DPI.