Public Schools of North Carolina

NC DPI: Data Privacy and Security

KC Elander
Karl Pond
Rosalyn Galloway

1

Data Privacy

General Assembly of North Carolina Session 2013

PART II. INCREASE TRANSPARENCY ON STUDENT PRIVACY ISSUES
SECTION 2. Article 29 of Chapter 115C of the General Statutes is amended by 41 adding a new section to read:
"**§ 115C-402.15. Parental notification regarding rights to student records and opt-out opportunities.**

(a) Annual Parental Notification. – Local boards of education shall annually provide parents, by a method reasonably designed to provide actual notice, information on parental rights under State and federal law with regards to student records and opt-out opportunities for disclosure of directory information as provided under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and notice and opt-out opportunities for surveys covered by the Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h

(b) Notice Content. – The notice shall include information on parental rights under 1 State and federal law to:

(1) Inspect and review education records.
(2) Seek to amend inaccurate education records.
(3) Provide written consent prior to disclosure of personally identifiable information from education records, except as otherwise provided by law. Information shall be included on disclosure of directory information and parental rights to opt out of disclosure of directory information.
(4) File a complaint with the U.S. Department of Education concerning alleged failures to comply with the Family Educational Rights and Privacy Act.
(5) Receive notice and the opportunity to opt out prior to the participation of the student in a protected information survey under 20 U.S.C. § 1232h."

Data Privacy

- Student vs Staff privacy laws, regulations and best practices
- Sharing Date
  - Interagency
  - Agency to LEA
  - Agency to External Researchers
  - Open records requests, parental requests
  - Link to Data Request Docs: http://www.ncpublicschools.org/data/management/research/

Contractors/Agents

- Joel Reidenberg, a Fordham University law professor who focuses on privacy and the internet, told legislators that student data is being stored indefinitely, and contracts between school districts and companies are often weak, with few specifics on privacy and security measures.

http://www.pbs.org/newshour/updates/data-child-public/

Public Schools of North Carolina

Data Privacy and Vendors

*"**The Vendor may utilize partners and/or subcontractors to assist** in the provision of the Services, so long as the **State Data is not removed from the United States** unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations."*

*"**Remote access to Data from outside the continental United States, including, without limitation,** remote access to Data by authorized Services support staff in identified support centers, is **prohibited unless approved in advance** by the State Chief Information Officer or the Using Agency."*

Public Schools of North Carolina

8

Contractors/Agents

- Access as needed
  - Do not share IDs and Passwords
- Access based on Role
  - External Vendor Product (3rd Party)
  - Internal Contractor
- Confidentiality Agreements
- Data Destruction Documents

Public Schools of North Carolina

Public Schools of North Carolina

Data Privacy

Google for Education

G Suite for Education (Online) Agreement

•7. **Confidential Information.**

- 7.4 **FERPA.** The parties acknowledge that (a) Customer Data may include personally identifiable information from education records that are subject to FERPA ("FERPA Records"); and (b) **to the extent that Customer Data includes FERPA Records, Google will be considered a "School Official" (as that term is used in FERPA and its implementing regulations) and will comply with FERPA.**

Data Security

Secure transfer of sensitive data

- Encrypted Files
- Password Protected Files (as long as the password is not contained within the e-mail, file, or on the electronic device containing the data)
- Secure FTP Servers

On-line Tools

- With nearly 100,000 public schools online, or "connected," personal student information collected by schools has moved from filing cabinets and local servers to the cloud.
  - If a school or teacher is using an online tool to store student information, then the teacher and some school administrators can access this information along with the company that provides the online platform. How exactly companies use that data is spelled out in the terms of service agreed to by a teacher, administrator or school district.

http://www.pbs.org/newshour/updates/data-child-public/

Data Security: Storage

From the State Chief Risk Officer - Effective immediately -

All State agencies MUST ensure that State data is stored on approved onsite or offsite solutions that meet the intent of policies and State law (N.C.G.S. 1438-1376). The State CIO must ensure compliance of all State data stored in non-State facilities. Personal cloud storage, file sharing and collaboration solutions such as:

- **Dropbox,**
- **iCloud,**
- **Google Drive,**
- **!Drive,**
- **OpenDrive,**
- **Adobe**

And others **are strictly prohibited** for cloud storage or internal/external file sharing **due to concerns regarding security and data sovereignty**.

Data Security: Storage

Use of these services does not provide the State with the ability to audit the security controls in place and therefore significantly increases the risk of a data breach that could result in the following:

- Loss of competitive advantage;
- Loss of business relationships;
- Unauthorized disclosure of personal information;
- Reputational damage.

Secure Methods of Transmitting Data Electronically

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

- Email privacy, without some security precautions, can be compromised because:
  - 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.

Public Schools of North Carolina

Additional Best Practices

- **Other Considerations**
  - Security not only applies to electronic delivery or systems
    - PII cannot be left visible to or shared with in hard copy persons not approved to have access
      - Hard copies should be secured when not in use
    - Should not be visible via monitor to those not authorized
      - Monitors should be locked when not in use
  - Aggregate data typically does not contain PII. However, small cell suppression must be applied to aggregate data when reported
  - No student level data should be submitted to the federal government

Public Schools of North Carolina

Public Schools of North Carolina

Contacts

kc.elander@dpi.nc.gov
karl.pond@dpi.nc.gov
rosalyn.galloway@dpi.nc.gov

18

Questions