Student Data Privacy Updates

APRIL 9, 2018

Update on Draft Regulations

Regulations will:

- Implement the statute's provisions.
- Supplement the parent's bill of rights for data privacy and security.
- Clarify uncertainties.
- Establish information security and privacy standards.
- Provide model policies.

To achieve these goals

The Chief Privacy Officer is working with:

- The Data Privacy Advisory Council
- Technical Experts
- US Department of Education

Data Security and Privacy Standards

2-d (5)(b) provides that the standards for data security and privacy policies shall include:

- Data privacy protections.
- Criteria to ensure that the use of personally identifiable information benefits students and educational agencies.
- Processes to ensure that personally identifiable information is not included in public reports or other public documents.
- Data security protections for data systems monitoring, data encryption, incident response plans, limitations on access and safeguards for PII transmittal over communication networks, and destruction of PII when no longer needed.
- Application of the standards to third-party contractors.

What is a Standard?

The International Organization for Standardization (ISO) defines a standard as a document:

- Established by consensus.
- Approved by a recognized body.
- That provides for common and repeated use, rules, guidelines, or characteristics for activities or their results.
- Aimed at the achievement of the optimum degree of order in a given context.

Data Security and Privacy Standards

Several options considered in selecting a standard:

- Home grown requirements
- Patchwork of several standards
- National Standard
- Prescriptive vs. voluntary

Identified Preferred Qualities for a Standard:

- Credible
- Durable
- Enforceable
- Understandable
- Supportable

Process

The Work Group consults with:

- Technical experts
- US Department of Education's Privacy Technical Assistance Center
- Other states

Proposed Standard

- Identified the National Institute of Standards and Technology (NIST) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, as a possible model or standard.
- Known to meet the above noted qualities:
  - Credible - most other standards are derived from NIST standards.
  - Durable - US Department of Commerce keeps the standard current.
  - Enforceable - audit resources exist for NIST standards.
  - Understandable - most widely adopted data privacy and security standard in the United States.
  - Supportable - knowledge transfer to districts and vendors supported by federal resources and the private sector.

Other Standards Considered

The Consortium for School Networking, COSN

Center for Internet Security, CIS

NYS Enterprise Information Security Office

US Department of Education's Privacy Technical Assistance Center

Electronic Privacy Information Center, EPIC.org

FedRAMP (applies NIST to Cloud providers)

NYS Comptroller Best Practices

Benefits of Adopting a Standard

- Helps establish common security requirements.
- Helps better understand, manage, and reduce cybersecurity risks.
- Helps prioritize investments and maximize the impact of each dollar spent on cybersecurity.
- Used as a strategic planning tool to assess risks and current practices.
- Incorporates best practices and conformance requirements.
- Reduces the number of technical and process variations.
- Offers a way to measure products and services against objective criteria and provide a basis for comparing products.
- Implements security controls that meet legal and regulatory requirements.

National Institute of Standards and Technology (NIST)

- NIST is a federal agency within the United States Department of Commerce whose mission is to develop and promote measurement, and standards.
- NIST is also responsible for establishing computer and information technology related standards and guidelines for federal agencies to use.
- Many private sector organizations have made widespread use of these standards and guidelines voluntarily for several decades.

Data Collection Transparency

- Reviewed collection practices and eliminated 3 data elements:
  - Date of Entry into the United States
  - Country of origin
  - Immunization Date for First Polio Vaccination
- Added one new data element pursuant to NYS's approved ESSA plan:
  - Out-of-school suspensions data (Beginning in the 2017-18 school year New York State started collecting out-of-school suspensions data at the individual student level to aid with holding schools accountable for out-of-school suspension rates as a measure of school quality and student success.)
- The data elements table on NYSED's website will be updated with this new information.

Planned Public Forums – May 1-11 and June 4-15, 2018

- Eastern Suffolk BOCES
- Monroe 1 BOCES
- ERIE 1 BOCES
- CNYRIC (Syracuse)
- South Central RICS (Binghamton)
- Champlain Valley Ed Services
- Nassau BOCES
- Southern Westchester BOCES
- Capital Region BOCES
- Manhattan
- Brooklyn
- Bronx
- Queens
- Staten Island

Purpose of Forums

- To get input from parents and other education and expert stakeholders to develop additional elements of the parents bill of rights for data privacy and security.
- Get feedback from stakeholders regarding concerns about the privacy and security of protected information for purposes of crafting regulations that adequately address these issues as provided by the statute.
- Gain a better understanding of provider pain-points (teachers, administrators, etc.).
- Not a substitute for SAPA 60 day comment period that will commence in the Fall.
- Format is a listening tour.

Steps to Presenting a 2-D Regulatory Proposal to the Board

- April – Work Group working sessions
- May/June – Public Forums
- June – Data Privacy Advisory Council meeting
- June/July – NYSED review and finalization of draft
- September – Update to Board
- September – Publish in State Register and commence 60 day public comment period
- January 2019 – Present final draft to board
- July 2019 – Effective Date