Memorandum

Prepared By

INGERMAN SMITH LLP

Hauppauge Office
150 Motor Parkway, Suite 400
Hauppauge, New York 11788
(631) 261-8834

Harrison Office
550 Mamaroneck Avenue, Suite 209
Harrison, New York 10528
(914) 777-1134

VIA ELECTRONIC TRANSMISSION

To: **Boards of Education & Board of Cooperative Educational Services**
(Via Email to District Clerks for distribution to Members of the Board)

Superintendents of Schools, District Superintendent,
Business Officials & Assistant Superintendents

Re: News Article

Date: March 21, 2019

We are pleased to share the attached article, written by Diana M. Cannino, Esq. of our office, concerning the protection of student data and the newly proposed regulations from the New York State Education Department. The article was published earlier this week in Volume 20, No. 4 of On Board and is reproduced in full herein.

SED to issue regulations on 2014 law requiring protection of student data

By the New York State Association of School Attorneys

In March 2014, the New York State Legislature created a new section of the Education Law to address an important topic: the safeguarding of student data and privacy. Now, five years later, the Board of Regents is poised to issue regulations that clarify what is expected of school districts and BOCES.

Draft regulations issued Jan. 30 answer many questions about what is required under Education Law Section 2-d but don't resolve all ambiguities. Also, some new obligations will be created. For example, districts must create a complaint procedure for parents, and school board members must receive training.

The regulations will become official when approved by the Board of Regents, which is expected to act in May. The State Education Department is accepting comments on the proposed rules until April 1.

Below is a summary of items clarified by the proposed regulations and a list of new obligations.

Items clarified in the regulations

Since the law was passed five years ago, many school districts and BOCES have struggled to interpret what, specifically, is required under Education Law Section 2-d. The proposed regulations provide clarity on several items:

Guidance for local policy-makers. Perhaps the most awaited regulatory guidance involves a required data security and privacy policy that each school board must adopt by Dec. 31, 2019. The proposed regulation specifically adopts the National Institute for Standards and Technology Cybersecurity Framework – the components of which must be included in the new policy. Guidance from SED states that its chief privacy officer, together with the Regional Information Centers and BOCES throughout the state are developing a model policy

Breach protocols. The proposed regulations provide districts with a clear timeline for notification when a breach occurs. Third-party contractors must report a breach no more than seven calendar days after discovery of such breach. The district is then required to notify SED's chief privacy officer of the breach no more than 10 calendar days after it is informed of the breach, and notify affected parents, eligible student, teachers and/or principals no more than 14 days after the discovery of a breach. The proposed regulations also establish an exception to the required notice to affected parents, eligible students, teachers and/or principals, when notification would "interfere with an ongoing investigation by law enforcement or cause further disclosure of personal information by disclosing an unfixed security vulnerability." In these circumstances, a district has until seven days after the security vulnerability has been corrected or the risk of interference with the investigation ends.

Website disclosures. In addition to the law's explicit requirement to publish a Parents' Bill of Rights on the district's website, the draft regulations clarify that "supplementary information" gathered by districts should be published on websites, attached to the Parents' Bill of Rights. This includes information on every contract where a third-party contractor will receive "personally identifiable information" (PII) on students. In the context of the proposed regulation, PII would include items such as a student's name, email address and Social Security number. For each contract, the attachment should explain "the exclusive purposes for which the data will be used" and "how the third-party contractor will comply with all applicable data protection and security requirements," including encryption.

Click-through agreements. Developers of software applications, including many that are available free of charge, typically require users to abide by certain terms by clicking a box labeled "I agree." The proposed regulations make it clear that when an educational agency enters into a "contract or other written agreement" with a third-party contractor, this includes individual students or teachers making authorizations through "click-through" agreements in software. All of the provisions of Section 2-d and the proposed regulations apply to click-through agreements, including an encryption requirement.

New district responsibilities

According to the State Education Department, the proposed rule "does not impose any program, service, duty or responsibility on educational agencies beyond those imposed by the statute." Despite this assertion, which was published in the New York Register, the draft regulations do create some new obligations beyond those articulated under the statute. Under the proposed regulation, school districts and BOCES must:

1. Provide annual training on information privacy and security awareness to school board members and employees with access to personally identifiable information. Such training may be delivered using online training tools and may be included as part of existing forms of training.

2. Designate a data protection officer. The regulations clarify that this can be an existing employee who assumes this additional duty.

3. Establish procedures for addressing parent complaints of breach or unauthorized release of personally identifiable information, and communicate these procedures to parents. While the law made it clear that districts must designate a person to whom complaints should be directed, a specific procedure for addressing such complaints was not required. The regulations, however, require districts to promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect any personally identifiable information.

4. Ensure, in writing, that all vendors pledge to fully comply with federal and state law as well as the district's data security and privacy policy. The proposed regulations create a requirement that districts ensure that every relevant contract or separate confidentiality and data sharing agreement contain provisions that protected data will be maintained in accordance with federal and state law and the district's data security and privacy policy. No longer will a more general "compliance with law" provision suffice.

Not all vendors may wish to comply with such requirements, particularly companies that make software available for free. This could lead to a reduction in the use of free educational application software. To address this concern, the district could require students and teachers to not provide PPI, perhaps by using randomly generated usernames or proxy email addresses. Also, Regional Information Centers could act as software clearinghouses and handle contracts with vendors.

Lingering questions

The primary goal of the law and regulations is to protect "student data," which is defined as "personally identifiable information" (PII) from student records of an educational agency. Both the law and the proposed regulations borrow the definition of PII from the Family Educational Rights and Privacy Act (FERPA) of 1974, which defines the term broadly.

However, unlike Section 2-d and the proposed regulation, FERPA provides an exception for "directory information" – information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Legally, designating certain items as directory information is what allows school districts to indicating a student's name in a photo caption or discuss the student's accomplishments in a news release.

Even if a school district has designated such information as directory information, Section 2-d and the proposed regulations arguably still treat this information as protected.

While school districts would still be permitted to release this information, sharing such information with third party contractors could now require the protection set forth in Section 2-d. Whenever "student data" is received by a vendor, encryption would be required. Also, there would need to be contractual provisions, privacy plans and disclosure of supplemental information.

Unless the proposed regulation is revised to clarify that PII as defined in FERPA includes the exception for directory information, or SED issues a clarifying guidance, Section 2-d facially appears to protect seemingly harmless items such as a students' email address. Therefore, schools would not be able to use apps that require a user's email address without contracts and additional provisions to ensure the app developer encrypts and otherwise protects this information.

Other issues for schools include:

- **An aggressive implementation timeline.** The proposed regulations are expected to be considered by the Board of Regents for adoption in May and go into effect on July 1. That means districts would have less than two months to implement the new responsibilities described in this article.
- **Adoption of the NIST Cybersecurity Framework.** The National Institute for Standards and Technology Cybersecurity Framework was developed to improve cybersecurity risk management in critical infrastructure. The regulations do not clarify how it will be applied in school districts. However, model policies to be developed by SED's chief privacy officer could clarify that.

NYSSBA plans to submit written comments to the State Education Department before the regulations are made final.

More information is available at www.nysed.gov/student-data-privacy.

Cannino

Members of the New York State Association of School Attorneys represent school boards and school districts. This article was written by Diana M. Cannino of Ingerman Smith, L.L.P.