THE
NATIONAL LAW REVIEW

NYS Education Department Proposes to Significantly Strengthen Data Security and Privacy Protocol

jackson lewis.

Article By
Frank J. Fanshawe
Jackson Lewis P.C.
Workplace Privacy Blog

- Communications, Media & Internet
- Labor & Employment

- New York

Tuesday, February 5, 2019

Government agencies, businesses, hospitals, and universities are the frequent targets of staggering data breaches that can affect millions of individuals. But K-12 schools are also at risk for cyber attacks as they rely more on technology for day-to-day operations and typically maintain a wealth of sensitive information about their students, teachers, administrators, and other staff.

News reports of cyber attacks on schools surface regularly. A phishing attack on San Diego Unified School District in California enabled hackers to steal Social Security numbers and addresses of more than 500,000 students and district staff. Discovered in October 2018, this far-reaching incident occurred between January 2001 and November 2018. And generally, data breaches are on the rise – a recent report found that nearly half a billion consumer records containing sensitive personal information were hacked in 2018, in comparison to 198 million sensitive records in 2017.

To address these gathering cyber threats against schools, the New York State Department of Education ("SED") recently proposed new regulations that will, once adopted, require school districts and state-supported schools to develop and implement robust data security and privacy programs to protect any personally identifiable information ("PII") relating to students, teachers and principals.

The SED's regulation is comprised of a number of key sections, including:

- **Parent's Bill of Rights.** Each school must publish a parent's bill of rights on its website. Schools must also include the bill of rights in every third-party contract where a third party contractor will receive PII. Schools will be required to establish a clear path for parents to communicate and file complaints about breaches or unauthorized releases of student data, including a challenge to the accuracy of the student data.

- **Data Security and Privacy Standard and Plan.** The National Institute for Standards and Technology Cybersecurity Framework ("NIST CSF") is the standard for school security policies. Additionally, each time a school enters into a third party contract with an entity that will receive PII, a data security and privacy plan must be provided. The plan must outline, among other things, how the third-party contractor will safeguard PII consistent with the school's data security and privacy program. All officers or employees of the third-party contractor who have direct access to PII must receive training on applicable federal and state law.

- **Training for Educational Agency Employees.** Information privacy and security awareness training, online or in person, must be provided annually by schools to their officers and employees that have access to PII.

- **Data Protection Officer Appointment.** Every school is required to appoint a Data Protection Officer ("DPO"), filled by a new or existing employee, that is responsible for implementing all required security and privacy policies and procedures. The DPO will serve as the point of contact within the school on all data security and privacy matters.

- **Reports and Notifications of Breach and Unauthorized Release.** Regarding any breach or unauthorized release of PII, third-party contractors must report to all affected schools without unreasonable delay but in no case no more than seven calendar days from the date of discovery. After a third-party breach notification, or after independent discovery by the school itself, the affected school must notify SED within 10 calendar days. Regardless of where the breach or unauthorized release was discovered, the school must notify affected individuals without unreasonable delay but in no case no more than 14 calendar days from the date of discovery. If, however, notification would expose an ongoing vulnerability or interfere with a law enforcement investigation, the notification may be delayed until no later than seven calendar days after the vulnerability has been remedied or the investigation has concluded.

- **Chief Privacy Officer's Powers and Responsibility.** The Chief Privacy Officer ("CPO") of SED will have access to all records, audits, and documents within a school regarding the PII of individuals. Additionally, the CPO will have the authority to require schools to perform privacy and security risk assessments at any given time.

- **Third Party Contractor Civil Penalties.** After each breach or unauthorized release of PII by a third-party contractor, the civil penalty will be up to $10 per affected student, teacher, and principal. It will be the CPO's responsibility to investigate each breach or unauthorized release from a third party entity.

After the required 60-day public comment period for the proposed regulation, it will likely be presented for permanent adoption to the Board of Regents during its May 2019 meeting. If adopted by the Board of Regents, the regulation will be effective July 1, 2019.

Co-Author: *Gabrielle Bruno*

Source URL: https://www.natlawreview.com/article/nys-education-department-proposes-to-significantly-strengthen-data-security-and