Annual Report on Data Privacy and Security

September 2016 - December 31, 2017

1. Summary of Data Privacy and Security Activities

BACKGROUND

NYS Education Law §2-d was passed in 2014 and effective April 1, 2015. The law's focus is to strengthen data privacy and security practices in educational agencies to protect the privacy and security of personally identifiable information (PII) and imposes requirements on both educational agencies and the third-party contractors they utilize to provide services that have access to PII. This annual report covers ta period beginning in September 2016 when I took office through the following calendar year.

DATA PRIVACY ADVISORY COUNCIL

The Chief Privacy Officer formed the Data Privacy Advisory Council (DPAC) which comprises of representatives of the New York State United Teachers, Big 5, NYS PTA, School Administrators Association of NYS, New York State School Board Association, New York City Department of Education, New York State Council of School Superintendents, Future of Privacy Forum, a school attorney, New York Civil Liberties Union, Boards of Cooperative Educational Services (BOCES), Regional Information Centers (RICS), other stakeholders and privacy advocates. DPAC's tasks relate to implementing New York's student data privacy law by aiding the Department in the work of drafting regulations to implement Education Law §2-d. Currently, the DPAC is working to provide input and recommending provisions for inclusion in regulations to implement NY Education Law Section 2-d; provide recommendations to further develop the parent bill of rights for student data privacy and security; provide input on data security and privacy standards for educational agencies and provide recommendations for best practice guidelines to minimize the collection of personally identifiable information.

WEBSITE AND COMPLAINT PROCESS

The office maintains a website at http://www.nysed.gov/student-data-privacy which serves as a means of communicating updates about the regulatory process and other issues, includes a process by which parents, eligible students, teachers and principals may report unauthorized disclosures of personally identifiable information using an online form .

EDUCATION AND OUTREACH

The office continues to serve as a resource for State Education Department (SED) employees and educational agencies such as school districts, Board of Cooperative Educational Services (BOCES), Regional Information Centers (RICS) the field for best practices concerning data privacy and security. The office also fields inquiries from school district teachers, administrators, parents and advocates on a wide range of data privacy concerns.

2. Summary of Reported Incidents

The Education Department is committed to maintaining the privacy and security of student data and complying with New York Education Law, Section 2-d and has implemented an online complaints process. Only complaints about possible breaches of student, teacher or principal data are fielded through this process. Such complaints may be filed by a parent of a student or eligible student (student who is at least 18 years of age or attending a postsecondary institution at any age), principals, teachers, and employees of an educational agency. In the period covered by this report, four complaints were received. All these complaints were initiated by parents. None of the complaints related to third party contractors but concerned educational agency staff and practices. My office worked directly with the school superintendent of each district to ensure the complaints were resolved. Below is a summary of each reported incident.

a. School District, November 2016
   DataBreaches.net notified a BOCES of a possible incident involving a web site that displayed a scrambled/randomized ("hashed") set of student data. In response, the affected district immediately blocked all external access to the identified server, removed any sample data from the server and determined that no accounts were compromised.

b. Edmodo, May 2017
   Platform was hacked and account information (usernames, passwords, email addresses, and telephone number where provided) were acquired by an unknown, unauthorized third

party. No student personally identifiable information was maintained by the platform. Users were advised to reset passwords.

c. School District, May 2017
A district laptop that contained student data was stolen from a district employee's car. No student personally identifiable information was accessed.

d. School District, November 2017
District provided report cards electronically through email to a student's parent/guardian. Due to a merge error, one student's report card was attached to all emails distributed. The process was immediately cancelled. The district determined to look for alternatives to email for future report card distribution. The affected student's parents were notified.

Temitope Akinyemi

Chief Privacy Officer