DATA PRIVACY AND SECURITY

2019 ANNUAL REPORT

Pursuant to NYS Education Law §2-d, the Chief Privacy Officer is required to issue an annual report on (1) data privacy and security activities and progress, (2) the number and disposition of reported breaches, if any, and (3) a summary of any complaints of possible breaches of student data or teacher or principal annual professional performance review data (PII). This report covers the reporting period of January 1 to December 31, 2019.

I. Summary of Data Privacy and Security Activities and Progress

Building upon the work of drafting the Education Law § 2-d implementing regulations with the Data Privacy Advisory Council (DPAC), the office advanced the regulation to the Board of Regents. In accordance with the State Administrative Procedure Act, on January 30, 2019, the Notice of the Proposed Rule Making for Part 121 of the Regulations of the Commissioner of Education relating to Protecting Personally Identifiable Information was published in the State Register. In response to the comments received from the public during the first comment period, the regulation was revised, and the Notice of Revised Rule Making was published in the State Register on July 31, 2019. Following the public comment period for the revised regulation, the regulation was revised again; the Notice of Revised Rule Making was published in the State Register on October 23, 2019. Finally, 8 NYCRR 121 of the Commissioner of Education's Regulations was adopted on January 14, 2020 and came into effect on January 31, 2020.

Although the regulation was revised multiple times, one of the core elements, the standard for data security and privacy practices for educational agencies, has remained unchanged. This standard is version 1.1 of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The NIST CSF provides standards, guidelines and best practices that will help educational agencies improve and strengthen their data privacy and data security practices.

Pursuant to the requirements of Education Law § 2-d, the current inventory of data elements collected by the Department is available on the Department's website for public review, and lists the

following information for each data element: data element name, description, purpose(s) for collection, statutory authority for collection, and the intended uses and disclosure.

The education sector increasingly became a target for cybercriminals in 2019. Sixteen school districts and one Board of Cooperative Educational Services (BOCES) reported ransomware attacks. My office coordinated responses to the incidents with the affected educational agencies, the NYS Office of Information Technology Services, state cybersecurity teams and resources including the Cybercommand center, NYS Division of Homeland and Emergency Security Services and NYS Intelligence Center. The attacks were investigated, and the affected educational agencies have recovered from the incidents and implemented processes to mitigate a recurrence.

The Department continues to maintain the nysed.gov Data Privacy and Security webpage which serves as a means of communicating updates and providing resources to stakeholders. The website includes an electronic form and easy submission process that parents, educators and administrators may utilize to report alleged breaches or unauthorized releases of protected data. The site also includes an electronic form for educational agencies to utilize in reporting breaches and unauthorized disclosures of PII.

My office continues to serve as a resource for Department employees and our colleagues in district offices, Boards of Cooperative Educational Services and Regional Information Centers as we promote the implementation of sound information practices for the privacy and security of student data or teacher or principal data, and field multiple inquiries from school district teachers, administrators, parents and advocates on a wide range of data privacy concerns.

Below, we have summarized the complaints and reports received during the reporting period. In every case, the goal of my office is to provide guidance and direction to assist the educational agencies to improve their data privacy and security practices, and drive transparency by providing stakeholders with information.

II. Number of Reported Incidents and Submitted Complaints Reported in 2019

Reported Incidents	**Number**
Incidents reported by educational agencies or vendors that implicated APPR Data	***0***
Incidents reported by educational agencies or vendors that implicated Student Data	***23***
Complaints submitted by parents	***13***
Complaints submitted by Teachers or Principals	***0***

III. Summary of Incidents Reported by Educational Agencies That Implicated Student PII

#	Description
1	A school coach sent a roster of team players to parents using a third-party application the parent believed was insecure.
2	When printing test score reports, the printer setting was set to double sided, resulting in some students receiving their score as well as another student's score on the other side of the sheet.
3	A teacher allowed a student to borrow the teacher's notebook, providing the student with the ability to access student information, including grades.
4	During a review for a standardized test, a school official, acting under the belief that the test materials were example materials, erroneously disclosed a student's test.
5	A software vulnerability in a vendor's multiple component application was reported by the vendor and multiple educational agencies. This incident was reported by thirty-four (34) educational agencies, including one BOCES. These educational agencies have recovered from the incident and the vendor advanced the end of life date for the software, so it is no longer in use.
6	An unauthorized disclosure of student data affecting one educational agency occurred when a vendor failed to verify that a data import was completed correctly. The imported data was delinked, and the educational agency has recovered from the incident.
7	Ransomware attacks were reported by sixteen (16) educational agencies. The attack was investigated, and the affected educational agencies have recovered from the incident.
8	A former faculty member was reported to have used student information for marketing purposes.

IV. Summary of Complaints by Parents/Eligible Students alleging unauthorized disclosure of student PII

#	Description
1	Student photo and family income information was sent to parent of another student.
2	At a function for parents, a teacher yelled information about a student while in an area that was full of parents such that others heard it.
3	Student's Google account was compromised; the password is the school ID, which is displayed on each student's ID badge and is the same ID used for school lunches was used to access the account.

#	Description
4	A teacher read exam scores for each student to the student's class, identifying each student with each score attained.
5	A teacher provided a student name and other personal information about the student to a parent who offered tutoring services to students.
6	Special education information regarding multiple students including their names, grade levels, and areas where the student was receiving special education assistance was sent home with a student who was also included in the list.
7	Video of student's activities while on the educational agency's grounds reviewed by school personnel who had no connection to the student.
8	Information regarding a student's disciplinary history that included the student's name posted online by a school official.
9	Student photographs were posted to social media websites by a school employee without permission.
10	Student information was accessed by a non-school official and changed without permission.
11	School official disclosed student information including the student's name, grades and progress reports to a third-party without consent.
12	Student IEP plan that included the student's name was disclosed to a third-party.
13	Student received a list personally identifying information for other students including names and addresses.

V. Investigations and Dispositions

Upon receiving complaints or reports of an unauthorized disclosure or a breach, my office investigates by interviewing the parties involved and/or requesting a detailed investigation report from the educational agency with a goal of driving resolution, improving transparency for the agency's parents and stakeholders, and helping the educational agency improve its data privacy and security policies and practices.

Temitope Akinyemi

Chief Privacy Officer