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 offMy of

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