CHIEF PRIVACY OFFICER'S 2020 ANNUAL REPORT ON DATA PRIVACY AND SECURITY

Pursuant to NYS Education Law §2-d, the Education Department's 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, 2020.

I. Summary of Data Privacy and Security Activities and Progress

The COVID-19 pandemic made 2020 a challenging year for the entire world and the education sector was no exception. School closures caused districts to increasingly rely on technology platforms to deliver education. This increased digital footprint required increased vigilance in the areas of data protection and cybersecurity. The work the privacy office has been doing with districts since 2017 paid off, as districts were able to quickly pivot to remote learning while taking steps to protect personally identifiable information. To aid this work, my office issued guidance and model terms and conditions to help districts as they negotiated contracts with technology vendors to implement the shift to remote learning.

While the education sector remained a target for cybercriminals, there was a decrease in reported incidents of ransomware; additionally, reported attacks on school districts and other educational agencies were less severe than in previous years. The number of reported ransomware incidents decreased from 16 in 2019 to 10 in 2020. 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 recovered from the incidents and developed processes to mitigate a recurrence. The largest category of reported incidents was inadvertent disclosures. Training of staff that have access to PII is of paramount importance in protecting data and we continue to urge all educational agencies to make training a priority.

The Department continues to maintain the Data Privacy and Security webpage http://www.nysed.gov/data-privacy-security, which serves as a means of communicating updates and providing resources to stakeholders. The website includes an electronic form and a simple 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.

The Privacy Office continues to serve as a resource for school districts, charter schools, Boards of Cooperative Educational Services and Regional Information Centers, and other entities that operate in the education sector as we promote the implementation of sound information practices for the privacy and security of student data and teacher or principal data. We field inquiries from school district teachers, administrators, parents, legal practitioners, and advocates on a wide range of data privacy concerns.

Below, I 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. Incidents and Submitted Complaints Reported in 2020

Category	*Number of Incidents*
Incidents reported by educational agencies or vendors that implicated APPR Data	***0***
Incidents reported by educational agencies that implicated Student Data	***44***
Complaints submitted by parents	***10***

III. Categories of Incidents Reported by Educational Agencies in 2020

Category	*Number of Incidents*
Inadvertent Disclosures	***31***
Ransomware	***10***
Insider Attack/Student Hacker	***3***

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

#	*Description*
1	A student, in response to a challenge, accessed the school network and obtained a file containing student network login information
2	Ransomware.
3	Ransomware.
4	School staff sent a report containing student PII to the wrong parent.
5	Student accessed a file containing student PII because access to the file was not properly restricted.
6	School district erroneously sent an email containing a file of 66 student records that included, among other things, student transcripts, names and addresses to one student.
7	School support staff, in preparation for a parent meeting, sent student PII to the wrong parents.
8	Ransomware.
9	Ransomware.
10	A teacher's twitter post included a photograph of students and their full names.
11	Ransomware.
12	During a webinar, a participant displayed a spreadsheet containing student PII.
13	Student PII discovered by parent on public district webpage.
14	Ransomware.
15	Board of Education erroneously posted an agenda that included student PII to its website.
16	BOCES employee accidently posted a spreadsheet containing the names of 12 students.
17	Student PII from appointment scheduler was discoverable on the Internet.
18	Lack of updated files caused student PII to be faxed to the physician listed in the student's record who was no longer treating the student.
19	A staff member forwarded an email regarding a student's scheduled teletherapy session to another student's parent.
20	Continuity of learning plans for two students were mixed up and sent to the wrong parents.
21	Improperly configured file permissions allowed a parent who clicked a link in an email to view student PII for all members in a certain grade and class.
22	A school nurse inadvertently sent an email containing student PII to all of the students who were present in the school building.
23	Clerical staff erroneously emailed an attachment containing student PII to parents.
24	Information disclosed in response to a FOIL request included a spreadsheet document containing a hidden column with student PII
25	Ransomware.
26	Improperly configured file permissions for a Google sheet allowed access to an entire Google sheet containing PII for multiple students.
27	Student IEPs were sent to parties not authorized to receive them.
28	Parent discovered that she had access to another student's PII on her child's Google drive.
29	Ransomware.
30	During a class session with distance learners who were taking an exam, a teacher who was looking through IEP and 504 files inadvertently shared her screen with the distance learners, disclosing at least one student's 504 file.

31	During a remote learning session, a teacher was holding a piece of paper containing a student's SAT score that was visible to the remote learners.
32	Two incidents of cleaning staff improperly disposing of PII into unsecured trash cans at the same school.
33	School psychologist shared student PII with the wrong parent.
34	A third-party contractor's maintenance operation resulted in some student PII being visible to education professionals from other school districts.
35	Teacher sent student PII home with the wrong student.
36	Ransomware.
37	In response to an email message with multiple recipients, a staff member inadvertently sent student PII to all recipients instead of one.
38	Unencrypted emails with PII sent to the parents of two students.
39	A school district laptop computer and student workpapers were stolen from a school district employee's unlocked vehicle.
40	Ransomware.
41	In a school district newsletter, student names and GPAs were disclosed.
42	An educational agency employee sent a template populated with student PII to a different school district.
43	A Google reporting form on school district's website did not have correct permissions, and respondents could view a summary of responses which they should not have been able to access.
44	Student accessed School Tool using a teacher's username and password and accessed student PII.

IV. Summary of Complaints by Parents/Eligible Students/Teachers Alleging Unauthorized Disclosure of Student PII

#	*Description*	*Disposition*
1	Passwords used by the school district and assigned to the students used information that could possibly be ascertained by others and therefore were not secure enough.	District directed to take corrective action
2	Complainant's child's home address and phone number were provided to the parents of another student and Complainant received a letter containing student PII that was addressed to that student's parents.	District directed to take corrective action
3	Teacher complaint alleging that a school staff member sent a photograph that included, in the background and among other things, a student's name and IEP information to all of the school's staff and administrators.	District directed to take corrective action
4	Permissions in a school district's software tool allowed a student to access and view student PII.	District directed to take corrective action
5	A parent's request to review the records for the parent's children was denied by the school district.	District directed to take corrective action
6	Three complaints alleged that a school district improperly disclosed protected student PII when the school district, in response to a FOIL request, provided a document that included student PII.	District directed to take corrective action
7	A school district's newsletter that included the names of students on the honor roll included the GPA for each student.	District directed to take corrective action
8	An outgoing school board member downloaded data from the school district's server to a private email account.	District directed to take corrective action
9	Parent filed FERPA opt out for directory information, which included no consent for photographs, and child's photograph was taken despite opt out.	District directed to take corrective action
10	Parent complained that teacher took a photograph of the student with the teacher's personal cell phone and sent it to the parents using an application.	Matter investigated; allegation not substantiated

V. Investigations and Dispositions

Upon receiving complaints or reports of an unauthorized disclosure or a breach, my office opens an investigation which consists of 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,
NYS Education Department