CHIEF PRIVACY OFFICER'S 2022 ANNUAL REPORT

ON DATA PRIVACY AND SECURITY

Pursuant to Education Law § 2-d, the New York State Education Department's (NYSED) 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 (APPR) data.

This report addresses the reporting period of January 1 to December 31, 2022.

I. Opening and Summary of Data Privacy and Security Activities and Progress

Part 121 of the Commissioner's regulations, which implement Education Law § 2-d, require educational agencies[1] to report "every discovery or report of a breach or unauthorized release of student, teacher or principal data" to my office no more than 10 calendar days after such discovery [§ 121.10 (d)]. A breach is broadly defined to mean "any unauthorized acquisition, access, use or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use or receive the student data or the teacher and/or principal data." [§ 121.1(a)]. Unauthorized disclosure or release is defined as "any disclosure or release" not permitted/authorized by: (1) federal or State statute or regulation; (2) a lawful contract or written agreement, or (3) a lawful order, including those issued by a court or tribunal [§ 121.1 (t)].

Educational agencies continue to express confusion as to what should be reported to my office. These regulations—which were enacted in January 2020 and have not been amended—require that almost any unauthorized release of student data or teacher and/or principal APPR data be reported.

---

[1] Education Law § 2-d defines educational agency as a school district, board of cooperative educational services (BOCES), school or NYSED. Schools are defined to include charter schools.

Reporting should **not** be conflated with the term "cyberincidents." Most incidents reported to the Privacy Office are the result of human error, typically the inadvertent sending of information to the wrong family or attaching the wrong document.

2022 saw a substantial, and continued, increase in reported data incidents. Reports have grown from 44 (2020) to 71 (2021) to 140 (2022). I believe this year's increase is based on several factors:

- The changed landscape of the post-pandemic world, where online learning is now commonplace.
- The Illuminate Education Breach, which occurred in the beginning of 2022 and was responsible for 38 data incident reports, including 11 incidents that NYSED took note of on behalf of educational agencies, mostly charter schools, once confirmation was received by Illuminate Education, that a breach occurred.
- Public Outreach. As promised last year, I spent an extensive amount of time in 2022 engaging with the field though conferences, meetings, emails, and phone calls.

Additionally, over 45 percent of the 2022 incidents (65 incidents) were the result of human error. This suggests that we are working too quickly and that there is a lack of knowledge and understanding of privacy laws and protections, even among educational agency administrators. The data we work with is incredibly important. Once it is disclosed, it cannot be un-disclosed. Educational agencies must utilize preventive strategies to prevent future incidents.

In addition to a substantial increase in data incident reports this year, the Privacy Office investigated and issued determinations resolving four complaints of possible breaches of student data. A more detailed description of the complaints is provided to assist educational agencies as they navigate Education Law § 2-d and Family Educational Rights Privacy Act (FERPA) compliance.

The Privacy Office has multiple goals for 2023, including:

1) Continue to engage with internal and external stakeholders, with an emphasis on school administrators and charter schools;
2) Issue, in collaboration with the Office of Information and Technology, the biometric identifying technology report required by State Technology Law § 106-b;
3) Continue to collaborate with the Office of the Attorney General on the investigation of the Illuminate Education breach;
4) Develop a monitoring initiative of educational agencies for compliance with FERPA, Education Law § 2-d and Part 121 of the Commissioner of Education's regulations; and
5) Investigate, and take steps to obtain membership in a national consortium addressing privacy with education vendors and contractors.

Sections II and III of this report contain an analysis and description of the number and nature of reported breaches, with a disposition of data incident report filings. Sections IV and V of

this report contain a summary of complaints concerning possible breaches of student data or teacher or principal annual professional performance review (APPR) data during 2022 as well as the Privacy Office's investigations and dispositions of these complaints.

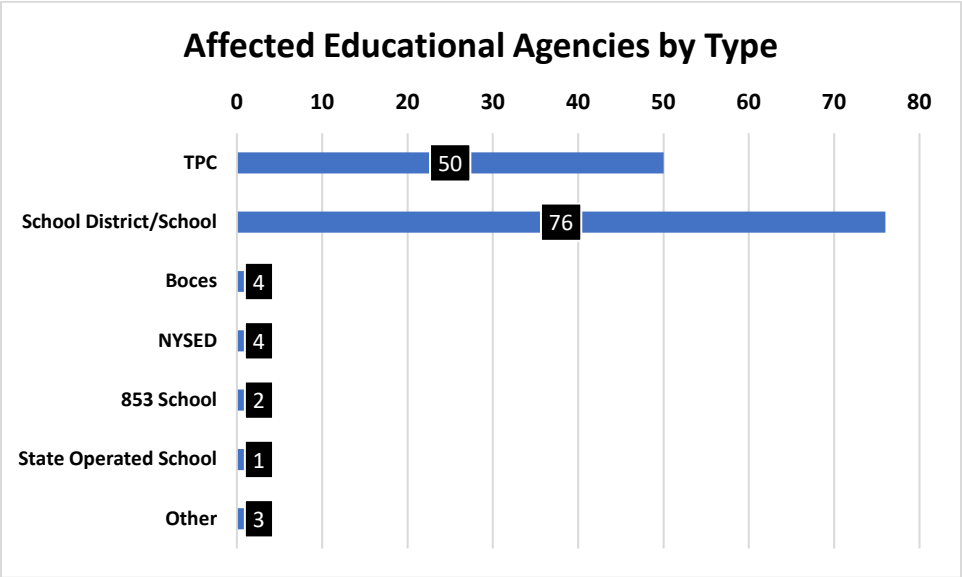
The Privacy Office looks forward to our continued work with our external stakeholders: school districts, charter schools, Boards of Cooperative Educational Services (BOCES) and Regional Information Centers (RICs), parents and advocates as well as our internal stakeholders at NYSED, as we continue to provide guidance about the requirements and importance of privacy and security.

Finally, I must acknowledge the assistance of Nicole Masi, who provided valuable service in her work as an intern, particularly in sorting through the 2022 data incident reports. Thank you for your valuable contribution to this report, Nicole.

Louise DeCandia
Chief Privacy Officer

II. Reported Breaches 2022

In 2022, the Privacy Office received 140 data incident reports for 109 educational agencies, a nearly 100 percent increase from the 71 incidents reported in 2021. Of the 140 reported data incidents, 50 were due to the actions or inactions of third-party contractors that resulted in unauthorized access and unauthorized disclosure of student data.



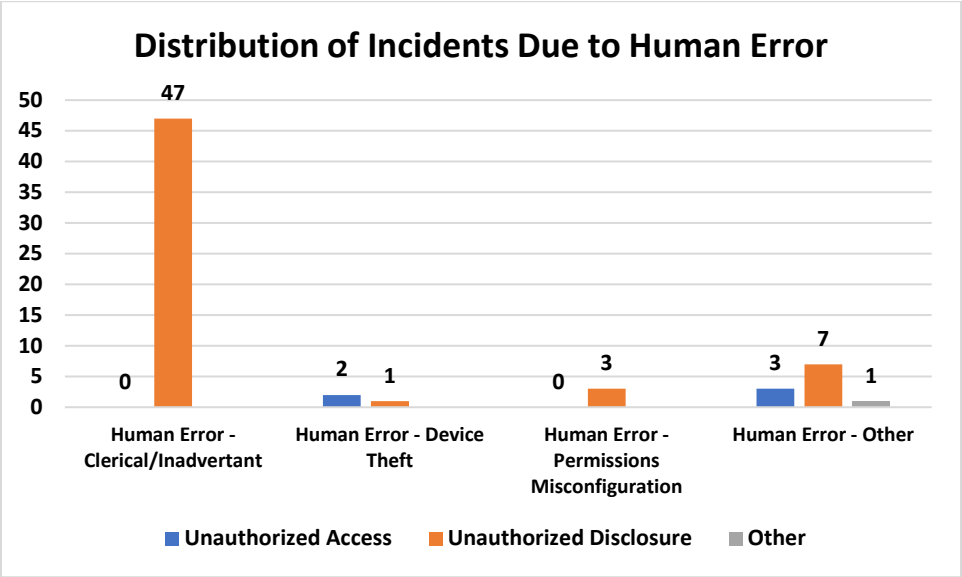
Human Error and Unauthorized Disclosures

Human error accounted for 64 of the 140 incident reports. As seen in the chart below, human error directly caused 58 unauthorized disclosures and 5 unauthorized access incidents. Many of these incidents resulted in unauthorized disclosure of Personally Identifiable Information (PII) through email accounts; some resulted in unauthorized access to email accounts. Human error most frequently included an improper staff release of PII via email, often involving information pertaining to students with disabilities being sent to the wrong family.

Other unauthorized disclosures arising from human error included PII being displayed on a screen during product training; including of PII in documents obtained by Freedom of Information Law (FOIL) requests; student PII posted onto a school's guidance website; and in one instance, and staff release of PII to an individual who impersonated a student.

Some examples of human error allowing unauthorized access include the following:

- A teacher's car was stolen, including two school-issued laptops.
- A school received a damaged package in the mail from a shipping service and discovered student scantron sheets for a standardized assessment were missing.
- Permissions errors allowed unauthorized users to view PII.
- School surveys and sign-up results inadvertently disclosed PII to others. This variety of error was particularly problematic this past year.



Unauthorized Access to Email Platforms, Servers, and Applications:

- Unauthorized users engaged in phishing attacks and gained access to information at multiple educational agencies. At one, an email from a school staff member was sent out with a link directing students and staff to input their school emails and passwords. Approximately 20 individuals clicked on the link and transmitted their credentials via the phishing site.
- A substitute left their Student Management System log-in visible, and a student used the log-in to access another student's data. The student then used this data to log into another student's email account and sent inappropriate emails to teachers.
- A group of students exchanged email passwords, logged into each other's accounts, and some students sent inappropriate emails to staff members.
- A staff member opened a phishing email, which resulted in the compromise of their login credentials. Emails were sent via the hacked account asking internal and external sources for their credentials. The unauthorized user viewed some files on the staff member's online storage account (OneDrive). None of these files contained PII.

- A staff member's email account credentials were compromised under unknown circumstances, which resulted in unauthorized logins from an unidentified IP address located out-of-state.

- A student's student information management system account was compromised when a classmate watched the student enter his credentials. The classmate thereafter accessed the account and sent inappropriate emails.

- A malicious actor pretending to be a representative of an employment website gained access to the Microsoft 365 accounts of a student and a staff member. The actor thereafter used these accounts for phishing purposes.

Unauthorized Access to Other Platforms, Servers, and Applications:

- At three educational agencies, a video surveillance system (Intralogic) became infected with Malware.
- At one educational agency, staff checked a server after hours and identified a shell command that had failed. The educational agency contacted Homeland Security, installed appropriate patches, manually checked its file system, and installed cybersecurity software as a further precaution.
- At one educational agency, permission misconfigurations by a student management system allowed teachers outside of the district to access a small number of student assignments.
- At one educational agency, it was believed that bad actors were staging a ransomware attack by accessing a student's virtual desktop by logging into their student account. There was no evidence to support that any student PII was accessed.
- It is believed that Black Cat Ransomware encrypted and locked down two servers at one educational agency; no PII was compromised.
- A staff member's payroll and bank account information were imperiled when the staff member provided their Microsoft account credentials in response to a phishing email. The unauthorized user was unable to access the staff member's Microsoft account due to multifactor authentication; however, the unauthorized user accessed payroll and bank information as the staff member used the same credentials for that account.

Administrators and staff

- A principal sought, and received assistance in connection with, the placement of special education students by emailing the names, special education placement information, and grade levels of students to a former colleague.

- A school administrator prepared spreadsheets with PII to share with individuals outside of the school district for the purpose of seeking student participation in youth sports.
- A teaching assistant was discovered taking and selling photos of students to companies that license stock photos as part of an outside business.
- A teacher sent the names, school identification numbers, and dates of birth of her classroom students to each student in the class in preparation for Valentine's Day.
- Guidance counselors shared PII via guidance counselor websites, forwarded SAT scores to colleges and/or universities that were not requested by students, forwarded links for academic assistance that allowed students to see who signed up, and, in one case, sent a student's file to a classmate pretending to be the student.

Ransomware and Phishing

In 2022, seven educational agencies reported that they were subject to ransomware or discovered that ransomware was being staged. In each instance, good cybersecurity practices and end point security stopped the threat actors from accessing student data.[2] Similar security practices thwarted several phishing attempts in multiple educational agencies—even when staff fell victim to such attacks. This data emphasizes the necessity of administrator and staff training regarding human risk and its role in securing the privacy of student and staff data.

Other Highlights:

- Data incident reports were received from 31 different counties across the state of New York:
    - The most incidents were reported from Westchester (20 Incidents) and Monroe (14 Incidents) Counties.
    - Long Island reported 23 incidents, the NYCDOE reported 13 incidents, and NYSED reported 4 incidents.
    - 4 incident reports involved COVID-19 test status information.
- 76 of the 140 incidents (54 percent) were attributable to educational agencies' actions or inactions.

[2] The information of 99 employees from one education agency was exposed because of the Cryptolocker virus.

III. Disposition of Data Incident Report Filings

Education Law § 2-d and Section 121.10 of the regulations of the Commissioner of Education require educational agencies to report every discovery or third-party contractor notification of a breach or unauthorized disclosure of student, teacher, or principal data to the Chief Privacy Officer within 10 calendar days of discovery. When a data incident report is filed with NYSED's Privacy Office, there may be follow-up discussions with the educational agency to answer additional questions and, most importantly, to determine if PII was released and whether the proper procedures were implemented when a breach has occurred. If a data incident report reveals a system compromise without evidence of unauthorized access to student, teacher or principal data, the Privacy Office will maintain contact with the educational agency or third-party contractor until a final determination is made as to whether unauthorized access of student, teacher or principal data occurred. Additionally, after an investigation of a system compromise or breach, the Privacy Office may request that a Data Privacy/Cybersecurity Post-Incident Recovery Form be completed and submitted.

Collecting this data allows the Privacy Office to share information about system compromises and breaches within the education field to all of New York's educational agencies. This information can help identify where technical assistance may be necessary and assist education agencies in improving data privacy and security practices.

IV. Summary of Complaints 2021

In 2022, the Privacy Office received 4 complaints. Each was investigated, resulting in the following determinations:

(1) A parent complained that a School District employee emailed a link providing access to a confidential guidance department document to approximately 45 students. The document contained the PII of 286 students, including their statuses as students with disabilities and English language learners; whether they were at risk for Academic Intervention Services; and whether they were displaced or qualified for free or reduced-price lunch. The Privacy Office contacted the School District's administration, requesting that the district investigate and issue a written response summarizing the incident. Upon review of the district's investigation summary and response, the Privacy Office determined that the District was required to: (1) review and update its unauthorized disclosure response plan and policies, especially its

family notification procedures; (2) timely file a data incident report with the Privacy Office; (3) provide written notification to the complainant parent addressing the specific information required to be disclosed under 8 NYCRR 121.10 (g); and (4) submit evidence to the Privacy Office that it had come into compliance with 8 NYCRR 121.4.

(2) A parent complained that a teacher released a student's PII, without consent, to a teaching website and the teacher's personal social media (Twitter) account. The Privacy Office contacted the School District's administration, requesting that the district investigate and issue a written response summarizing the incident. Upon review of the district's investigation summary and response, the Privacy Office determined that: (1) the teacher's actions constituted an unauthorized, impermissible disclosure of student PII; (2) the District failed to timely file a data incident report with the Privacy Office; and (3) the District's data confidentiality training was out of date and must be updated to reflect educators' obligations under Education Law § 2-d and all other applicable data privacy laws and regulations.

(3) A parent complained that two ELA educators had implicitly revealed PII (student reading scores) by publicly rewarding students who had improved their reading scores with ice cream and excluding those students whose reading scores had not improved. The complainant asserted that the public reward allowed the entire class to deduce which students' reading scores had improved and which students' reading scores had not improved by observing who received ice cream. The Privacy Office contacted the School District's Administration, requesting that the district perform an investigation and issue a written response summarizing the incident. Upon review of the district's investigation summary and response, the Privacy Office determined that while excluding select students from a public reward is inadvisable, no student's actual reading scores or any other portion of their educational records were disclosed. Thus, there was no violation of either FERPA or Education Law § 2-d.

(4) A parent complained that their child's PII, in the form of a video, was shown to other parents as part of a disciplinary investigation. The Privacy Office contacted the School District's administration, requesting that the district perform an investigation and issue a written response summarizing the incident. Upon review of the district's investigation summary and response, the Privacy Office determined that it lacked sufficient evidence to determine that a violation of Education Law § 2-d had occurred but encouraged the District to review and update its policies related to data privacy and security and use of video and audio systems. The District was also encouraged to review the United States Department of Education's Privacy Technical Assistance Center (PTAC) guidance regarding the use and disclosure of photos and videos under FERPA and to incorporate such guidance into any revised policies.

V. Investigations and Dispositions of Complaints

Section 121.4 of the regulations of the Commissioner of Education and NYSED's § 2-d Bill of Rights for Data Privacy and Security authorize parents, eligible students, teachers, principals, and other staff of an educational agency to file complaints about possible breaches and unauthorized releases of PII. When a complaint is filed with NYSED's Privacy Office, the educational agency is often asked to provide a detailed investigation report. Additional investigation may be undertaken directly by the Privacy Office. The Privacy Office strives to render timely decisions that assist educational agencies and complainants in understanding the laws, regulations and requirements pertaining to student, teacher and principal data privacy and security.

This report, previous years' reports, the Parents' Bill of Rights, information on how to file a complaint and information on student privacy and Education Law § 2-d can be found on NYSED's data privacy and security web page.