CHIEF PRIVACY OFFICER'S 2021 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 data.

This report addresses the reporting period of January 1 to December 31, 2021.

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

Much to the consternation of many administrators and educators throughout the country, the ongoing COVID-19 pandemic required schools to continue exclusively pivoting to remote instruction during this reporting period. This often meant delivering instruction on-line and learning through digital platforms. While some of the immediate concerns regarding student privacy, data sharing and on-line learning have subsided as educators adapted to a pandemic that is more than two years old, vigilance regarding privacy is always required — and even more so during on-line learning.

Indeed, NYSED's Privacy Office saw a substantial increase in reported data incidents this past year, from 44 incidents reported in 2020 to 71 in 2021. This year's annual report will analyze the incident reports received to better inform New York's educational agencies. Of note, nearly half of the incidents resulted from human error. This emphasizes the importance of privacy training for all organizations that maintain personally identifiable information (PII), especially educational agencies. Educational agencies are already required to provide training to their officers and employees with access to PII on an annual basis in compliance with Section 121.7 of the Commissioner of Education's regulations; however, the increase in data incidents and the high percentage due to human error emphasizes the need for further privacy training.

In addition to a substantial increase in data incident reports over the past year, the Privacy Office received 12 complaints of possible breaches of student data and investigated or intervened in seven of these complaints. Again, 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.

As of January 2022, NYSED's Privacy Office is comprised of several new employees, including a new Chief Privacy Officer. Stakeholder feedback will be used to help determine the Privacy Office's priority tasks regarding interpretation of and compliance with Education Law 2-d and Part 121 of the Commissioner of Education's regulations. The new team has identified several priorities of immediate concern:

(1) One of the first priorities of the Privacy Office is to improve internal and external stakeholder communication over the next year. To this end, the first of a series of regular newsletters to educational agencies' Data Protection Officers were sent to help bridge the communication gap.
(2) Next, the Privacy Office will focus on improving instructions for reporting data incidents and filing complaints. The Privacy Office can only assist LEAs with addressing privacy issues when it is fully briefed regarding incidents as they occur.
(3) The Privacy Office will also undertake additional monitoring of educational agencies for compliance with Education Law §2-d and Part 121 of the Commissioner of Education's regulations this year.

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 received of possible breaches of student data or teacher or principal annual professional performance review (APPR) data during 2021 as well as the Privacy Office's investigations and dispositions of these complaints.

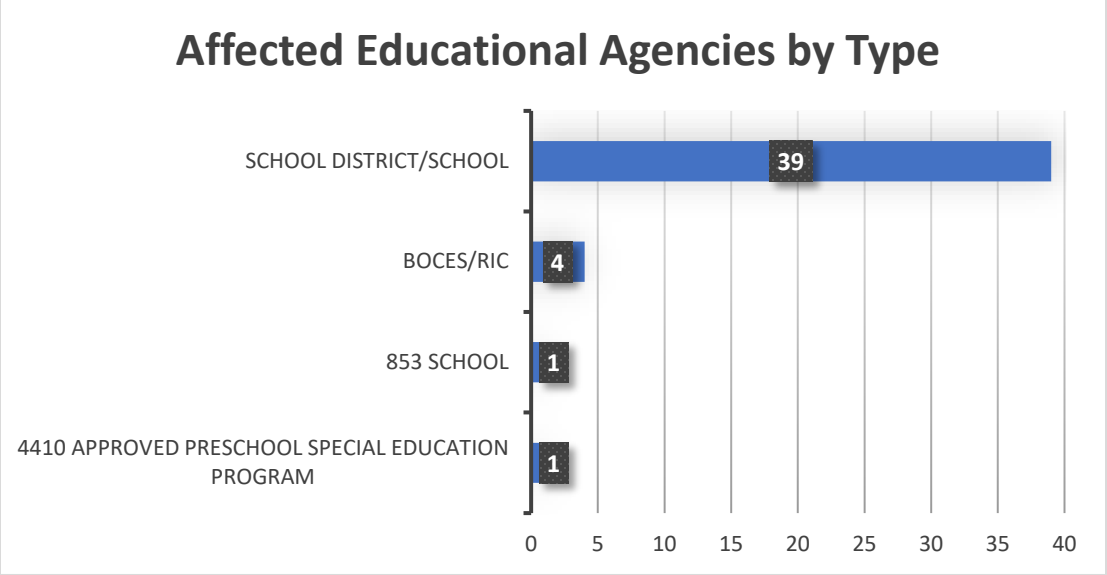
The Privacy Office looks forward to working with school districts, charter schools, Boards of Cooperative Educational Services (BOCES) and Regional Information Centers (RICs) as we continue to provide guidance about the requirements and importance of privacy and security.

Louise DeCandia

Chief Privacy Officer

II. Reported Breaches 2021

In 2021, the Privacy Office received 71 data incident reports for 45 educational agencies,[1] which is a 61 percent increase from the 44 incidents reported in 2020. Of the 71 reported data incidents, 2 were due to the same third-party contractor's misconfiguration of an account, resulting in student data being sent to a person in the wrong school district.



Human Error and Unauthorized Disclosures

Of the 71 incident reports, human error accounted for 35 of the incidents. As demonstrated in the chart below, human error directly caused 30 unauthorized disclosures and allowed for unauthorized access in another 5 instances. Many of these incidents resulted in the unauthorized disclosure of PII and many involved email accounts. Human error involving email accounts most frequently included:

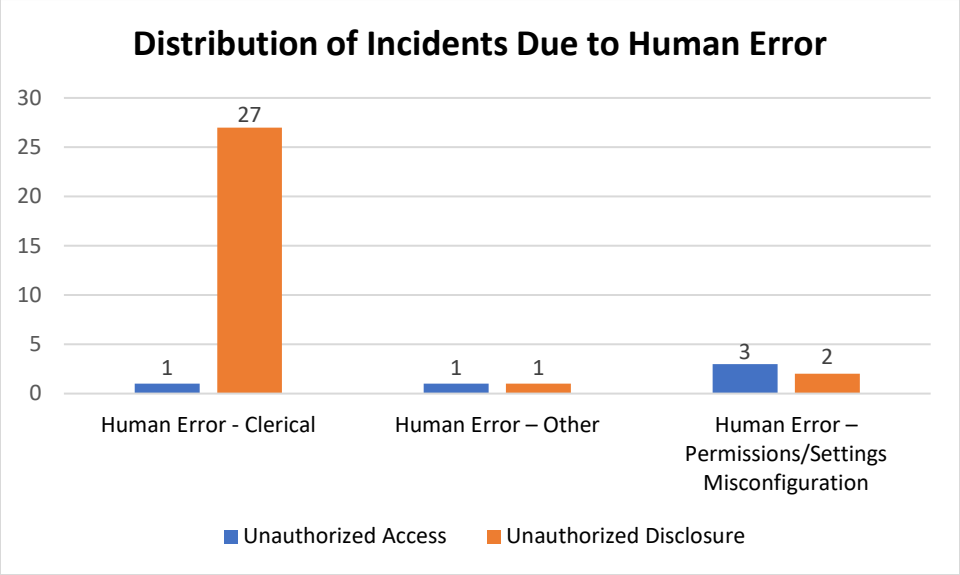
- Emails with PII sent to the wrong parents;
- Emails with PII sent to the entire student body; and
- Emails with PII sent to the wrong school district.

[1] One incident report was filed by a BOCES on behalf of itself and 23 school districts. Additionally, some educational agencies reported more than one incident in 2021.

Other instances of unauthorized disclosure due to human error included PII being sent home with the wrong student; PII being mailed to the wrong parent, fax transmissions sent to an incorrect recipient; and the disclosure of PII without parental permission.[2]

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

- a school district sold a damaged device on eBay without properly destroying the PII contained on the device,
- a laptop was stolen from a teacher's automobile, and
- permission errors allowed shared users to view PII from school districts other than their own.



Unauthorized Access

In 2021, 36 reported incidents involved unauthorized access to an educational agency's network infrastructure. External attackers accounted for 31 of these incidents, while human errors that created an open door for entry accounted for 5 of these incidents.

Unauthorized Access to Email Platforms, Servers, and Applications:
Fifteen of the reported unauthorized access incidents involved the educational agency's email system. These incidents include:

- A user email account was compromised by an unauthorized party in Nigeria. Upon review of the email account's contents, it was determined that the bad actor did not access any protected information.

[2] This incident, which involved multiple students, occurred in 2020 but was not reported to our office until 2021.

- A different educational agency suffered a similar unlawful access incident via email. Although it has been unable to determine exactly how the attacker gained access to one of its email accounts, the educational agency moved forward with remediation, restoration, and recovery efforts by addressing the most popular ways that outside attackers exploit email accounts.

- While investigating spotty email service, an educational agency discovered that its email system had suffered a breach that included the insertion of a password sniffer into the system. As part of its remediation actions, it removed the password sniffer and worked with its RIC to enhance its security system.

- New York State Cyber Command reported that 3 educational agencies suffered Microsoft Exchange exploits. Two of these educational agencies were struck by a "zero-day" exploit.[3]

- An educational agency's users began receiving increased account alerts, prompting an investigation. It found that over one hundred users received the alerts, which had been caused by an attacker in The Bahamas engaged in a brute force attack to gain access to its systems vis-à-vis the affected accounts. The educational agency immediately began containment and assessment actions to stop and minimize the impact of the attack. In recovery, the agency worked with the provider to enhance security. At a different educational agency, the brute force attack was aimed at one specific account.

- An educational agency discovered that its email server had been attacked at the shell level. The investigation uncovered evidence that the attackers responded to emails in the system with a message that included links designed to capture the recipient's credentials. During containment and remediation, the links were rendered inactive so that, when clicked, the user's credentials would not be captured.

- Two educational agencies did not disclose the methodology that was used to access email accounts, but in one instance, the breach expanded beyond the email system; the bad actor also accessed data linked to the breached email account.

- The email system for several educational agencies was accessed without authorization due to phishing attacks. At two educational agencies, a staff member clicked on the phishing link that led to the access. In another instance, three staff members clicked the phishing link.

- Insider wrongdoing accounted for multiple email system breaches. At one educational agency, a small group of students collected and maintained a list of student numbers and passwords, and one student attempted to sell this information.

[3] A "zero-day" exploit is an attack on a previously undetected or not-yet-addressed vulnerability in a system. These particular attacks were perpetrated by HAFNIUM, a well-known hacking organization that uses such exploits to attack systems and mine PII, among other information.

Student email accounts at a different educational agency were accessed by students exploiting a permissions misconfiguration.

Unauthorized access to other platforms, servers, and applications

The remaining summaries describe incidents involving bad actors who achieved unauthorized access by using a backdoor to gain domain controller access.

- At one educational agency, bad actors gained access to a student's credentials and used those credentials to remotely access the educational agency's domain controllers. Another educational agency reported that unauthorized access provided the opportunity for the bad actor to create an administrator account that was used to obtain staff PII. With that information, the bad actor attempted to achieve financial gain.

- In several instances, students achieved unauthorized access to applications other than email. At one educational agency, a student who improperly accessed their grades was asked by other students to access their grades, too. Some of the students provided passwords to their school accounts. Students at another educational agency encouraged their friends to access their accounts using a home computer. The home computer cached the login credentials that were used to gain access to student accounts. Through observation, one student discovered a common denominator among school generated passwords and tested the hypothesis by accessing a different student's school accounts. An error in setting the permissions for files containing student data allowed students to access more than 15 files containing student data.

- Two educational agencies reported that an external attacker gained access to a student's account for one platform to access another, more expansive platform.

- One educational agency reported that unauthorized users "bombed" into a virtual class session.

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 a follow-up discussion 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 describes 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 target necessary technical assistance for educational agencies and assist them to improve data privacy and security policies and practices.

IV. Summary of Complaints 2021

In 2021, the Privacy Office received 12 complaints. Of those 12, five were not investigated by the Privacy Office because they fell outside the jurisdiction of Education Law § 2-d. Additionally, the Privacy Office received, and investigated, three complaints alleging the improper denial of access to educational records.

Complaint Summaries

(1) A parent complained that a School District should not be using a specific digital platform and application that had been breached in the past. The parent was concerned that student PII was at risk and asked why the School District was allowed to use the platform and application. The Privacy Office spoke with the Data Protection Officer for the School District and researched the past breaches. The Privacy Office determined that in one situation, no PII was accessed during the breach. In the other situation, the application in question was removed from production soon after the breach incident. The Privacy Office contacted the parent and explained that decisions on whether to use any technology tool, content, or service are made at the local level and suggested that the parent speak with the School District regarding their privacy concerns.

(2) A complaint was received asking whether a School District's data privacy and security policy, posted on the district's website, was new and whether it had such a policy prior to October 1, 2020. The Privacy Office reviewed the School District's website, determined that it did not comply with the requirements of Education Law § 2-d, and

ordered the School District to bring its website into compliance within thirty days. The School District provided documentation of the actions that were undertaken to bring the website into compliance. The Privacy Office reviewed the documentation and website and determined that the School District's website complied with the law.

(3) A complaint was received regarding the release of contact information for parents and guardians of students in response to a Freedom of Information Law ("FOIL") request. The complaint was amended to include the release of one document containing a specific student's PII. The Privacy Office asked the School District to confirm and explain the release of information. The School District responded, stating that the contact information disclosure was appropriate because that information is directory information; however, upon review the Privacy Office found that the contact information at issue was not included in the School District's directory information policy. Also, the School District admitted that it inadvertently released a document containing one student's PII. The Privacy Office noted that the School District failed to report the inadvertent disclosure and ordered the School District to review its policies concerning the required actions when an unauthorized disclosure or release occurs.

(4) A parent filed a complaint alleging that their child's school disclosed the child's PII to individuals without a reason to know the information, and improperly denied the parent access to the student's records.[4] The Privacy Office reviewed the School District's response to the allegations and ordered the School District to provide the parent with hard copies of all the requested educational records within 30 days. Additionally, the School District was cautioned to remain vigilant with its Education Law § 2-d compliance by ensuring that only School District Officials with a legitimate educational interest be provided access to student educational records.

(5) A parent complained that their request to view video footage of a potential Dignity for All Students Act ("DASA") violation was improperly denied. The District explained that the denial was due to the poor quality of the video. The Privacy Office contacted the School District to request the issue be addressed. The School District reviewed the video footage with the parent.

(6) A complaint was filed alleging that a school hung student artwork that included student names and pronouns on the wall in a hallway of the school, in violation of both Education Law § 2-d and FERPA. The School District confirmed that the artwork

[4] Although the Parents Bill of Rights for Data Privacy and Security grants parents "the right to inspect and review the complete contents of their child's education record," the Education Law § 2-d complaint process does not explicitly authorize the Privacy Office to investigate violations of this right (Education Law § 2-d[3][b][2] and [5]). Nevertheless, because the complaint included allegations of the improper disclosure of student PII, the Privacy Office decided to investigate and address the alleged student education records access denial.

was displayed in the hallway. The School District stated that the project was part of a grammar lesson on pronouns that also provided students with the opportunity for the teacher to be cognizant of students that identify with a "non-traditional" pronoun. The Privacy Office found that Education Law § 2-d was not violated but cautioned the School District to be mindful of its role protecting the health and safety of its students. Citing to NYSED's Guidance to School Districts for Creating a Safe and Supportive environment for Transgender and Gender Nonconforming Students, the Privacy Office stated that transgender students' right to privacy is of utmost importance and that such disclosures cannot be made absent an understanding of the scope and implications of such a disclosure and consent for the disclosure.

(7) A former student submitted a complaint alleging improper denial of access to their educational records. The Privacy Office contacted the School District, asking for an investigation and the results of such investigation. The School District re-opened the records request, and the complaint was deemed resolved.

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.