April 2024

DPO NEWSLETTER

NYSED Privacy Office – Education Law § 2-d is 10 Issue

Volume 3
Issue 2

2023 Annual Report is Posted

The 2023 Annual Report has been posted on the NYSED data privacy and security webpage. The data incident reports have increased from 140 in 2022 to 204 in 2023. As discussed below, the Privacy Office expects another busy year in 2024 since, as of March 15th, our Office has already received 191 reports. Similar to what has been done in the past, the report contains anecdotes and data breach examples that occurred across New York's educational agencies last year.

Privacy complaints also increased in 2023, from 4 in 2022 to 31 in 2023. This resulted in 14 determinations being rendered by the Privacy Office. The determinations can be found on NYSED's data privacy and security webpage. Finally, the Annual Report also includes information regarding the Office's 2023 monitoring of educational agencies' websites.

The increasing number of data incident reports requires the Privacy Office to change the method of reporting erroneous and accidental data incidents caused by human error. Switching to a Microsoft Form to document these incidents will make processing the reports quicker, easier, and more consistent.

Potential Funding Opportunity

As part of the Infrastructure Investment and Jobs Act (IIJA) of 2021, Congress established the State and Local Cybersecurity Improvement Act, which established the State and Local Cybersecurity Grant Program (SLCGP) appropriating funds to be awarded to states and territories. This funding is administered by the U.S. Department of Homeland Security (DHS) through the Federal Emergency Management Agency (FEMA) and is allocated to the State Administrative Agency (SAA) for all states and territories on an annual basis. There are a total of four program years for these program funds, with the first iteration beginning in Fiscal Year 2022 and the final year ending in Fiscal Year 2025. The New York State and Local Cybersecurity Grant Program (SLCGP) is planning to use its Infrastructure Act Grant Funding to purchase multi-factor authentication (MFA), cybersecurity scholarships and cybersecurity training resources on behalf of public sector entities. This includes school districts.

- Here is Governor Hochul's press release on the Federal Infrastructure and Investment Jobs Act (IIJA) Cyber Gant https://www.governor.ny.gov/news/governor-hochul-releases-new-york-state-cybersecurity-grant-plan
- The NY State Local Cyber Grant Committee has decided to use the first year's funding for three statewide shared service offerings 1) multi-factor authentication, 2) cyber certification, and 3) cyber awareness training.
- In order to better understand how many local governments and schools are interested in each of the three offerings the Committee has developed an online interest form.
- To get to the Interest form - go to NYS Division of Homeland Security Emergency Services (NYS DHSES) Federal Grants Page https://www.dhses.ny.gov/federal-programs. There are two links 1) NYS Cyber Grant Cybersecurity Plan and 2) the Interest Form
- The Interest Form is open until April 5,2024. The Interest form does not commit your school district, it is only used to get an idea of how many entities are interested. A formal application process will ensue after interest is assessed.

The interest form will assist Homeland Security to determine spending priorities. This may be an excellent opportunity for school districts that have not yet procured MFA to obtain it. Any questions can be sent to the grant program administration at: Grant.Info@dhses.ny.gov

Education Law § 2-d Turns 10!

Things you can do to celebrate!

- Review the files in your Distict or School's Domain to make sure that they do not contain student data. If those files need to be in the domain, then make sure they are encrypted and password protected.
- Conduct a surprise phishing exercise to see how well your teachers and staff are trained. The general consensus is that phishing attacks are increasing.
- Remind teachers and staff that, when sending email, they need to double check the receipient's name(s) to make sure that the email is going to the intended reciepient(s).
- Implement MFA if you have not done so already. CISA lists MFA as the highest priority security step for K12 schools. You can read more here: CISA Recommendation 1
- Check the permissions on your shared folders to make sure that only individuals with a legitmate educational interest have access to the information in the folder.
- Consider reviewing and updating your annual data privacy and security training. Staff will appreciate keeping the material fresh!
- Remind teachers and staff that if they no longer need electronic copies of documents that contain student data, the documents should be deleted in acordance with educational agency policy.
- Review your data privacy and security webpage for parents. Is the information current? Are links operational? Is the current Data Protection Officer listed? If you haven't yet created a webpage devoted to data privacy and security, the tenth birthday of Education Law § 2-d may be a good time to do so! As a reminder examples can be found here: https://www.nysed.gov/data-privacy-security/school-district-and-charter-school-website-honor-roll

Phishers, accessible data, and an avalanche of breach reports… Oh My!

While folklore attributes the month of March to roaring in like a lion and going out like a lamb, for data incidents, 2024 has roared in like a lion and so far, the roaring continues. As of March 22nd, the Privacy Office has already received over 95% of the number of reports that we received in all of 2023. That is a jaw dropping statistic! Although most reports are attributed to two third-party contractor incidents, the number of reports outside of those two incidents is still outpacing last year's results.

We cannot predict the future, but we know that breaches in the form of erroneous and accidental disclosures will continue to occur. To make the reporting of erroneous and accidental disclosures easier, and to also limit the data collected by the Privacy Office, we are providing a new form for educational agencies to report these types of disclosures.

Beginning April 1, 2024, the "Educational Agencies Report of Erroneous or Accidental Accessibility or Disclosure" form will be available at https://forms.office.com/r/v8fRwtde8e, and will be processed in the same manner as the current Data Incident Reporting Form. There are many benefits to using this revised form:

- Responses are securely stored by NYSED.
- The form is shorter, more appropriate for erroneous and accidental disclosures and easier to use.
- Educational agencies will be able to save a copy of their submitted response.
- After filing with our Office, educational agencies will receive an email documenting the report.

What qualifies as an erroneous or accidental disclosure are disclosures that are made by mistake. Examples when an educational agency should use this new form are when an email containing student data or APPR data is sent to someone who does not have a legitimate educational interest or need to know the student data, or when there are improper permissions configurations on files or folders allowing inappropriate access to student data or APPR data.

Other examples of what is considered an erroneous or accidental disclosure:

- An email with student transcripts for the senior class at School A is sent to a group of teachers at School B. The email was intended only for a group of teachers with a legitimate educational interest at School A.
- An email containing student data for multiple students is sent to teachers and a parent. The parent did not need to know the information.
- A student's individualized education program is sent to the wrong parents.
- A network shared folder for guidance counselors is mistakenly configured to provide access to all teachers instead of limiting access to the guidance counselors.

For incidents such as these, use the new Educational Agencies Report of Erroneous or Accidental Accessibility or Disclosure Form found here: https://forms.office.com/r/v8fRwtde8e

Examples of what is **not** considered an erroneous or accidental disclosure:

- A student obtains a teacher's username and password, copies them and uses the teacher's credentials to log into the School District's student management system to view other students' PII and/or change grades. This is not an erroneous or accidental disclosure and requires filing the Data Incident Reporting Form.
- The consequences of a phishing attack. Yes, the user may have mistakenly clicked on the bait, but the cybersecurity concerns necessitate the filing of a Data Incident Reporting Form.
- **Any** incident caused by a third-party contractor, no matter how minor. In all instances where a third-party contractor is at fault, a Data Incident Reporting Form needs to be filed.

For incidents such as these, please continue to use the current Data Incident Reporting Form found here: Privacy Office Data Incident Reporting Form

In the future, the Privacy Office will also be making some changes to the current Data Incident Report Form so that it is more user friendly, and to remove some unnecessary data requests. If you plan on attending the RIC One DPSS Conference on May 2d Breakout Session 3, we will be presenting. If you want to learn more, please join us!

Questions about the reporting forms or whether and how to report a data incident can always be sent to the Privacy Office at privacy@nysed.gov.

PTAC Training on FERPA

PTAC is offering the National Student Privacy & Data Security Spring Webinar Series training in April. This FERPA training will be offered on three consecutive Thursdays. The dates, topics and registration links are below.

Day 1: FERPA 101 and Data Security Best Practices, April 10, 2024, 2-4pm ET covers the basics of FERPA and provides training on current data security best practices for education data systems.

Day 2: FERPA 201 and Transparency, April 17, 2024, 2-4pm ET dives into scenarios faced by schools and districts and highlights PTAC's research on transparency.

Day 3: Incident Response and Vetting Educational Technology, April 24, 2024, 2-4pm ET leads participants through a simulated data breach and explores how to assess online educational technology for privacy protections and general FERPA compliance.