October 21, 2024

Dear Chief Privacy Officer Dennis Doyle:

The Parent Coalition for Student Privacy, which I co-founded and co-chair, was encouraged to learn that the DOE has finally gotten around to revising Chancellors regulation A-820 that pertain to student privacy, more than ten years after the NY State student privacy law was passed by the Legislature.

We led the campaign for this student privacy law, and though we advocated for even more rigorous provisions, the law that was approved Education Law 2D was a substantial improvement over the chaotic and uncontrolled privacy practices that previously prevailed. Updating the Chancellors regulations is long overdue, especially considering the sharp increase in DOE's use of ed tech programs that collect, store and process personal student information, and the concurrent increase in the number of damaging data breaches, as well as the use of children's personal data for commercial and even criminal purposes.

Yet we were extremely troubled upon reading the revised regulations to learn that the proposed language will weaken rather than strengthen the existing protections for student data in Chancellor regulation A-820, in ways that contradict the provisions and intent of Education Law 2D, as well as federal and state guidance.

We previously expressed our concerns about these issues to you in detailed comments on Oct. 8 that were unfortunately ignored. We now strongly urge you to delay any vote on this troubling language until it can be fundamentally revised and aligned with existing law and guidance, and until you have met with parent leaders and privacy advocates to hear our concerns.

While there are too many weaknesses in the proposed draft to describe them all here, the following three areas we consider the most critical:

1. **The overly broad and unlimited definition of Directory information that could be shared without any privacy protections**

According to the federal Family Educational Rights and Privacy Act (FERPA), certain categories of personal student information called Directory Information can be shared by districts or schools without parent consent, if this disclosure would not be harmful or an invasion of privacy.[1] In those cases, parent opt out instead must be provided, with an annual notice to parents that explains which categories of personal

[1] https://studentprivacy.ed.gov/content/directory-information

student data are considered to be Directory Information (DI), and describes how parents can opt out of their disclosure.

Notably, the state student privacy law, Ed Law 2D, does not mention Directory Information, and thus does not exempt any categories of personal student information from its protections. All student personal data can only be disclosed to certain authorized third parties that provide specific educational services to the school or district, and even then, only with written agreements that specify how the data will be used, secured, and protected. Any other disclosures with few exceptions can be made only with parental consent. Moreover, any personal student data is prohibited from being sold or used for marketing or commercial purposes, with or without parent consent.

And yet in Section II of these new Chancellors regulations, it is proposed that the DOE or individual schools can provide a huge amount and types of student personal information to anyone they please, without any of the privacy protections of 2D. The student data elements which are proposed to be shared in this unrestrained manner as Directory Information are as follows:

"include but are not limited to the following: name; address; telephone number; e-mail address; photographs; date of birth; grade level; enrollment status; dates of enrollment (but not daily or class period attendance); participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and schools attended ."

It is simply unacceptable, especially in this day and age, that this vast array of sensitive children's data could be released by DOE or NYC schools to anyone they please, without the recognition of how potentially dangerous that could be. Very few parents would consider that disclosing their child's phone number, email address, home address and/or date of birth would not be very risky, as this could enable identity theft, the opportunity for abduction, or worse. The proposed language in these regulations even allows for even more unspecified categories of personal data to be considered Directory Information to be shared with anyone for any purpose, as suggested by the words "include but are not limited to".

The language proposed in this draft is far less protective than in the current Chancellor's regulations, that do not specify any student personal information as Directory Information, or cite any exceptions to the need for parental consent in its disclosure, except in very limited cases of health and safety, court order, governmental audit, or the US military for the purposes of recruitment, as established by Federal law.[2]

Enabling such broad categories of personal data disclosure without any restrictions and without parental consent is also far less protective than what the DOE website currently says about this issue:

Only a few pieces of information about your child are eligible to be considered directory information. These include their name; participation in school activities; honors, awards and recognition they've received; photographs of them; school enrollment and graduation details; their major field of study; their grade level and, in the context of their participation in school-based athletics, their height and weight.

[2] According to federal law, schools will provide student Name, address, telephone, year of birth, level of education, academic major, degrees received, educational institution in which the student was most recently enrolled, if the parent does not opt out https://www.schoolcounselor.org/newsletters/april-2018/military-recruiters-%E2%80%93-parent-opt-out-provisions-un

*There are also other types of student information that can be considered directory information, including home addresses, telephone numbers, and dates of birth**. However, the DOE considers these types of information to be sensitive in nature**.[emphasis added]* [3]

Why the DOE would now carelessly go against its own advice and include these same categories of data as Directory Information that could be shared without consent and without any of the privacy or security protections in Ed Lawa 2d is unacceptable and frankly bizarre.

We also looked at the data considered Directory Information by school districts elsewhere in the state and found none that were as expansive as the list now proposed by DOE. For example:

- The BOCES Capital region policy excludes student birth dates, addresses, phone numbers and email addresses.[4]
- Nassau County BOCES policy do not include birth date, email, or phone number as Directory Information.[5]
- The Fabius-Pompey school district in upstate NY includes only name, grade level, degrees and honors, sports participation, and team members' weight and height as Directory Information. Moreover, the district says they will disclose this information only for the purposes of yearbooks, honor rolls, graduation programs and the like. [6]
- Scarsdale categorizes as Directory Information only a student's name, address, and school, and says they provide this information only to PTAs and the Village of Scarsdale for the purpose of mailings and pool passes.[7]
- Elsewhere in the nation, Boston public schools only include student's name, age, grade level, and dates of enrollment as Directory Information, understanding that releasing other sorts of data without restrictions would be too risky and too intrusive.[8]

As dangerous as the overly broad definition of Directory Information in these proposed regulations is the lack of any restrictions or standards to whom DOE and schools may disclose this information and for what purposes.

Instead, if these proposed regulations were adopted, the DOE would have the authority to hand over student names, emails, phone numbers, birth dates, home addresses and possibly even more sensitive personal information to anyone they choose, including data brokers, commercial enterprises, drug

---

[3] https://www.schools.nyc.gov/about-us/policies/data-privacy-and-security-policies

[4] https://www.capitalregionboces.org/about-us/annual-notifications/#:~:text=Parents/guardians%20or%20eligible%20students%20have%20until%20September,news%20happenings%2C%20graduations%20or%20other%20public%20events

[5] https://www.nassauboces.org/about-us/policies-plans-and-public-notices/policy/~board/policies-and-procedures/post/release-of-student-directory-information

[6] See https://go.boarddocs.com/ny/fabius/Board.nsf/files/BV7LVT537C2C/$file/7241%20Student%20Directory%20Information.pdf

[7] https://www.scarsdaleschools.k12.ny.us/Page/8816

[8] https://www.bostonpublicschools.org/Page/7409

companies, social media companies and the like – including the very same companies the city is suing for undermining children's mental health and stability.[9]

This flies in the face of the US Department of Education Directory Information model form that says the following:

The primary purpose of directory information is to allow the School or School District to include information from … education records in certain school publications. Examples include: A playbill, showing your student's role in a drama production; The annual yearbook; Honor roll or other recognition lists; Graduation programs; and Sports activity sheets, such as for wrestling, showing weight and height of team members.[10]

We looked at Directory Information policies elsewhere in the state and nation to see which organizations could receive this data, and found that again, they were far more restrictive than what the DOE has proposed. For example:

- Erie BOCES policy specifies that DI will be provided only to designated organizations, clubs, athletic teams, media, and other parties connected with school activities to promote achievement and participation in school-sponsored activities.[11]
- The Los Angeles Unified school district provides directory information only to other LA government agencies, PTAs, and something called the L.A. Trust for Children's Health, a non-profit established by their elected school board to run school-based health centers.[12] Moreover, the district allows parents to opt out or opt into the disclosure to each particular agency and organization separately, which is a best practice.

The overly broad types of personal data and its unrestricted disclosure as described in these proposed revisions also ignore the fact that there is NO mention of directory information in Ed Law 2D, and no exemption of any type of personal student data from its protections. Accordingly, the Privacy Office of the NY State Education Department has issued the following guidance:

"When sharing PII, educational agencies must ensure that the release of any information, including Directory Information, will benefit students and the educational agency; and a student's PII is not being sold or released for any commercial or marketing purpose, defined as the sale of student data or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly, for advertising purposes, or to develop, improve or market products or services to students."[13]

And yet the language of this proposed regulation does not contain any of this language, and thus appears to violate Ed Law 2D.

We strongly urge DOE to revise the Directory Information section of these proposed regulations to require that all types of student personal data must be protected according to the rigorous provisions of Ed Law

---

[9] https://www.nyc.gov/office-of-the-mayor/news/125-24/mayor-adams-lawsuit-against-social-media-companies-fueling-nationwide-youth-mental-health

[10] https://studentprivacy.ed.gov/sites/default/files/resource_document/file/ferpa-dir-info-not_0.doc

[11] https://www.e1b.org/en/shared-content/ferpa-regulations.aspx

[12] https://www.lausd.org/cms/lib/CA01000043/Centricity/Domain/1236/Fill2023-24InfoRelease_Eng.pdf

[13] https://www.nysed.gov/sites/default/files/programs/data-privacy-security/directory-guidance-final-june-2023.pdf

2D. At the very least, if this information is to be shared outside the school context, the information should be limited to only a student's name, age, grade level, and dates of enrollment, as Boston does, and require that that this information be provided only to school-based organizations and those with written contracts that establish how the data will be protected, secured, and prohibited from being sold or used for commercial or marketing purposes. Without these protections, anyone who receives this data from DOE or from schools could simply use the data anyway they please, and even sell the data to less scrupulous actors.

We also urge DOE to create a Directory Information form that allows parents to opt out of the disclosure of their children's information according to types of data and the purposes and organizations to which the data may be disclosed. A model opt out form is linked to below. [14] This form should be made available in all ten official parent languages and must be strictly adhered to if parents opt out, with rigorous oversight by DOE.

We already have heard from many parents who have used the DOE form to opt out of the disclosure of their children's information to charter schools, and yet charter schools have obtained this information anyway and have deluged them with phone calls and mailers.

Anything less than a complete rewriting and revision of this section would betray the DOE's ethical and legal responsibilities to NYC students and their families and would put their health and safety at risk.

2. **The exemption of certain medical/health records maintained by schools from the protections of FERPA and Ed Law 2D**

Section II.F.2.c. of the proposed regulations say that "*Records maintained by New York City Department of Health and Mental Hygiene personnel in the schools are also not considered Education Records. They are medical Records subject to their own confidentiality requirements*."

Yet the US Department of Ed has emphasized that any medical records held by a school should be treated as education records and thus subject to FERPA, even if district school employees did not produce them:

"Health records that directly relate to students and are maintained by a health care provider, such as a third party contractor, acting for a FERPA-covered elementary or secondary school, would qualify as education records subject to FERPA regardless of whether the health care provider is employed by the school." [15]

Moreover, there is nothing in Education Law 2D that would exempt medical records held by schools from the protections of that law, even if they were made by another City agency such as the Department of Health.

We have already seen examples of how NYC personal student data has been subjected to flagrant abuse and predatory marketing in the case of Teenspace, which has a $26 million contract with the Department of

---

[14] A model Directory Information opt out form is included as Appendix B of the Parent Toolkit for Student Privacy, from the Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood, now named Fairplay for Kids, at https://www.studentprivacymatters.org/wp-content/uploads/2017/05/Parent-Toolkit-for-Student-Privacy.pdf

[15] See https://studentprivacy.ed.gov/sites/default/files/resource_document/file/2019%20HIPAA%20FERPA%20Joint%20Guidance%20508.pdf

Health to provide online mental health services to children. And yet its public-facing Privacy Policy allows their personal data to be used for marketing purposes, and shared with unnamed partners, all of which would be strictly prohibited by Ed Law 2D.[16]

In response, the NYC Department of Health claims it does not have to abide by Ed Law 2D because it is not an educational agency. [17] Yet we found that any student who visits the Teenspace website to sign up for services has their personal information shared with 15 ad trackers and 34 cookies, as well as Facebook, Amazon, Meta, Google, and Microsoft, among others. [18] This wholesale disclosure of student information is particularly concerning, given how the city is suing many of these social media companies for undermining children's mental health, and are designed to cause addictive behavior to maximize their revenues via targeted advertising.[19]

Ed Law 2D regulations also clearly state that no educational agency should facilitate the use of personal data in ways that would violate the provisions of the law. Thus, any health records kept by schools and that result from services delivered by non-DOE staff in those schools, whether employees of the Department of Health or from organizations contracted through the Community Schools program, must be strictly protected as any other school records, according to the provisions of FERPA and Ed Law 2d.

3. The security standards in the draft regulations are far too lax.

More than a million current and former NYC students have already experienced damaging data breaches because of DOE's lax data practices, by those DOE vendors who have failed to employ sufficiently rigorous security safeguards. One of the most important provisions in the regulations for Ed Law 2d is that any district or school that provides access to personal data by vendors must ensure that those companies maintain high levels of data security at least as strong as those specified by the National Institute for Standards and Technology Framework Cybersecurity version 1.1. [20]

Ed Law 2d also requires that districts must ensure data minimization and deletion by any third party with access to personal student information, so that the minimum amount of data is collected and retained necessary to perform their contracted services.

Yet in Section III, d (2), all these draft revisions say about these security provisions is the following: *"Protect PII when it is stored or transferred by using encryption, firewalls and password protection, and ensure such safeguards meet industry standards and best practices."*

Yet as we have seen by repeated student data breaches, not just in NYC but throughout the nation, current ed tech industry standards are NOT best practices, and in fact the two are mutually exclusive. In addition,

---

[16] https://studentprivacymatters.org/privacy-concerns-about-nycs-promotion-of-the-teenspace-online-counseling-service/

[17] https://studentprivacymatters.org/wp-content/uploads/2024/10/DOHMH-Teenspace-Response-Letter-9.23.24.pdf

[18] https://studentprivacymatters.org/our-follow-up-letter-to-the-city-reaffirming-our-concerns-with-teenspace-violations-of-student-privacy/

[19] https://www.nyc.gov/office-of-the-mayor/news/125-24/mayor-adams-lawsuit-against-social-media-companies-fueling-nationwide-youth-mental-health#/0

[20] https://govt.westlaw.com/nycrr/Document/Ib337fb928de111eab5d1fa703d617df0?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)&bhcp=1

there is no mention of the specific NIST standards as required by Ed Law 2D regulations, which should be incorporated in the Chancellor regulations as well.

Furthermore, there is no mention of data deletion anywhere in the proposed Chancellors regulations, which is perhaps the most important security provision required by the state law. The Illuminate breach exposed the personal data of hundreds of thousands of students who had long graduated from DOE schools and left the system – and whose data should never have been retained by the company in the first place. This fact made it difficult for DOE to notify former students as the law requires, to alert them to the risk of identity theft and that they should avail themselves of the free credit/identity monitoring services provided.

In short, there needs to be a much stronger focus on data security, minimization, and deletion in these regulations, as well as in DOE practices and policies to safeguard against breaches, ransomware, and hacking.

There are many other problematic weaknesses that should be addressed in these Chancellors regulations to ensure that student data will be sufficiently protected, especially given the increased risk to student privacy represented by the expanded use of AI programs in schools. There is also no mention, as far as we can see, of the need to protect the personal data of former students as rigorously as current students. Yet we do not have the time or space to go into detail concerning all these issues in this letter.

On behalf of the Parent Coalition for Student Privacy and the families we represent, we urge you to delay any vote to approve these revised regulations until DOE has systematically strengthened them. We also ask that you postpone the enactment of any new privacy regulations until you have met with NYC parents and privacy advocates to hear from them directly about the need for more rigorous and responsible data practices and policies on the part of DOE. We would be happy to set up such a meeting, at your convenience.

Sincerely yours,

Leonie Haimson
Executive Director, Class Size Matters
Co-chair, Parent Coalition for Student Privacy
www.studentprivacymatters.org
info@studentprivacymatters.org

cc: DOE Chancellor Melissa Aviles-Ramos; General Counsel Liz Vladeck; Members of the Panel for Educational Policy; Marina Marcou O'Malley, Alliance for Quality Education; Beth Haroules, NYCLU; Shannon Edwards, AI for Families