



# Data Privacy and Education Law § 2-d

## **Mandatory Module for Students & Faculty Working with P-12 Schools**

**by Hudson Valley Teacher Education  
Consortium**

© September 16, 2020

## Disclaimer

This module is for educational purposes only; it is not intended as legal advice. Consult with your legal counsel regarding the obligations of Colleges/Universities under Education Law § 2-d and related affiliation agreements.

(Drohan, Smith, & Smarra, 2020)

## Special Thanks to ...

Roberta Greene, Executive Director, Mid-Hudson School Study Council

Nancy Hackett, Former President, Mid-Hudson School Study Council

James Drohan, Esq., Allison Smith, Esq., and Nicholas Smarra, Esq. from the office of Thomas, Drohan, Waxman, Petigrow & Maye, LLP

# Introduction

This module is designed to introduce you to NYS Education Law §2-d and other regulations that are intended to protect the data and privacy of students, teachers, and principals.

In this module, you will learn about

- ❖ NYS Education Law §2-d
- ❖ Your responsibility in protecting student, teacher, and administrator privacy.

## What Is Education Law § 2-d?

Education Law §2-d is a statutory and regulatory framework designed to protect an educational agency's sensitive data (**student data** and **teacher/principal data**) and shifts responsibility to third party contractors.

# Why Do We Have This Law?

Listen to the InBloom story as told by Leonie Haimson. (She tells the InBloom story in the first 6 ½ minutes of the video. Continue to listen for more information on student privacy.)



# How Does Education Law §2-d Work?

It places obligations on **educational agencies** and **third party contractors** to:

- ❖ Create policies regarding the use and handling of sensitive information;
- ❖ Incorporate data security and privacy requirements in contracts with third-party contractors/sub-contractors;
- ❖ Establish complaint procedures that may be utilized in the event of a breach or unauthorized release of sensitive information;
- ❖ Properly train officers and employees who will have access to sensitive information;
- ❖ Report and notify any breaches or unauthorized releases; and
- ❖ Apprise parents and eligible students of their rights regarding sensitive information under the law.

# What Is An **Educational Agency**?

Educational Law §2-d defines educational agencies as:

- ❖ A P-12 Public School
- ❖ A School District
- ❖ A Board of Cooperative Educational Services (BOCES)
- ❖ The New York State Education Department

Colleges are NOT educational agencies under Educational Law §2-d.

## How Does Education Law §2-d Define a Third Party Contractor?

*“Any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to, data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities pursuant to Education Law section 211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.” 8 NYCRR 121.1(s).*

<http://www.nysed.gov/common/nysed/files/programs/data-privacy-security/part-121.pdf>

# Is a College a Third Party Contractor Under Education Law §2-d?

**In some situations, a college may likely be a Third Party Contractor.**

A college could be considered a third party contractor and would have to comply with the requirements under Education Law §2-d when:

- ❖ Operating an Educator Preparation Program (EPP), colleges and school districts enter into a written affiliation agreement in which college students conduct fieldwork or student teaching in P-12 schools and have access to student and/or teacher and/or principal confidential data.
- ❖ Student teaching affiliation agreements are just one example of which a college could be considered a third-party contractor for the purposes of Education Law § 2-d.

# What does Education Law §2-d mean to the Third Party Contractors?

*Services of a third-party contractor covered under Education Law §2-d include, but are not limited to, data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs.*

*When an educational agency enters into a contract with a third-party contractor, under which the third-party contractor will receive student data, the contract or agreement must include a data security and privacy plan that outlines how all local, state, and federal data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy.*

*A signed copy of the Parents' Bill of Rights must be included, as well as a requirement that any officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access.*

*Each third party contractor that enters into a contract or other written agreement with an educational agency under which the third party contractor will receive student data or teacher or principal data must also comply with additional requirements outlined in Education Law §2-d*

- such as limiting internal access to education records to those individuals that are determined to have legitimate educational interests,*
- not using the education records for any other purposes than those explicitly authorized in its contract;*

- *not disclosing any PII [Personal Identifiable Information] to any other party that is not an authorized representative of the third party contractor to the extent they are carrying out the contract*
    - (i) *without the prior written consent of the parent or eligible student; or*
    - (ii) *unless required by statute or court order and the party provides a notice of the disclosure to NYSED, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;*
- maintaining reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody; and*
- using encryption technology to protect data while in motion or in its custody from unauthorized disclosure.*
- ( <http://www.nysed.gov/data-privacy-security/frequently-asked-questions-about-data-privacy-and-security> )

## In summary...

*When a third party contractor enters into a contract with a District or school it must do the following:*

- *Adopt technology, safeguards and practices that align with National Institute of Standards and Technology (NIST).*
- *Comply with the District's data security and privacy policy, Education Law § 2-d, and its regulations;*
- *Limit internal access to PII to those individuals who have legitimate educational interests;*
- *Agree that PII will not be used for any other purposes other than only what is authorized in the contract;*

**If a college is acting as a third-party contractor, they must enter into a data privacy agreement whereby they agree to comply with Education Law § 2-d.**

# Addendum to Agreement

## ADDENDUM TO AGREEMENT

### *Regarding*

### *Data Privacy and Security*

### *In Accordance with Section 2-d of the New York Education Law*

This is an addendum (the "Addendum") to an agreement (Clinical Affiliation "Agreement") dated \_\_\_\_\_ ("Original Agreement"), entered into by between \_\_\_\_\_, with its principal place of business located at \_\_\_\_\_ ("Third Party Contractor"), and \_\_\_\_\_ ("Educational Agency"). Upon being executed by Contractor's and Educational Agency's authorized representatives, this Addendum shall be deemed to have been in full force and effect as of the effective date of the Agreement it amends.

**WHEREAS**, Educational Agency is an educational agency within the meaning of New York State Education Law, Section 2-d ("Section 2-d"), and Contractor is a third party contractor within the meaning of Section 2-d; and

**WHEREAS**, Contractor and its authorized officers, employees, students and agents shall have access to "student personally identifiable information (PII)," "student data" and/or "teacher or principal data" regulated by Section 2-d; and

**WHEREAS**, the provisions of this Addendum are intended to comply with Section 2-d in all respects. To the extent that any term of the Agreement conflicts with the terms of this Addendum, the terms of this Addendum shall apply and be given effect.

**NOW, THEREFORE**, it is mutually agreed that the Agreement is hereby amended in accordance with this Addendum, as follows:

# 1. Confidential Information

1.1 Contractor agrees that in performing the Original Agreement with the Educational Agency, Contractor may have access to confidential information in the possession of Educational Agency, including student, teacher or principal personally identifiable information (“PII”). For the purposes of this Addendum and the Original Agreement, it is agreed that the definition of Confidential Information includes all documentary, electronic or oral information made known to Contractor or developed or maintained by Contractor through any activity related to the Original Agreement. This Confidential information includes student, teacher and/or principal data (as the terms are defined under Section 2-d).

1.2 Contractor agrees to comply with Section 2-d, and the corresponding regulations promulgated by the Commissioner of Education of New York (“Commissioner”) thereunder, and relevant Educational Agency policies. In addition, Contractor agrees to comply with any changes in Section 2-d, the Commissioner’s regulations and relevant Educational Agency policy that may be amended or modified during the term of the Original Agreement.

1.3 Upon expiration of the Agreement to which this Addendum applies, without a successor agreement in place, Contractor shall assist Educational Agency in exporting all student, teacher

1.4 The parties further agree that the terms and conditions set forth in this Confidential Information section and all of its subparts shall survive the expiration and/or termination of the Original Agreement.

# Addendum cont'd.

## **2. Challenges to Data**

In the event that a student's parent or an eligible student wishes to challenge the accuracy of student data (pertaining to the particular student) that may include records maintained, stored, transmitted, and/or generated by Contractor pursuant to the Agreement, the challenge will be processed in accordance with the procedures of Educational Agency.

A teacher or principal who wishes to challenge the accuracy of data pertaining to the teacher or principal personally, which is disclosed to Contractor pursuant to the Agreement, shall do so in accordance with the procedures for challenging APPR data, as established by Educational Agency.

## **3. Training**

Contractor represents and warrants that any of its officers, employees, and/or assignees who will have access to student, teacher and/or principal data pursuant to the Original Agreement will receive training on the federal and state laws governing confidentiality of such student, teacher and/or principal data, prior to obtaining initial or any further access to such data.

# Addendum cont'd.

## **4. Use/Disclosure of Data**

4.1 Contractor shall not sell or use for any commercial purpose student, teacher and/or principal data that is received by Contractor pursuant to the Agreement or developed by Contractor to fulfill its responsibilities pursuant to the Agreement.

4.2 Contractor shall use the student, teacher and/or principal data, records, or information solely for the exclusive purpose of and limited to that necessary for the Contractor to perform the duties and services required under the Original Agreement. Such services include, but are not limited to \_\_\_\_\_. Contractor shall not collect or use educational records of Educational Agency or any student, teacher and/or principal data of Educational Agency for any purpose other than as explicitly authorized in this Addendum or the Original Agreement.

4.3 Contractor shall ensure, to the extent that it receives student, teacher and/or principal data pursuant to the Agreement, that it will not share Confidential Information with any additional parties, including an authorized subcontractor or non-employee agent, without prior written consent of Educational Agency.

# Addendum cont'd

## **5. Contractor's Additional Obligations under Section 2-d and this Addendum**

Contractor acknowledges that, with respect to any student, teacher and/or principal data received through its relationship with Educational Agency pursuant to the Agreement it is obliged to maintain a Data Security & Privacy Plan, and fulfill the following obligations: :

- execute, comply with and incorporate as Exhibit "A" to this Addendum, as required Section 2-d, the Parents' Bill of Rights for Data Privacy and Security developed by Educational Agency;
- store all data transferred to Contractor pursuant to the Agreement by Educational Agency, in an electronic format on systems maintained by Contractor in a secure data facility located within the United States or hard copies under lock and key;
- limit internal access to student, teacher and/or principal data to Contractor's officers, employees and agents who are determined to need such access to such records or data to perform the services set forth in the Original Agreement;
- not disclose student, teacher and/or principal data to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under the Agreement, unless: (I) the other party has the prior written consent of the applicable student's parent or of the eligible student; or (II) the other party has the prior written consent of the applicable teacher or principal; or (III) the disclosure is required by statute or court order, and notice of the disclosure is provided to Educational Agency no later than five business days before such information is required or disclosed (unless such notice is expressly prohibited by the statute or court order);

## Addendum cont'd.

- use reasonable administrative, technical and physical safeguards that align with the NIST Cybersecurity Framework and are otherwise consistent with industry standards and best practices, including but not limited to encryption, firewalls and password protection as specified by the Secretary of the United States Department of HHS in any guidance issued under P.L. 111-5, Section 13402(H)(2), to protect the security, confidentiality and integrity of student and/or staff data of Educational Agency while in motion or in custody of Contractor from unauthorized disclosure;
- not mine Confidential Information for any purposes other than those agreed to in writing by the Parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited; notify Educational Agency, in the most expedient way possible and without unreasonable delay, of any breach of security resulting in an unauthorized release of any PII. In addition, Contractor shall take immediate steps to limit and mitigate the damage of such security breach or unauthorized release to the greatest extent practicable, and promptly reimburse Educational Agency for the full cost of any notifications Educational Agency makes as a result of the security breach or unauthorized release. Contractor further acknowledges and understands that Contractor may be subject to civil and criminal penalties in accordance with Section 2-d for violations of Section 2-d and/or this Agreement.
- understand that any breach of the privacy or confidentiality obligations set forth in this Addendum may, at the sole discretion of Educational Agency, result in Educational Agency immediately terminating this Agreement; and
- familiarize its applicable officers, employees and agents with this Addendum and with the "Parents' Bill of Rights for Data Privacy and Security."

## Addendum cont'd.

The Contractor acknowledges that failure to fulfill these obligations shall be a breach of the Agreement.

6. Except as specifically amended herein, all of the terms contained in the Original Agreement are hereby ratified and confirmed in all respects, and shall continue to apply with full force and effect.

**IN WITNESS WHEREOF**, Contractor and Educational Agency execute this Addendum to the Agreement as follows:

*Contractor Name:*

*Educational Agency:*

*By:* \_\_\_\_\_

*By:*

*Title:* \_\_\_\_\_

*Title:*

*Signature:* \_\_\_\_\_

*Signature:* \_\_\_\_\_

*Date:* \_\_\_\_\_

*Date:* \_\_\_\_\_

Prepared by the Law Offices of Thomas, Drohan, Waxman, Petigrow & Mayle, LLP as part of the Education Law § 2-d training for the Hudson Valley Teacher Education Consortium for educational purposes and should not be considered legal advice

# What Is Protected Under the Law?

- ❖ **Student Data** – *Personally identifiable information (PII) from the student records of an educational agency (same protected information under the **Family Educational Rights and Privacy Act [FERPA]**).*
- ❖ **Teacher and/or Principal Data** – *Personally identifiable information(PII) from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law sections 3012-c and 3012-d.*

(<http://www.nysed.gov/data-privacy-security/federal-laws-protect-student-data> )

# What is **Personally Identifiable Information (PII)**?

***Personally identifiable information (PII)** for education records is a **FERPA** term referring to identifiable information that is maintained in education records and includes direct identifiers such as a student's name or ID number, indirect identifiers such as a student's date of birth or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.*

(<https://studentprivacy.ed.gov/content/personally-identifiable-information-education-records>)

# It Is Not Within the Purview of Education Law §2d When....

## ...data are not identifiable.

The confidentiality and privacy provisions of **Education Law §2-d** and **FERPA** extend only to PII, and not to student data that are not personally identifiable. Therefore, de-identified data (e.g., data regarding students that uses random identifiers), aggregated data (e.g., data reported at the school district level) or anonymized data that could not be used to identify a particular student are not considered to be PII.

(<http://www.nysed.gov/data-privacy-security/frequently-asked-questions-about-data-privacy-and-security> )

# What is **FERPA**?

*The **Family Educational Rights and Privacy Act (FERPA)** [of 1974] (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.*

***FERPA** gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."*

*(<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>)*

**FERPA** is the reason why parents cannot access college students' records unless they sign forms giving permission to do so.

## Other Federal Laws To Be Aware Of

**Protection of Pupil Rights Amendment (PPRA)** defines the rules that the states and school districts must follow when giving tools to students such as surveys, analysis, and evaluations funded by the US Department of Education.

The **Children's Online Privacy Protection Rule (COPPA)** protects children through requirements placed on operators of websites, games, mobile apps or online services that focus on children under 13 years old, and operators of other websites or online services that know that they are collecting personal online information from a child under 13 years old.

(<http://www.nysed.gov/data-privacy-security/frequently-asked-questions-about-data-privacy-and-security> )

# Health Insurance Portability & Accountability Act (HIPAA)

This is a law that protects a patient's medical data privacy. You have likely been asked to sign a form at a doctor's office stating that you have been given access to the practice's privacy policy. This is a result of HIPAA.

*HIPAA does the following:*

- *Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs;*
- *Reduces health care fraud and abuse;*
- *Mandates industry-wide standards for health care information on electronic billing and other processes; and*
- **Requires the protection and confidential handling of protected health information**

(<https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatIsHIPAA.aspx> )

# Implications of Education Law §2-d

# Parents' Bill of Rights for Data Privacy and Security

*[Since] the New York State Education Department collects and maintains certain personally identifiable information about students enrolled in public schools across the state, Education Law §2-d requires each educational agency in the State of New York to develop a Parents' Bill of Rights for Data Privacy and Security and publish it on its website. The purpose of the Parents' Bill of Rights is to provide information to parents (which also include legal guardians or persons in parental relation to a student, but generally not the parents of a student who is age eighteen or over) and eligible students about certain legal requirements that protect personally identifiable information pursuant to state and federal laws. (<http://www.nysed.gov/data-privacy-security/bill-rights-data-privacy-and-security-parents-bill-rights>)*

# Rethinking the Products We Use with Data Security In Mind

*Effectively, these regulations will impact schools and the products many of them rely on in a basic way. Teachers will no longer be able to use “Click through” programs that collect or use protected data with standard “Terms and Conditions.” Contractors regardless of where they do business must accept the specific requirements in compliance with the law if they are to do business with an educational agency located in New York State.*

*(<https://www.bsk.com/news-insights/preparing-for-imminent-changes-in-the-new-york-state-education-law-regarding-data-privacy>)*

Both educational agencies and third party contractors will need to use products that are Education Law §2-d compliant to protect data, thus limiting the products available for use, and possibly eliminating some products already in use.

# What Are Reasonable Safeguards to Protect Student Data?

What is considered a “reasonable safeguard” depends on the context; however, the following examples are a good starting point:

- ❖ Implement encryption when sending and storing information;
- ❖ Use firewalls;
- ❖ Have password protected computers and computer programs;
- ❖ Use physical locks and keys (especially for paper records);
- ❖ Adopt policies for computer usage (e.g. not leaving unlocked computers unattended, internet safety and security training, etc.);
- ❖ Only use educational technology pre-approved by your school or school district that is Education Law §2-d compliant;
- ❖ Dispose of student data when you are done by shredding paper files and deleting electronic files;
- ❖ Do not put any student data (including images) on social media.

# What To Consider When Working With Student Data

- ❖ **DO** ask yourself:
  - Am I sharing student information?
  - Can someone personally identify my student from this information?
  - Do I have parental consent?
- ❖ **DON'T ever** email personal student or teacher data in an EMAIL; in fact, be very careful how personal email is used for school purposes.
- ❖ **DO** ask your teacher or district for guest access to any online systems or ask your teacher for assistance accessing those systems. **Password sharing is strongly discouraged.**
- ❖ **DON'T** use educational technology programs that your school does not have a contract for. Check with your school administration if you are unsure whether a contract exists for a particular program.
- ❖ **DON'T** send student grades and other educational record information via email – if parents ask for their child's grades, pick up the phone instead!

(Do's and Don'ts from: [https://www.fordham.edu/download/downloads/id/1850/09\\_-\\_dos\\_and\\_donts\\_for\\_teachers.pdf](https://www.fordham.edu/download/downloads/id/1850/09_-_dos_and_donts_for_teachers.pdf))

# Special Considerations when Collecting Data for the edTPA and Field-related Assignments

- ❖ Remember to **PROTECT STUDENT NAMES under all circumstances**, (collecting student IEP and other plan information for your Context for Learning; reflections, lesson plans, differentiation, etc.). **CODE** your students' names (student A, B, C, etc. and the name of the school and teacher) and keep that code list at home in a protected place.
- ❖ Do not **EVER** take home or transmit confidential, identifiable information about a student (e.g. a portion of an IEP, grades, behavioral report, etc.)
- ❖ **Protect ANY data** you collect electronically (on your phone or computer) with passwords and other reasonable safeguards.

## Remember: When FINISHED with Student Data...

- ❖ Always ensure that they are stored somewhere **SAFE AND SECURE**, and **LOCKED**.
- ❖ When finished with data and your assignment (e.g., your reflections are graded, you've received your passing edTPA score report), you are required to destroy all data (shred actual documents, completely delete online, identifying information, etc.).

35

# Quiz 2

- ❖ 1. River videotaped a lesson to share with their college's field supervisor. During the lesson, a student becomes disruptive and the cooperating teacher takes disciplinary action. The class became out of control and by the end of the day, River was wiped out. When River returned to the dorm, their roommate asked how the day went. River felt the need to tell someone about the day. Which of the following would be the best course of action for them to take?

- (a) Show their roommate the video so that they can see for themselves what kind of day you had.
- (a) Tell their roommate in great detail what happened over dinner.
- (b) Tell their roommate they had a challenging day at school and then write in their journal using pseudonyms for their students.
- (a) Call their mom and cry that maybe they chose the wrong career.

2. Maya has been writing in her reflective logs about some 10th graders in her class with behavioral issues. This week, the students were sent out of the classroom and received detention. When Maya sends her logs to her college supervisor, which of the following does she have to consider to be compliant with Education Law § 2-d?
- (a) She should not use the student's real names or other personal identifiable information in her logs.
  - (b) She should send her logs through encrypted email or post them through an Education Law § 2-d compliant platform.
  - (c) Since she may be late for class, she might want to have her roommate deliver the logs to her supervisor, since her supervisor prefers to collect assignments on paper.
  - (d) a & b

- ❖ 3. Professor Grantham loves the latest technology. She is excited about all the new STEM apps available that can enhance student engagement and cannot wait to tell her student teachers about them as they get ready for the edTPA. Professor Grantham thinks that some of these new apps might solve the issues the student teachers have been having with keeping their own students off of their phones, believing that this will allow the student teachers to take charge by turning the phones into a learning tool rather than a distraction. However, Professor Grantham just took a training on Education § 2-d. What should she do now?

- (a) Tell her students about all of the apps and let them worry about Education Law § 2-d.
- (b) Call the placements of her student teachers, find out if any of the newly discovered apps are district-approved as Education Law § 2-d compliant, and then tell the student teachers those the school/school district has contracts for or has approved.
- (c) Tell her students about all of the apps, and tell them that it's okay to use them because the chances are that no one is actually checking.
- (d) Give up on trying to use technology altogether, deny her own passion and forget about trying to creatively solve the problem of the chronic cellphone abuse in her student teachers' classrooms.

# What Happens When There Is a Confidentiality Breach or a Security Leak?

- Where there is a breach and unauthorized release of PII by a third party contractor or its assignees, the third party contractor must notify the educational agency (e.g. the school district) of the breach in the most expedient way possible and without unreasonable delay.
- The educational agency must then notify the parents in the most expedient way possible and without unreasonable delay.
- NYSED's Chief Privacy Officer will investigate reports of breaches or unauthorized releases of PII by third-party contractors. As part of the investigation, the CPO may require that the parties submit documentation, provide testimony, and may visit, examine and/or inspect the third-party contractor's facilities or records.

<http://www.nysed.gov/data-privacy-security/frequently-asked-questions-about-data-privacy-and-security>

## In the Event of a Breach...

The college must be notified immediately. Each college will have a designated person (John McCabe at Manhattan College) who will be responsible for addressing data security and privacy issues.

Students should make sure that their fieldwork or student teaching supervisor is notified.

Students and faculty must immediately notify the designee within their program, who in turn, will notify the designated point person within the college or university, Mr. McCabe, who will notify the Educational Agency, which will notify NYSED's Chief Privacy Officer and affected parties.

# When the Third Party Contractor Reports a Breach or Unauthorized release of PII...

The third-party contractor (the college) is obligated to promptly notify the District of the breach or unauthorized release of PII ***without unreasonable delay, but no more than seven (7) calendar days after discovery of the breach.***

Notice of the breach must include to the extent available:

- ❖ *Brief description of the breach or unauthorized release;*
- ❖ *Dates of the incident and the dates of discovery;*
- ❖ *Description of the types of PII affected (if known);*
- ❖ *Estimate of the number of records affected;*
- ❖ *Brief description of investigation or plan to investigate; and*
- ❖ *Contact information for representatives who can assist parents or eligible students that have additional questions.*

8 NYCRR 121.10 (g)

# When a Breach Occurs, the Third Party Contractor Is Expected to Take Responsibility

- ❖ *Third-party contractors must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII.*
- ❖ *The third-party contractor shall pay for or promptly reimburse the educational agency for the full cost of the required notification.*  
*8 NYCRR § 121.10*
- ❖ *Third-party contractors may wish to check with their insurance carrier to ascertain such events are covered under their policies.*

# The Third Party Contractor May Face Penalties

The NYSED Chief Privacy Officer may impose certain penalties such as

- A monetary fine;
- Mandatory training regarding federal and state law governing the confidentiality of student data, or teacher or principal (Annual Professional Performance Review)APPR data;
- Preclusion from accessing any student data, or teacher or principal APPR data, from an educational agency for a fixed period **up to five years.**

(<http://www.nysed.gov/data-privacy-security/frequently-asked-questions-about-data-privacy-and-security> )

## In Summary

- ❖ The college should be informed a.s.a.p. because it has a responsibility to inform the school district as soon as possible, but in no more than 7 days.
- ❖ The school district notifies NYSED.
- ❖ NYSED's Chief Privacy Officer will conduct an investigation.
- ❖ The college will be expected to cooperate with the investigation.
- ❖ The school district will inform all affected families without unreasonable delay, and the college will be expected to pay for or promptly reimburse the District for the notification process.
- ❖ The Chief Privacy Officer at NYSED will impose penalties against the college which could include:
  - Monetary fines,
  - Mandatory training on data privacy, and
  - Not being allowed to access any student, teacher or principal data, which essentially means not being able to access classrooms, for up to 5 years.

**OVERALL, THIS HAS THE POTENTIAL TO BE VERY COSTLY TO THE COLLEGE.**

47

# Quiz 3

1. As a fieldwork student taking a course in literacy, Angel discovers Spelling Bee, a fun spelling app for the third grade class you are assigned for 30 hours. As a gift to the teacher, she signs up each student to receive the App. The App requires that the spelling grades of each student be uploaded to track student progress. Angel adds the grades for each student. Angel then sends the teacher a list of students' names and the password she used for each pupil. Please identify what should happen next.

- a. The teacher should thank Angel for being so thoughtful and giving the students such a wonderful gift.
- b. Since this is a data breach, the teacher should publicly admonish Angel.
- c. Angel should notify the college's designated officer immediately, without even informing the college supervisor
- d. Angel should inform the college supervisor when she gets back to campus that evening.

2. Thankfully, Angel's cooperating teacher, Mr. Davies is a patient, gentle man. He calmly explains to Angel that what she has done has put the student's data at risk and asks her to take a break and call her college to report the breach, which she does. What should happen next?



a) The college officer assigned to deal with such matters can submit needed documents within a month.

b) The college officer assigned to deal with such matters makes sure that the school district is informed immediately. The school district notifies NYSED completing a full report.

c) The college officer assigned to deal with such matters contacts NYSED directly within 2 weeks, and makes sure to complete a full report.

d) The college officer assigned to deal with such matters talks only to the MC student, the cooperating teacher and principal.

3. Thankfully, the college officer reports the incident fully in a timely manner. The Chief Privacy Officer conducts the investigation. The college is asked to reimburse NYSED for the cost of notifying the families of the breach, and of providing data security protection monitoring for the next 12 months. However, the college considers itself lucky. Which of the following would be a particularly challenging penalty for a College Educator Preparation Program (EPP)?

- a) Pay an additional monetary fine of \$1000.**
- b) Attend additional training**
- c) Write letters of apology to all affected students and their families**
- d) Be denied access to that educational agency for 5 years**

# Some Questions a **Student Teacher/Fieldwork Student** Should Ask the Cooperating Teacher and/or Principal:

- ❖ For additional security, can I be issued a school email account to use for communications? Or, is there another way to ensure security?
- ❖ What are the expectations for data privacy in the school? Does it have a policy for teachers?
- ❖ What forms of permission does the school already have in place for students (such as parent forms)?
- ❖ What is the best way to distribute permission slips for the purpose of video recording for observations, class assignments, and the edTPA?
- ❖ Is there a list of approved apps or online tools that are Education Law §2-d compliant for this school/school district, and that I can see for lesson planning purposes?
- ❖ May I have a copy of the Parents' Bill of Rights?

# Some Questions a **Student Teacher/Fieldwork Student** Should Ask the Cooperating Teacher and/or Principal:

- ❖ For additional security, can I be issued a school email account to use for communications? Or, is there another way to ensure security?
- ❖ What are the expectations for data privacy in the school? Does it have a policy for teachers?
- ❖ What forms of permission does the school already have in place for students (such as parent forms)?
- ❖ What is the best way to distribute permission slips for the purpose of video recording for observations, class assignments, and the edTPA?
- ❖ Is there a list of approved apps or online tools that are Education Law §2-d compliant for this school/school district, and that I can see for lesson planning purposes?
- ❖ May I have a copy of the Parents' Bill of Rights?

# Some Questions a **Faculty Member** Should Ask the Cooperating Teacher and/or Principal:

- ❖ For additional security, should I be issued a school email account or another way to use for communication?
- ❖ What are the expectations for data privacy in the school? Do they have a policy to which teachers will adhere?
- ❖ What forms of permission does the school already have in place for students (such as parent forms)?
- ❖ What is the best way to distribute permission slips for the purpose of video recording for observations, class assignments, and the edTPA?
- ❖ Is there a list of approved apps or online tools that are Education Law §2-d compliant for this school/school district that I can see for the purpose of advising my students?
- ❖ May I have a copy of the Parents' Bill of Rights? Who is the point person at the school?

# Quiz 4

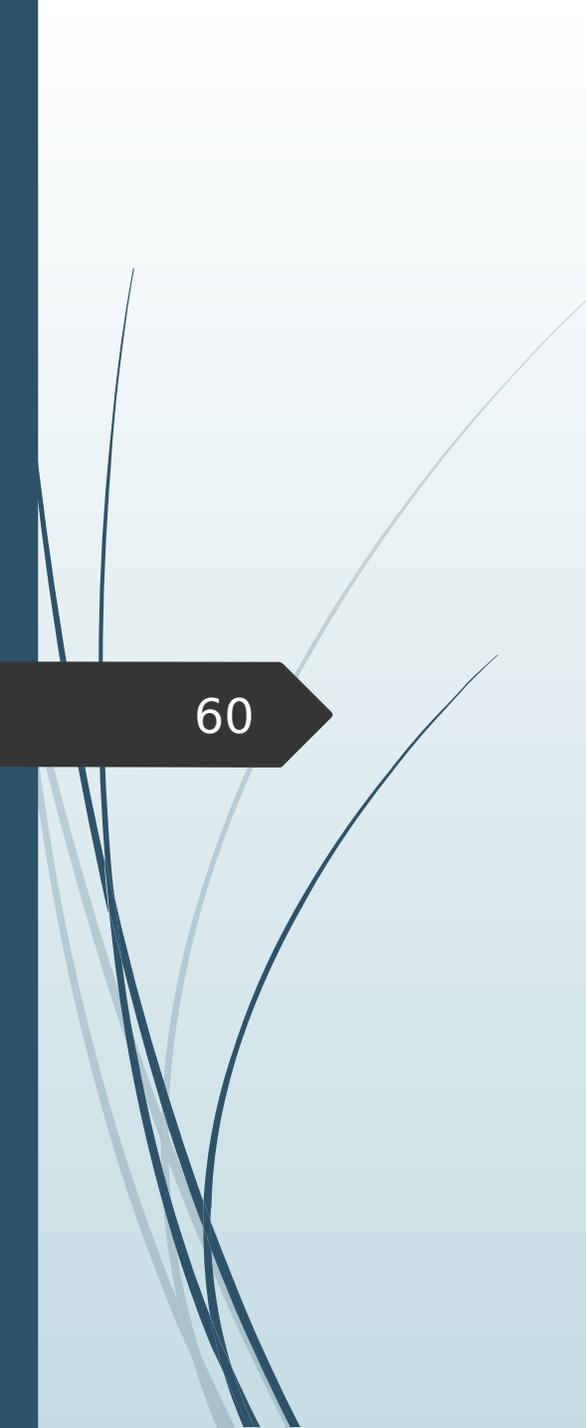
57

# 1. Which of the following is not an educational agency under NYS Education Law § 2-d?

- (a) The New York City Department of Education
- (b) Albany High School , in Albany, New York
- (c) New Jersey Department of Education
- (d) Westchester BOCES
- (e) Poughkeepsie City School District

2. Henri, is a student teacher at the King School. She emails her cooperating teacher from her private email about the triennial IEP meeting on Tanya Johnson that she attended, and asks a question about the counseling and speech services Tanya receives. In which of the following scenarios would this not be a violation of Education Law § 2-d?

- a) Henri asks her question using no personal identifying information about Tanya Johnson in her email, referring to her only as a student, and focuses on the services not the student receiving them.
- b) Henri attaches the IEP with handwritten questions on it to the email which is sent through a common provider, whose security does not include sophisticated encryption.
- c) Henri remembers that it is not a good idea to send documents such as IEPs via email, so she describes Tanya Johnson's behavior regarding the speech services in great detail so that the cooperating teacher understands her question better.
- d) Henri tries to do the right thing by encrypting her email, but she accidentally addresses it to her friend, whose email is only one letter different from her cooperating teachers', and she hits send before she catches her mistake.



60

Do you have any questions or points that need further clarification?

# THANK YOU FOR COMPLETING THIS MODULE!

For more information, visit these sites:

- ❖ <http://www.nysed.gov/data-privacy-security>
- ❖ <https://studentprivacy.ed.gov/search/node/pii>
- ❖ <https://www.nist.gov/cyberframework/resources>
- ❖ <https://www.youtube.com/watch?v=iqPmxHf2IAk>

# References

CA.GOV. *Health insurance portability & accountability act*. (2019, June 13). <https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx>

Drohan, J., Smith, A. & Smarra, N. (2020 August). *Education law 2d training for Hudson Valley teacher education consortium*. Thomas, Drohan, Waxman, Petigrow & Maye, LLP

Geronimo, V. (2014, Fall). FERPA “*Do’s & don’ts*” *guide for teachers*. Fordham University School of Law, Technology and Privacy Law. [https://www.fordham.edu/download/downloads/id/1850/09\\_-\\_dos\\_and\\_donts\\_for\\_teachers.pdf](https://www.fordham.edu/download/downloads/id/1850/09_-_dos_and_donts_for_teachers.pdf)

New York State Education Department. *Amendment to the regulations of the commissioner of education Part 121: Strengthening data privacy and security in ny state educational agencies to protect personally identifiable Information*. <http://www.nysed.gov/common/nysed/files/programs/data-privacy-security/part-121.pdf>

New York State Education Department. Data privacy and security (2015-2019). *Federal laws that protect student data*. (<http://www.nysed.gov/data-privacy-security/federal-laws-protect-student-data>)

New York State Education Department. Data privacy and security. *Frequently asked questions about data privacy and security*. <http://www.nysed.gov/data-privacy-security/frequently-asked-questions-about-data-privacy-and-security>

New York State Education Department. (2014-2019). Data privacy and security. *Part 121 of the Regulations of the commissioner of education*. <http://www.nysed.gov/data-privacy-security>

New York State Education Department. Data privacy and security. *Bill of rights for data privacy and security (parents' bill of rights)*.  
Da<http://www.nysed.gov/data-privacy-security/bill-rights-data-privacy-and-security-parents-bill-rights>

New York State Education Department. Data privacy and security (2015-2019). *Federal laws that protect student data*.  
(<http://www.nysed.gov/data-privacy-security/federal-laws-protect-student-data>

New York State Education Department. Data privacy and security. *Frequently asked questions about data privacy and security*.  
<http://www.nysed.gov/data-privacy-security/frequently-asked-questions-about-data-privacy-and-security>

New York State Education Department. (2014-2019). *Data privacy and security. Part 121 of the Regulations of the commissioner of education*.  
<http://www.nysed.gov/data-privacy-security>

Richmond, S. (2020, January 7). *Preparing for imminent changes in the New York State Education Law regarding data privacy*. News and Insights. <https://www.bsk.com/news-insights/preparing-for-imminent-changes-in-the-new-york-state-education-law-regarding-data-privacy>

Sirius Radio-The Michelangelo Signorie Show. (2015, November 20). *Cheri Kiesecker & Leonie Haimson on student privacy* [Video]. Class size matters. <https://www.classsizematters.org/video-cheri-kiesecker-leonie-haimson-on-student-privacy>

U.S. Department of Education. (2018, March 1). *Programs: Family educational rights and privacy act (FERPA)*. <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

U.S. Department of Education. *Protecting student privacy*. <https://studentprivacy.ed.gov/content/personally-identifiable-information-education-records>