2019
SUMMER LAW CONFERENCE

Protecting Digital Student Records and Responding to Data Breaches

Presented By: Julie M. Shaw, Esq., Partner
Shaw, Perelson, May & Lambert, LLP

Date: July 23, 2019

Introduction

2019
SUMMER LAW CONFERENCE

- In response to statewide opposition to the contractual relationship sought by SED with inBloom to house Personally Identifiable Information (PII) regarding all public school students, the New York State Legislature enacted §§ 2-c & 2-d of the Education Law, effective March 31, 2014.
- These provisions primarily address the electronic transmittal and storage of personally identifiable student data and teacher/principal Annual Professional Performance Review ("APPR") data by third-party contractors.

Introduction (Cont'd)

2019 SUMMER LAW CONFERENCE

- To be covered by Education Law §2-d, the data involved must be either:
  - Student personally identifiable information ("PII"); or
  - Teacher/Principal PII related to APPR data, as defined in Education Law §3012-c(10).

Introduction (Cont'd)

2019 SUMMER LAW CONFERENCE

- Education Law §2-d established the SED position of Chief Privacy Officer ("CPO").
- The Commissioner, in consultation with the CPO, was tasked with drafting regulations to implement §2-d.
- In 2017, the CPO created the Data Privacy Advisory Council, an advisory committee comprised of parents, diverse stakeholder groups and experts in the field, to provide input into various areas related to the regulations, and to receive input to develop further aspects of the Parents Bill of Rights for Data Privacy and Security ("PBR").

Proposed Part 121 Regulations

2019 SUMMER LAW CONFERENCE

- In January of 2019, proposed new Part 121 Commissioner's regulations to implement Education Law §2-d relating to protecting PII were considered by the Board of Regents. The draft regulations underwent a 60 day public comment period which closed on March 31, 2019.
- At the July 15, 2019 Board of Regents meeting, revised Part 121 Commissioner's regulations were presented to the Board of Regents, which will undergo another 45 day public comment period, after which the regulations will be considered by the Board of Regents for permanent adoption at its October 2019 meeting, to become effective October 23, 2019 (unless further modified following the new public comment period). The revised proposed regulations are available at: http://www.regents.nysed.gov/common/regents/files/719p12d1-%20REVISED.pdf.

Proposed Part 121 Regulations (Cont'd)

2019 SUMMER LAW CONFERENCE

- The revised proposed regulations outline requirements for Educational Agencies and Third-Party Contractors to ensure the security and privacy of PII.
- The revised proposed regulations include a definition of "Encryption" technology that cross-references the standards set forth at Education Law §2-d(5)(f)(5), for ensuring PII in motion or in custody will be unusable, unreadable, or indecipherable to unauthorized persons, which makes reference to HIPAA guidance.

Who is a Third Party Contractor?

2019 SUMMER LAW CONFERENCE

- A third-party contractor ("TPC") is "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..." *See* 8 NYCRR §121.1(s).
- An educational agency is defined as a BOCES, a school District, a school, or SED. 8 NYCRR §121.1(g).

2019 SUMMER LAW CONFERENCE

Bill of Rights for Data Privacy & Security

- Each public school district & BOCES was required to post on its website and issue to each of its third party vendors by July 29, 2014 its Parents Bill of Rights for Data Privacy & Security ("bill of rights").
- The Commissioner's regulations at §121.3, in conjunction with Education Law §2-d(3), set forth the requirements for the bill of rights.

Bill of Rights (Cont'd)

2019 SUMMER LAW CONFERENCE

Contents of the Bill of Rights (Education Law §2-d[3][b]):

- A Student's PII cannot be sold or released for any commercial purposes;
- Parental right to inspect and review the complete contents of their child's education record;
- The Educational Agency has adopted safeguards associated with industry standards and best practices under state and federal law to protect confidentiality of student PII, including encryption, firewalls and password protection, which must be in place whenever such data is stored or transferred;

Bill of Rights (Cont'd)

2019 SUMMER LAW CONFERENCE

- A complete list of all student data elements collected by the State is available for public review at: http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/collected-data-elements.pdf;
- Parents have the rights to have complaints about possible breaches of student data addressed. Complaints should be addressed to: (provide contact information for the designated official's phone number, email and mailing address).

Bill of Rights: Supplemental Information

2019 SUMMER LAW CONFERENCE

- The bill of rights shall include the following supplemental information for each contract an educational agency enters into with a TPC, where the TPC receives PII:
  - A statement of the exclusive purpose(s) for which the student, teacher or principal data will be used by the TPC, as defined in the contract;
  - How the TPC will assure legal compliance by its subcontractors with state and federal laws and regulations governing data privacy and security;

Bill of Rights: Supplemental Information (Cont'd)

2019 SUMMER LAW CONFERENCE

- The duration of the contract that sets forth its expiration date, and what happens to the data when the TPC's contract expires (e.g. whether, when and in what format the data will be returned to the educational agency, and/or whether, when and how the data will be destroyed);
- If and how a parent, student, teacher or principal may challenge the accuracy of the data that is collected;
- Where the data will be stored to protect data security, and the security protections taken to ensure the data will be protected and data security and privacy risks mitigated; and
- How data will be protected using encryption when in motion and at rest.

Publication of Bill of Rights & Supplemental Information

2019 SUMMER LAW CONFERENCE

- Each educational agency must publish its bill of rights and the supplemental information related to each contract with a TPC receiving PII on its website. *See* §121.3(a).
- The bill of rights and supplemental information related to each TPC receiving PII may be redacted "to the extent necessary to safeguard the privacy and/or security of the educational agency's data and/or technology infrastructure". *See* §121.3(d) & (e).
- The bill of rights must also be attached to each contract with a TPC receiving PII. *See* §121.3(b).

Complaints of Breach or Unauthorized Release of PII

2019 SUMMER LAW CONFERENCE

- Educational agencies must establish procedures for parents and eligible students to file complaints about breaches or unauthorized releases of PII.
- An educational agency *may* require complaints to be submitted in writing.
- The complaint procedures require a prompt acknowledgement upon receipt of the complaint and a prompt investigation of the complaint, with necessary precautions taken to protect any PII.
- A report with findings regarding the investigation must be issued promptly, but not later than sixty (60) days after the receipt of the complaint (unless additional time is needed where the response may compromise security or impede a law enforcement investigation).

Data Security & Privacy Standard

2019 SUMMER LAW CONFERENCE

NIST Cybersecurity Framework, Version 1.1:

School Obligation: Data Security & Privacy Policy

2019 SUMMER LAW CONFERENCE

- By July 1, 2020, each educational agency must adopt a data security and privacy policy that implements the requirements of Part 121, and aligns with the NIST Cybersecurity Framework, Version 1.1.
- SED is supposed to issue at least one model policy as per Education Law §2-d(5)(a).

School Obligation: Data Security & Privacy Policy (Cont'd)

2019 SUMMER LAW CONFERENCE

- Policy must address the data privacy protections consistent with Education Law §2-d(5), committing to the following principles:
  - Every use and disclosure of student PII will be for the benefit of the student and the educational agency (e.g. improve academics, empower parents and students with information and/or advance efficient and effective school operations).
  - PII will not be included in public reports or other documents.
  - The policy shall include all of the protections afforded under federal laws and regulations regarding student data privacy (i.e. FERPA and IDEA).
  - Policy must be posted on the educational agency's website, with notice of the policy provided to all officers and employees.

Data Security & Privacy Plan

2019 SUMMER LAW CONFERENCE

- A feature of every contract with a TPC is a required elaboration about how the contractor will implement all of the requirements of the federal and state student information privacy laws, as well as the local requirements of the contracting educational agency.
- *See* §121.6(a)(1)-(7).

Data Security & Privacy Plan (Cont'd)

2019 SUMMER LAW CONFERENCE

- As per §121.6 of the proposed revised regulations, each contract an educational agency enters into with a TPC must include a data security and privacy plan that is accepted by the educational agency, which:
  - Outlines how the TPC will implement all State, federal and local data security and privacy contract requirements over the term of the contract, consistent with the educational agency's data security and privacy policy;
  - Specifies the administrative, operational and technical safeguards and practices the TPC has in place to protect PII that it will receive under the contract;
  - Demonstrates that the TPC complies with the requirements of §121.3(c);

Data Security & Privacy Plan (Cont'd)

2019 SUMMER LAW CONFERENCE

- Specifies how officers or employees of the TPC who have access to PII will receive training on federal and state privacy laws before commencing work on the contract involving access to PII;
- Specifies if the TPC will use sub-contractors and if so, how it will manage those relationships and contract to ensure the protection of PII;
- Specifies how TPCs will manage data security and privacy incidents that implicate PII, including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency; and
- Describes whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the TPC when the contract is terminated or expires.

School Obligation: Training for Educational Agency Officers & Employees

2019 SUMMER LAW CONFERENCE

- Educational agencies will be required to provide annual training on information privacy and security awareness for those employees and officers with access to PII.
- Such training may be done through on-line sources and may be integrated within other annual training programs. *See* 8 NYCRR §121.7.

School Obligation: Appoint Data Protection Officer

2019 SUMMER LAW CONFERENCE

- Need not be a separate position and may be stipended.
- Requires training in state and federal privacy laws and regulations.
- Serves as the "point person" for contact by parents, eligible students, staff, the CPO and other agencies.
- Responsible for implementing the policy required by the Part 121 Regulations. *See* §121.8.

2019 SUMMER LAW CONFERENCE

Additional Third Party Contractors Requirements

- Adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework Version 1.1 (§121.9[a][1]);
- Comply with Education Law §2-d and the Part 121 regulations, as well as the policy of the educational agency with whom it contracts (§121.9[a][2]).
- Limit internal access to PII to only those employees or subcontractors that need access to the data (§121.9[a][3]).
- Not use PII for any purpose except as authorized by contract (§121.9[a][4]).

2019 SUMMER LAW CONFERENCE

Additional Third Party Contractors Requirements (Cont'd)

- Not disclose PII unless there is prior written consent given by the parent or by an eligible student (18 years of age or older), except for authorized representatives of the TPC to the extent they are carrying out the contract; or unless disclosure is required by statute or court order (§121.9[a][5][i]&[ii]).
- Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody (§121.9[a][6]).
- Use encryption to protect PII in its custody while in motion or in custody (§121.9[a][7]).
- Not sell, use or otherwise disclose PII for any marketing or commercial purpose or permit another party to do so (§121.9[a][8]).
- The revised proposed regulations note that when a parent or eligible student requests a service from a TPC and provides express consent to the use or disclosure of such PII by the TPC for the purposes of providing the requested product or service, such use by the TPC shall not be deemed to be a marketing or commercial purpose. *See* §121.9(c).

Reports and Notifications of Breaches & Unauthorized Disclosures

2019 SUMMER LAW CONFERENCE

- The regulations set forth a series of disclosures that must be made within specified timelines in the event of a PII breach or unauthorized disclosure.
  - TPCs must disclose known breaches or unauthorized disclosures to the BOCES or school district or within 7 calendar days after discovery thereof; and
  - The BOCES or school district has up to 10 calendar days from the date of the notification by the TPC to inform the CPO.
  - A regulatory duty exists for TPCs to cooperate with law enforcement and the educational agency in their investigatory efforts into the breach or unauthorized release of the PII. *See* §121.10(a)-(c)

Reports and Notifications of Breaches & Unauthorized Disclosures (Cont'd)

2019 SUMMER LAW CONFERENCE

- Any time there is a breach or unauthorized release of PII discovered by the educational agency, it must report the same to the CPO within 10 calendar days after the discovery (§121.10[d]).
- Educational agencies are to notify affected parents, eligible students, teachers and/or principals not more than 60 calendar days after discovery of a breach or unauthorized release of PII, unless the notification would interfere with an ongoing law enforcement investigation or disclose an unfixed security vulnerability, in which case the notification must be made within 7 calendar days after the vulnerability is remedied or the risk of interfering with a law enforcement investigation ends (§121.10[e]).
- In the event that the breach or unauthorized release is attributed to the TPC, then the TPC shall pay for or promptly reimburse the educational agency for the cost of the notification (§121.10[f]).

Notification of Breach or Unauthorized Disclosures

2019 SUMMER LAW CONFERENCE

- Notice must be provided by first-class mail, email, or telephone, and shall include:
  - A brief description of the breach or unauthorized release;
  - Dates of the incident and the discovery, if known;
  - Description of the types of PII affected;
  - An estimate of the number of records affected;
  - Brief description of the educational agency's plan to investigate; and
  - Contact information for representatives who may provide assistance if there are additional questions. *See* §121.10(g).

TPC Civil Penalties

2019 SUMMER LAW CONFERENCE

- If a TPC fails to notify an educational agency with which it contracts in the "most expedient way possible and without unreasonable delay" of a breach or unauthorized release of student data, or teacher or principal data, each such violation shall be punishable by a civil penalty of the greater of $5,000 or $10 per student, teacher and principal whose data was released, but not to exceed $150,000. *See* §121.11(a).
- Each violation by a TPC of any other provision of Education Law §2-d shall receive a civil penalty of:
  - Up to $1,000 for a first violation;
  - Up to $5,000 for a second violation by the TPC involving the same data;
  - Up to $10,000 for any subsequent violation by the TPC involving the same data. *See* §121.11(b).

TPC Civil Penalties (Cont'd)

2019 SUMMER LAW CONFERENCE

- The CPO is to investigate reports of breaches or unauthorized release of PII by TPCs. The Investigation may include:
  - Submission of documentation;
  - Testimony;
  - Visitation to the TPC;
  - Examination and/or inspection of the TPC's facilities and/or records by the CPO.

  See §121.11(c)

TPC Civil Penalties (Cont'd)

2019 SUMMER LAW CONFERENCE

- If, after investigating, the CPO determined that the TPC, through its acts or omissions, caused the breach or unauthorized release, then the CPO shall notify the TPC of such findings, and the TPC shall have the opportunity to submit a written response within 30 days. §121.11(c)
- Should the CPO determine the incident is a violation of Education Law §2-d, the CPO is authorized to:
  - Order the TPC be precluded from accessing PII from the affected educational agency for a fixed period of up to 5 years;
  - Order a TPC who knowingly or recklessly allowed for a breach or unauthorized release of PII be precluded from accessing PII from any educational agency in the state for a fixed period up to 5 years;
  - Order that a TPC who knowingly or recklessly allowed for a breach or unauthorized release of PII shall not be deemed a responsible bidder or offeror on any contract with an educational agency that involves sharing of PII, for a fixed period of up to 5 years.
  - Require that the TPC provide additional training regarding confidentiality of PII to all its officers and employees with reasonable access to such data and certify that such training has been performed at the TPC's expense. *See* §121.11(d)(1)-(4).

TPC Civil Penalties (Cont'd)

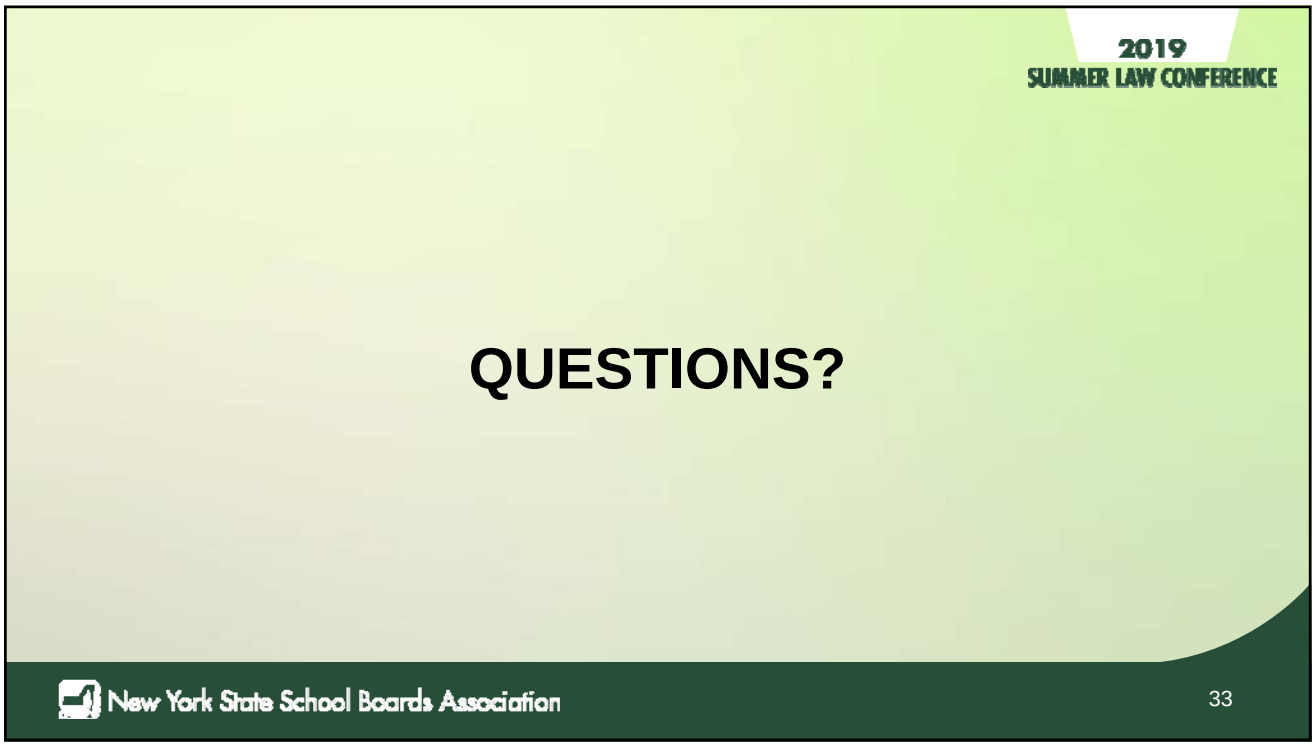
2019 SUMMER LAW CONFERENCE

- If the CPO determines that the unauthorized release of PII on the part of the TPC was inadvertent and done without intent, knowledge, recklessness or gross negligence, the Commissioner may determine that no penalty be issued to the TPC. *See* §121.11(f) & Education Law §2-d(6)(e)(5).
- There are no civil penalties for a data breach or unauthorized release of PII by an educational agency.

Implementation and Enforcement

2019 SUMMER LAW CONFERENCE

- As per Education Law §2-d(7)(c), there is no private right of action against an educational agency.


2019
SUMMER LAW CONFERENCE
QUESTIONS?
New York State School Boards Association
33