student's privacy rights under FERPA. Complete student records are maintained by schools and school districts and not at NYSED, which is the secondary repository of data, and NYSED make amendments to school or school district records. Schools and school districts are in the best position to make corrections to students' education records.

3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent (including but not limited to disclosure under specified conditions to: (i) school officials within the school or school district with legitimate educational interests; (ii) officials of another school for purposes of enrollment or transfer; (iii) third party contractors providing services to, or performing functions for an educational agency; (iv) authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as NYSED; (iv) (v) organizations conducting studies for or on behalf of educational agencies) and (vi) the public where the school or school district has designated certain student data as "directory information" (described below). The attached FERPA Model Notification of Rights more fully describes the exceptions to the consent requirement under FERPA).

4. Where a school or school district has a policy of releasing "directory information" from student records, the parent has a right to refuse to let the school or school district designate any all of such information as directory information. Directory information, as defined in federal regulations, includes: the student's name, address, telephone number, email address, photograph, date and place of birth, major field of study, grade level, enrollment status, dates of attendance, participation in officially recognized activities and sports, weight and height of members of athletic teams, s8d [(s8d LanTd c-1(e)4 nTur)3 (br)3erg

A more detailed description of the PPPL is available from the Committee on Open Government of the New York Department of State. Guidance on what you should know about the PPPL can be accessed at http://www.dos.ny.gov/coog/shldno1.html. The Committee on Open Government's address is Committee on Open Government, Department of State, One Commerce Plaza, 99 Washington Avenue, suite 650, Albany, NY 12231, their email address is coog@dos.ny.gov, and their telephone number is (518) 474-2518.

C. Parents' Rights Under Education Law §2-d relating to Unauthorized Release of Personally Identifiable Information

1. What "educational agencies" are included in the requirements of Education Law §2-d?

- The New York State Education Department ("NYSED");
- Each public school district;
- Each Board of Cooperative Educational Services or BOCES; and
- All schools that are:
  - a public elementary or secondary school;
  - a universal pre-kindergarten program authorized pursuant to Education Law §3602-e;
  - an approved provider of preschool special education services;
  - any other publicly funded pre-kindergarten program;
  - a school serving children in a special act school district as defined in Education Law 4001; or
  - certain schools for the education of students with disabilities - an approved private school, a state-supported school subject to the provisions of Article 85 of the Education Law, or a state-operated school subject to the provisions of Article 87 or 88 of the Education Law.

(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

3. What kind of student data is *not* subject to the confidentiality and security requirements of Education Law §2-d?

The confidentiality and privacy provisions of Education Law §2-d and FERPA extend only to PII, and not to student data that is 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 is not considered to be PII and is not within the purview of Education Law §2-d or within the scope of this Parents' Bill of Rights.

4. What are my rights under Education Law § 2-d as a parent regarding my student's PII?

Education Law §2-d ensures that, in addition to all of the protections and rights of parents under the federal FERPA law, certain rights will also be provided under the Education Law. These rights include, but are not limited to, the following elements:

(A) A student's PII cannot be sold or released by the educational agency for any commercial or marketing purposes.

- PII may

- The policies will also require security measures when providing student data to parents, to ensure that only authorized individuals receive such data. A parent may be asked for information or verifications reasonably necessary to ensure that he or she is in fact the student's parent and is authorized to receive such information pursuant to law.

(C) State and federal laws protect the confidentiality of PII, and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

Education Law §2-d also specifically provides certain limitations on the collection of data by educational agencies, including, but not limited to:

(A) A mandate that, except as otherwise specifically authorized by law, NYSED shall only collect PII relating to an educational purpose;

(B) NYSED may only require districts to submit PII, including data on disability status and student suspensions, where such release is required by law or otherwise authorized under FERPA and/or the New York State Personal Privacy Law; and

(C) Except as required by law or in the case of educational enrollment data, school districts shall not report to NYSED student data regarding juvenile delinquency records, criminal records, medical and health records or student biometric information.

(D) Parents may access the NYSED Student Data Elements List, a complete list of all student data elements collected by NYSED, at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or may obtain a copy of this list by writing to the Office of Information & Reporting Services

- When appointed, the Chief Privacy Officer of NYSED will also provide a procedure within NYSED whereby parents, students, teachers, superintendents, school board members, principals, and other persons or entities may request information pertaining to student data or teacher or principal APPR data in a timely and efficient manner.

5. Must additional elements be included in the Parents' Bill of Rights.?

Yes**.** For purposes of further ensuring confidentiality and security of student data, as an appendix to the Parents' Bill of Rights each contract an educational agency enters into with a third party contractor shall include the following supplemental information:

(A) the exclusive purposes for which the student data, or teacher or principal data, will be used;

(B) how the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

(C) when the agreement with the third party contractor expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

(D) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

(E) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

a. In addition, the Chief Privacy Officer, with input from parents and other education and expert stakeholders, is required to develop additional elements of the Parents' Bill of Rights to be prescribed in Regulations of the Commissioner.

6. What protections are required to be in place if an educational agency contracts with a third party contractor to provide services, and the contract requires the disclosure of PII to the third party contractor?

Education Law §2-d provides very specific protections for contracts with "third party contractors", defined as 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. The term "third party contractor" also includes an educational partnership organization that receives student and/or teacher or principal APPR data from a school district to carry out its responsibilities pursuant to Education Law §211-e, and a not-for-profit corporation or other non-profit organization, which are not themselves covered by the definition of an "educational agency."

any party relating to the alleged improper disclosure of student data or teacher or principal APPR data.

Where there is a breach and unauthorized release of PII by a by a third party contractor or its assignees (e.g., a subcontractor): (i) the third party contractor must notify the educational agency of the breach in the most expedient way possible and without unreasonable delay; (ii) the educational agency must notify the parent in the most expedient way possible and without unreasonable delay; and (iii) the third party contractor may be subject to certain penalties including, but not limited to, a monetary fine; mandatory training regarding federal and state law governing the confidentiality of student data, or teacher or principal APPR data; and preclusion from accessing any student data, or teacher or principal APPR data, from an educational agency for a fixed period up to five years.

8. Data Security and Privacy Standards

Upon appointment, NYSED's Chief Privacy Officer will be required to develop, with input from experts, standards for educational agency data security and privacy policies. The Commissioner will then promulgate regulations implementing these data security and privacy standards.

9. No Private Right of Action

interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

[Optional] Upon request, the school discloses education records without consent to officials of another school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer. [NOTE: FERPA requires a school district to make a reasonable attempt to notify the parent or student of the records request unless it states in its annual notification that it intends to forward records on request.]

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the [School] to comply with the requirements of FERPA. The name and address of the Office that administers FERPA are:

    Family Policy Compliance Office
    U.S. Department of Education
    400 Maryland Avenue, SW
    Washington, DC 20202

[NOTE: In addition, a school may want to include its directory information public notice, as required by §99.37 of the regulations, with its annual notification of rights under FERPA.]

[Optional] See the list below of the disclosures that elementary and secondary schools may make without consent.

FERPA permits the disclosure of PII from students' education records, without consent of the parent or eligible student, if the disclosure meets certain conditions found in §99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the parent or eligible student, §99.32 of the FERPA regulations requires the school to record the disclosure. Parents and eligible students have a right to inspect and review the record of disclosures. A school may disclose PII from the education records of a student without obtaining prior written consent of the parents or the eligible student –

- To other school officials, including teachers, within the educational agency or institution whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in §99.31(a)(1)(i)(B)(*1*) - (a)(1)(i)(B)(*2*)(

such as the State educational agency in the parent or eligible student's State (SEA). Disclosures under this provision may be made, subject to the requirements of §99.35, in connection with an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35)

- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4))

- To State and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a State statute that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records were released, subject to §99.38. (§99.31(a)(5))

- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§99.31(a)(6))

- To accrediting organizations to carry out their accrediting functions. (§99.31(a)(7))

- To parents of an eligible student if the student is a dependent for IRS tax purposes. (§99.31(a)(8))

- To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9))

- To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10)

- Information the school has designated as "directory information" under §99.37. (§99.31(a)(11))

APPENDIX S-1
Attachment To Parents' Bill Of Rights
For Contracts Involving Disclosure of Certain Personally Identifiable Information

Education Law §2-d, added by Ch. 56 of the Laws of 2014, requires that a Parents' Bill of Rights be attached to every contract with a third-party contractor (as defined in the law) which involves the disclosure of personally identifiable information (PII) derived from student education records ("Student Data"), or certain teacher/principal information regarding annual professional performance evaluations that is confidential pursuant to Education Law §30212-c ("APPR Data"). Each such Contr stude9999999-1 (s-6 (r)4 (9)4 i)(9)4 (9)4cl8d2 (ude)4

AMI has been providing records management and scanning services since 1984. The organization not only uses the market's top imaging software and state-of-the-art hardware, but also meets several industry standards in the industry– ANSI (American National Standards Institute), AIIM (Association for Information and Image Management), and ASCII (American Standard Code for Information Interchange). AMI understands the needs for security while managing sensitive documents, and currently provides these services for government agencies, insurance companies, engineering firms, and medical facilities.

In all cases where Questar works with other vendors, we have policies and procedures in place to ensure that the vendors meet our specifications and adhere to our strict security standards. They include the requirement that Questar staff personally vet the vendor, and, for the most part, we direct work to proven partners, like AMI.

Questar policies include the requirement that staff members of selected vendors are required to sign non-disclosure agreements and that only a limited number of a vendor's staff members work with materials containing secure items.

Questar staff also conduct onsite visits to all our key vendor and subcontractor facilities before and during production work. These visits are performed by senior staff and concentrate on basic project requirement reviews, security, quality control procedures and scheduling (planned production schedule and contingency planning).

We work directly with senior executives and production management staff to ensure all aspects of the project are understood.

After each project is completed, Questar conducts a debrief with each of our vendors and subcontractors to provide feedback and process improvement inputs and planning for the next test administration cycle.

As detailed in Section 3, AMI's designated staffing resources include a keen focus on ensuring security related to the scanning of the pilot and field tests. Carol Benardella and Ken O'Brien will work with Mr. Thoms to inspect quality and add another level of integrity to the work. To ensure that we scan every answer booklet correctly, Jason Garey and Justine Rodriguez will retain log notes for each scanning instance.

Prior to receipt of any materials, Mr. O'Brien of AMI will lead security training in handling sensitive materials as well as technical guidance well in advance of the arrival of materials.

In terms of physical security, AMI's 15,000 square foot facility site in Lacey Township was designed specifically as a records management facility. As such, security has been designed into the site with the utmost attention. The facility is protected by a state-of-the-art system.

Warehouse areas are accessible to warehouse and management personnel only. The warehouse

We recognize the sensitive nature of testing materials, individual student information, test scores, and statistical analyses. We will emphasize secure handling of students' Personally Identifying Information (PII) and adherence to FERPA throughout the contract at every stage of the process. Client data is stored on dedicated, isolated server environments that are highly redundant and supported by robust back-up strategies.

The servers reside in Minnesota within an Uptime Institute certified, Tier-III constructed data center facility that provides multiple layers of physical security, including 24x7x365 on-site monitoring and hardened construction. Questar also utilizes AES 256-bit SSL (Secure Socket Layer) technology, commonly known as HTTPS, which ensures that all transmissions of student data occur over secure network connections with authentication and encryption technologies.

Transmissions are encrypted with unique keys that ensure only authorized parties can decrypt the data. None of the software components can expose test content, student, or response data without specific and valid credentials provided by an authorized administrator or student. Questar also stores all secure data in encrypted format while at rest.

For this work, we will utilize our online scoring application, ScorePoint. ScorePoint, like all of Questar online applications (item authoring and test development system, online hand-scoring system, online test administration, etc.), is housed in secure enterprise-grade SQL database servers that are only accessible via encrypted HTTPS protocol. The underlying storage for the systems are highly distributed, redundant, multi-tenant, and flexibly supports the partitioning of data by client as well as by assessment function.

Access to these systems is controlled by Questar's comprehensive identity management, authentication, and authorization process, as well as role-based access controls. Roles are customizable, so that Questar is able to setup and control with great specificity who is able to access systems, and what actions they are able to take upon accessing.

Additional ScorePoint security features include:

- Usernames and passwords are required to access ScorePoint. Following the rubric and ScorePoint training and qualifying, the ScorePoint administrator activates individual scorers in the system, which allows them to score operational student responses.
- ScorePoint strictly controls access rights for each scorer to ensure that a scorer is only presented with student responses they are approved to score.
- Data and responses are available to scorers only through the secure application interface. The data and responses are not distributed to any other network, database, or system.

Questar engages annually with auditors to conduct vulnerability assessments of its information security controls. These audits assess the controls for both the internal and external environments by reviewing configurations of technical equipment, reviewing configurations of critical preventative and detective controls (e.g., anti-malware, backup system, email filtering, and logging), and reviewing authorization configurations for the Windows domain.

Physical controls are also audited to assess the sufficiency in the detective, corrective, and protective controls implemented to safeguard all of Questar's facilities. Auditors also evaluate protection measures used when handling customer private information before and during business operation hours. The final vulnerability report compilation of findings is gathered and reviewed. Questar takes corrective action to address concerns immediately.

Sec re FTP fo Enc p ed Da a T an fe

For the transfer of large electronic files that contain secure information, we will develop and maintain a secure FTP site. The site will house all proj.7e (in)-1.9 (a)6.9 (s)6(a)7 (ll2este)eg(in)-1.9 (a.s1/5 (73