Appendix S
PARENTS' BILL OF RIGHTS
FOR DATA PRIVACY AND SECURITY

To satisfy their responsibilities regarding the provision of education to students in pre-kindergarten through grade twelve, "educational agencies" (as defined below) in the State of New York collect and maintain certain personally identifiable information from the education records of their students. As part of the Common Core Implementation Reform Act, Education Law §2-d requires that each educational agency in the State of New York must develop a Parents' Bill of Rights for Data Privacy and Security (Parents' Bill of Rights). The Parents' Bill of Rights must be published on the website of each educational agency, and must be included with every contract the educational agency enters into with a "third party contractor" (as defined below) where the third party contractor receives student data, or certain protected teacher/principal data related to Annual Professional Performance Reviews that is designated as confidential pursuant to Education Law §3012-c ("APPR data").

The purpose of the Parents' Bill of Rights is to inform 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) of the legal requirements regarding privacy, security and use of student data. In addition to the federal Family Educational Rights and Privacy Act (FERPA), Education Law §2-d provides important new protections for student data, and new remedies for breaches of the responsibility to maintain the security and confidentiality of such data.

A. <u>What are the essential parents' rights under the Family Educational Rights and Privacy Act (FERPA) relating to personally identifiable information in their child's student records?</u>

The rights of parents under FERPA are summarized in the Model Notification of Rights prepared by the United States Department of Education for use by schools in providing annual notification of rights to parents. It can be accessed at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html, and a copy is attached to this Parents' Bill of Rights. Complete student records are maintained by schools and school districts, and not at the New York State Education Department (NYSED). Further, NYSED would need to establish and implement a means to verify a parent's identity and right of access to records before processing a request for records to the school or school district. Therefore, requests to access student records will be most efficiently managed at the school or school district level.

Parents' rights under FERPA include:

1. The right to inspect and review the student's education records within 45 days after the day the school or school district receives a request for access.

2. The right to request amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the

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, degrees, honors and awards received and the most recent educational agency or institution attended. Where disclosure without consent is otherwise authorized under FERPA, however, a parent's refusal to permit disclosure of directory information does not prevent disclosure pursuant to such separate authorization.

5. 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.

B. <u>What are parents' rights under the Personal Privacy Protection Law (PPPL), Article 6-A of the Public Officers Law relating to records held by State agencies?</u>

The PPPL (Public Officers Law §§91-99) applies to all records of State agencies and is not specific to student records or to parents. It does not apply to school districts or other local educational agencies. It imposes duties on State agencies to have procedures in place to protect from disclosure of "personal information," defined as information which because of a name, number, symbol, mark or other identifier, can be used to identify a "data subject" (in this case the student or the student's parent). Like FERPA, the PPPL confers a right on the data subject (student or the student's parent) to access to State agency records relating to them and requires State agencies to have procedures for correction or amendment of records.

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 Education Law Article 85, or a state-operated school subject to Education Law Article 87 or 88.

2. What kind of student data is subject to the confidentiality and security requirements of Education Law §2-d?

The law applies to personally identifiable information contained in student records of an educational agency listed above. The term "student" refers to any person attending or seeking to enroll in an educational agency, and the term "personally identifiable information" ("PII") uses the definition provided in FERPA. Under FERPA, personally identifiable information or PII includes, but is not limited to:

(a) The student's name;
(b) The name of the student's parent or other family members;
(c) The address of the student or student's family;
(d) A personal identifier, such as the student's social security number, student number, or biometric record;
(e) Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name[1];

[1] Please note that NYSED does not collect certain information defined in FERPA, such as students' social security numbers, biometric records, mother's maiden name (unless used as the mother's legal name).

(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 be used for purposes of a contract that provides payment to a vendor for providing services to an educational agency as permitted by law.
- However, sale of PII to a third party solely for commercial purposes or receipt of payment by an educational agency, or disclosure of PII that is not related to a service being provided to the educational agency, is strictly prohibited.

(B) Parents have the right to inspect and review the complete contents of their child's education record including any student data stored or maintained by an educational agency.

- This right of inspection is consistent with the requirements of FERPA. In addition to the right of inspection of the educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student's educational record.
- NYSED will develop policies for annual notification by educational agencies to parents regarding the right to request student data. Such policies will specify a reasonable time for the educational agency to comply with such requests.

- 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, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234; and

(E) Parents have the right to file complaints with an educational agency about possible breaches of student data by that educational agency's third party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov. The complaint process is under development and will be established through regulations to be proposed by NYSED's Chief Privacy Officer, who has not yet been appointed.

- Specifically, the Commissioner of Education, after consultation with the Chief Privacy Officer, will promulgate regulations establishing procedures for the submission of complaints from parents, classroom teachers or building principals, or other staff of an educational agency, making allegations of improper disclosure of student data and/or teacher or principal APPR data by a third party contractor or its officers, employees or assignees.

- 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."

Services of a third party contractor covered under Education Law §2-d include, but 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 state, federal, and local 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. However, the standards for an educational agency's policy on data security and privacy must be prescribed in Regulations of the Commissioner that have not yet been promulgated. 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 shall:

- limit internal access to education records to those individuals that are determined to have legitimate educational interests
- not use the education records for any other purposes than those explicitly authorized in its contract;
- except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any PII to any other party (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;
- maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody; and
- use encryption technology to protect data while in motion or in its custody from unauthorized disclosure.

7. What steps can and must be taken in the event of a breach of confidentiality or security?

Upon receipt of a complaint or other information indicating that a third party contractor may have improperly disclosed student data, or teacher or principal APPR data, NYSED's Chief Privacy Officer is authorized to investigate, visit, examine and inspect the third party contractor's facilities and records and obtain documentation from, or require the testimony of,

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

Please note that Education Law §2-d explicitly states that it does not create a private right of action against NYSED or any other educational agency, such as a school, school district or BOCES.

ATTACHMENT

Model Notification of Rights under FERPA for Elementary and Secondary Schools

The Family Educational Rights and Privacy Act (FERPA) affords parents and students who are 18 years of age or older ("eligible students") certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days after the day the [Name of school ("School")] receives a request for access.

   Parents or eligible students should submit to the school principal [or appropriate school official] a written request that identifies the records they wish to inspect. The school official will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.

2. The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.

   Parents or eligible students who wish to ask the [School] to amend a record should write the school principal [or appropriate school official], clearly identify the part of the record they want changed, and specify why it should be changed. If the school decides not to amend the record as requested by the parent or eligible student, the school will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.

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.

   One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. A school official is a person employed by the school as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel) or a person serving on the school board. A school official also may include a volunteer or contractor outside of the school who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, medical consultant, or therapist; a parent or student volunteering to serve on an official committee, such as a disciplinary or grievance committee; or a parent, student, or other volunteer assisting another school official in performing his or her tasks. A school official has a legitimate educational

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*) are met. (§99.31(a)(1))

- To officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of §99.34. (§99.31(a)(2))

- To 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 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 Contract must include this completed Attachment to provide specific information about the use of such data by the Contractor.

1. Specify whether this Contract involves disclosure to the Contractor of Student Data, APPR Data, or both.

   ☑ Disclosure of Student Data

   ☐ Disclosure of APPR Data

2. Describe the exclusive purposes for which the Student Data or APPR Data will be used in the performance of this contract.

   In order to perform the work called for in this RFP, the contractor is given access to student field test booklets on which the students have hand written their names and their school name and hand written responses to field test questions. No other personally identifiable information about the student is provided to the contractor.

3. Identify any subcontractors or other persons/entities with whom the Contractor will share the Student Data or APPR in the performance of this Contract, and describe how the Contractor will ensure that such persons/entities will abide by the data protection and security requirements of the Contract.

   Subcontractors or other entities with whom the Contractor will share data:

   In keeping with our commitment to fully meet NYSED's Minority and Women-Owned Business Enterprises (M/WBE) participation goals, we are joined in our proposed solution by two quality vendors: Alternative Micrographics, Inc. (AMI) and Let's be Direct, LLC.

   While we will not be sharing data files with Let's be Direct, it may be possible that, in the course of doing the necessary work, select subcontractor staff members may need to have access to secure data. Questar works with a very limited number of proven subcontractors. In such circumstances where we do work with a subcontractor, we strictly limit the access to student data or other secure information, which is the same standard we have for our own employees. The staff members of our subcontractors are also educated on Questar's security standards and are required to sign confidentiality and non-disclosure agreements.

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 area is secured for record storage pre and post scanning. All entrances and warehouse bay doors are gated and recorded for security. All guests are required to log in after allowed entry to the building. Keypad entry to the facility ensures that only employees can enter AMI.

AMI receives yearly security system certifications from both a third-party and the state of New Jersey, ensuring the highest level of security for your documents.

In the event the Contractor engages a Subcontractor or otherwise shares Student Data or APPR Data with any other entity, Contractor acknowledges and agrees that before any such data is shared with a Contractor or another entity, such party must agree in writing to be bound by the confidentiality and data protection provisions set forth in this Contract including, but not limited to, the "Data Security and Privacy Plan" set forth in Appendix R. Upon termination of the agreement between the Contractor and a Subcontractor or other entity, Contractor acknowledges and agrees that it is responsible for ensuring that all Student Data or APPR Data shared by the Contractor must be returned to Contractor or otherwise destroyed as provided in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

4. Specify the expiration date of the Contract, and explain what will happen to the Student Data or APPR Data in the Contractor's possession, or the possession of any person/entity described in response to Paragraph 3, upon the expiration or earlier termination of the Contract.

   Contract expiration date: 12/31/24

   ☑ Contractor agrees to return the Student Data or APPR Data to NYSED consistent with the protocols set forth in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

   ☐ Contractor agrees to securely destroy the Student Data or APPR Data consistent with the protocols set forth in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

5. State whether the Contractor will be collecting any data from or pertaining to students derived from the student's education record, or pertaining to teachers or principals' annual professional performance evaluation pursuant to the Contract, and explain if and how a parent, student, eligible student (a student eighteen years or older), teacher or principal may challenge the accuracy of the Student Data or APPR data that is collected.

   ☒ Student Data

   ☐ APPR Data

   Any challenges to the accuracy of any of the Student Data or APPR Data shared pursuant to this Contract should be addressed to the school, educational agency or entity which produced, generated or otherwise created such data.

6. Describe where the Student Data or APPR Data will be stored (in a manner that does not jeopardize data security), and the security protections taken to ensure that the data will be protected, including whether such data will be encrypted.

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.

To ensure backup and recovery of responses, we execute incremental backups. Complete backups are performed each weekend. As a part of normal backup procedures, archive tapes are created on a monthly basis and stored off-site. Network uptime is ensured with uninterrupted power supply systems on all servers and switches to deal with any possible power fluctuations and enables maintenance of schedules with little or no threat of service interruptions.

Limiting Network Access and Tracking Users

The physical components of Questar's network (e.g., servers, switches, and firewall) are located in secure data centers. Data center access is limited to a minimum number of people, and a card system is installed on the data center doors to track user access. Data centers are secured with motion-activated camera's as well.

Questar's network security is based on a strong password policy, frequent changes to passwords, and the principle of least privilege, meaning that users are given the network access required to efficiently perform their job functions and no more. This principle is carried out through network security that restricts access to network directories containing answer keys, score conversion tables, and other sensitive data to only those employees who will be analyzing and scoring the student response data.

Except for the program managers and key development staff, no other employees within Questar have access to the directories in which these sensitive files reside.

External Network Security Blocks Unauthorized Access

A firewall blocks all unauthorized access into and out of our internal network. One way the firewalls protect Questar and client data is by implementing Network Address Translation (NAT). A global policy, NAT rewrites and redirects packets sent to one range of IP addresses to a different range of IP addresses. The originating traffic and the reply traffic are both translated, thus keeping our internal IP address private.

We allow authorized HTTP web traffic out of our building using web content filters. The filters block access to unauthorized external websites. Additionally, the web content filters log user traffic for forensic purposes.

Security in Handling Materials and Data for Program Set-up and Processing

Only individuals with direct responsibility for program setup have access to secure materials. During every phase of processing and data handling, we follow established security procedures to ensure the security of test items and all test materials being used by staff.

Security Audits

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.

Secure FTP for Encrypted Data Transfer

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 project-related documents and serve as a secure forum for interaction and exchange of materials.

Access to information on this site will be limited to authorized Questar and NYSED staff, unless further sharing with other parties (such as AMI) is authorized in writing by NYSED. We will work closely with NYSED to establish a file folder structure applicable for the project to ensure that the secure FTP site will be used to transmit all appropriate data.

We further commit that this secure tool will be Questar's only means for electronic transmission of secure test materials unless authorized by NYSED, on a case-by-case basis, to use some other means. (Electronic transfer includes transfer via email, Internet, or fax.)

Once NYSED downloads secure data files from the secure FTP server, all confidential information will automatically be deleted by the FTP site according to a set interval. NYSED will provide Questar a list of individuals needing access, including any specific security requirements, and Questar will provide unique user names and passwords based on this list.