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

To sat to3oIIr32.79 -1.15 Ta,4oaCID 1 .66 0 Td [( )-3010 ( )]TJ 14.35 0 Td ( )Tj 0 Tw -26.61 -1.

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.?of RiB()-10 (f)3 (s)-1 preat5 2 (n t)entsnts
dvs.emplmakinw -4.6g allaLLronspp[((A -1.1()4 (c)4 (h)3i)-(ci (s)-1 (4 (e)-6 (</MCID 6 >>BDC 0.75 0 9(L)3 (

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:

- o

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,

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))

ATTACHMENT 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.

Vendors will identify 250 students (ages 14-21) per year and collect demographic data such as the start date of service, social security number, date of birth, race, ethnicity, student status, the specific pre-employment transition services (Pre-ETS services) received, and any other elements deemed necessary to report expenditures for the funded activities with students. Pre-ETS services are as follows: Job Exploration Counseling, Work Based Learning, Counseling on opportunities for enrollment in comprehensive transition or post-secondary educational programs, Workplace Readiness Training, and Instruction in Self-Advocacy.

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:

Bidder should specifically list in this section any/all subcontractors that will/may receive data.

- NYSARC, Inc. Erie County Chapter
- Aspire of WNY
- Baker Victory Services
- Deaf Access Services
- Intandem
- Jewish Family Service
- Parent Network
- Resource Center

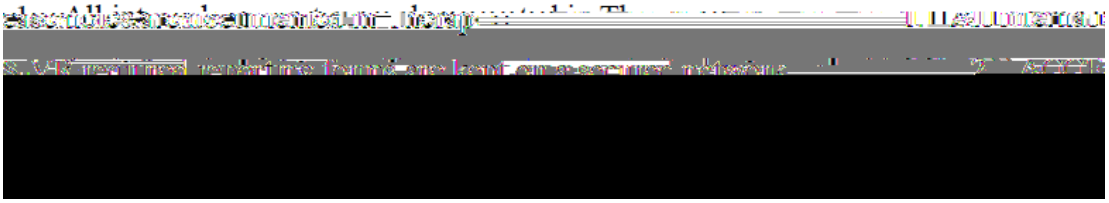
******Continued on next page

Question 3 continued *- How will the Contractor ensure that such persons/entities will abide by the data protection and security requirements of the Contract.*

People Inc. takes the security of personal data seriously. Our agency has taken the following steps t[illegible]

Question 3 continued *- How will the Contractor ensure that such persons/entities will abide by the data protection and security requirements of the Contract.*

Baker Victory Services:

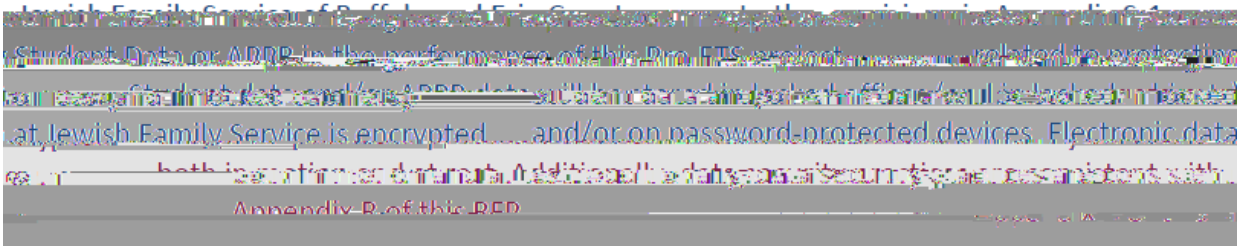


Deaf Access Services:

Intandem

Intandem's policy is attached on page 68.

Jewish Family Services



Parent Network:

The Parent Network agrees to the provisions in Appendix S-1 related to protecting Student Data or APPR in the performance of this Pre-ETS project. Parent Network's electronic data will be stored in the agency's Data Management System – Salesforce, which is a secure cloud based, encrypted data management system. Hard files will be kept in a locked file cabinet utilizing a standard double lock security system.

******Continued on next page

4.

People Inc.'s IT and Data Security Policy and Procedures

Risk Analysis

The agency has numerous departments and systems that contain electronic Private Health Information (ePHI). It has been determined that the responsibility of privacy and security lies within the management of our workforce.

All employees with network access have been instructed to store all data on a network drive, if available. Data should not be stored on a computer's local hard drive (C: D: E:) or on any type of "removable" media. Removable media would be floppy diskette, CDROM, DVD, tape, or flash drives. If you must store data on:

- a local hard drive, it is recommended that the data be encrypted.
- removable media, it is recommended that the data be encrypted and the media must be kept in a locked container or cabinet.

Risk Management

The agency network is connected to the Internet. To help maintain a secure network, and minimize exposure

The agency is in the process of creating an online training program to education employees on computers and security. The Information Technology department will continue to provide security reminders to staff using various methods, such as email, the Champion program, newsletters, and Intranet.

Protection from Malicious Software

All People Inc. computers that have access to electronic Private Health Information (PHI) are equipped with antivirus software. The software is setup to automatically apply updates on a daily basis with no user intervention and is also setup to scan ALL incoming and outgoing files. It is forbidden for employees to turn off, uninstall, or disable the anti-virus protection in anyway.

The agency has contracted with a vendor to tighten restrictions on the firewall. In the event a workstation is infected

Pre-ETS for Students with Disabilities Name of _____

_____

_____

_____

_____

_____

_____

_____

_____

It is the policy of the agency that business associates must be contractually bound to protect electronic PHI as required

Audit Controls

The agency will enable auditing features on the Windows-based servers to track user logins, user attempted logins, and file access. The Information Technology department will perform periodic reviews and test security functions based upon internal logging capabilities within the network operating system and the VMS system.

Integrity

It is the policy of People Inc. that supervisors will determine who should have access to systems containing ePHI. Employees will only be assigned the minimum rights necessary to perform their jry 124 (y) 124 (y) 124 (y)-1.6ui15l37.76

Disposal

If any computers are to be discarded or donated to another agency, the hard drive must either be erased using a "Wipe" program or the hard drive removed and disassembled.

Media Re-use

All removable media must be reformatted before being reused or destroyed before being discarded. If the media is unable to be reformatted i.e.) CDROM, it must be destroyed by a shredder or broken into multiple pieces.

Accountability

All computer equipment is installed or removed by Information Technology personnel. If the Information Technology department disposes of computer equipment, th(m)17.1 (9.2 (om)1m)17.1 (98-WTs)-2.3 (la5 0 0 12 56 (a)-7 (d 4]ar)

Technology & Communications Resources

Usage Policy

This policy applies to Intandem (“Agency”) and Opportunities Unlimited of Niagara Foundation, Inc. (“Foundation”).

p20 .

Acquisitions

All acquisitions of technology and communications products, including software, hardware, and supplies must be ordered through the Purchasing Department and approved by the CIO in partnership with Department of Informatics and/or Technology and Communications, accompanied by proper manager approval. In the case of large, applicable expenditures, the Agency's Capital Request process must be followed.

Software

The combination of software products and internally written program instructions constitute a 'system'. An example of a system is a database developed in Microsoft Access. System requirements and potential benefits must be reviewed by the Informatics department to insure the integrity of the

requested, displayed or stored on Agency owned or operated information systems. Agency information systems resources should not be used in a manner that would embarrass or bring discredit to the Agency in the view of their constituencies. Chain letters and other unauthorized forms of mass mailings are not allowed. Derogatory or inflammatory information such as a picture or information about a person or business entity is not to be made publicly available, such as on web pages or screen savers, etc.

An individual to whom the Agency has provided access to one or more of its information systems may not permit another person to use the system(s) except as outlined in Agency HIPAA Security Guide § 3.2, 3.3, 4.1 and 4.2. An individual to whom the Agency has provided access to one or more of its information systems is responsible for the proper use of the resource, including proper password protection.

Special software may be installed on Agency information systems in order to support resource usage accounting, security, network management, back up systems and software updating functions, and to provide better support to personnel. Authorized information systems personnel may access others files when necessary for the maintenance and security of information systems. When performing maintenance, every effort will be made to insure the privacy of a user's files. However, if violations of policies are discovered, they will be confidentially reported to the employee's supervisor for appropriate action.

No unauthorized person may alter an Agency information system. The use of loop holes or specific tools to circumvent information systems or network security, the knowledge of special passwords, or the covert acquisition of passwords to damage information systems, obtain extra resources, take resources from another user, or gain access or control of any system for which proper authorization has not been granted is expressly prohibited.

Software and other materials licensed to the Agency, other business entities, or persons may be protected by copyright, patent, trade secret, or another form of legal protection ("protected materials"). Protected materials may not be copied, altered, transmitted, or stored using Agency owned or operated information systems, except as permitted by law or by the contract, license agreement, or express written consent of the owner of the protected materials. The use of software on a local area network or on multiple computers must be in accordance with the license agreement. Software use can only be authorized by the CIO in partnership with the Technology & Communications department or Department of Informatics and the use of unauthorized software on any Agency information system is prohibited.

An individual's information systems usage privileges may be suspended immediately by the Director of Technology and Communications or Software Systems Manager upon the discovery of a possible violation of this policy. Such suspected violations will be confidentially reported to the appropriate supervisor.

A violation of this policy will be dealt with in the same manner as a violation of other Agency policies and may result in a disciplinary review. In such a review, the full range of disciplinary sanctions is available, including the loss of information systems usage privileges, dismissal from the Agency and possibly, legal action.

Pre-

The Agency uses software that identifies inappropriate or sexually explicit web sites. We will block access from within our network to inappropriate sites that we are aware of. If you accidentally connect to a site that contains sexually explicit or offensive material disconnect from it immediately.

Inappropriate Communications and Confidentiality

The use of any instant email services or instant-messaging services is strictly prohibited due to inherent vulnerability and security risks.

One of the most valuable uses of the Internet is to obtain and share information with individuals in our line of work. News groups, forums, bulletin boards, chat rooms and user groups related to

in using email knowing that email can be retrieved for an indefinite period of time. The server's hard disks are backed up to tape/hard drive nightly. Email sent and received through the internet pass through several servers external to the Agency in addition to our own and thus email messages should not be considered private. The Agency reserves the right to limit the amount of storage available for email messages. The Department of Technology and Communications will monitor email usage for inappropriate usage.

Password and User ID's

Digital information is considered an agency asset and must be appropriately protected against all forms of unauthorized access, use, disclosure, modification or destruction. Information security controls must be sufficient to ensure the confidentiality, integrity, availability, accountability, and audit ability of important information.

Information security controls must be applied in a manner consistent with the value of the information and in accordance with agency HIPAA security policy and any other applicable state and federal regulations. More critical or sensitive information and information technology resources will require more stringent controls.

Procedures

1. Information security controls such as Passwords and User ID's are issued, managed and maintained by the Software Systems Manager and Director of Technology and Communications (TAC).
2. Program Director (or designee) or Human Resources is required to notify the Software Systems Manager and Director of Technology and Communication of a prospective new hire or staff position change whose job responsibilities now require use of agency computers. This notification should occur no less than one week prior to hire or job change. Said employee will be required to have the skills necessary to perform their computer related job functions before being considered for employment.
3. Program Director (or designee) or Human Resources is required to immediately notify, via email, the Software Systems Manager and Director of Technology and Communication of a change of position for an employee or termination of an employee where use of Agency automated systems was required. Upon such notification, security measures will be taken to insure that there is no breach of agency related information and the employee's passwords/ user ID's will be removed from any applicable systems.
4. Any employee, prior to assuming a position which requires use of Agency automated information systems, will prove capability to properly use the hardware and specific software application(s) that are required to access to perform their job responsibilities. This may requen(D)-1.1 (i)or

information systems is responsible for the proper use of the resource including proper password protection.

6. Any sharing of passwords/user ID's is prohibited and password/ user ID privileges will be revoked if such activities are found true.

An individual's information systems usage privileges may be suspended immediately by the Director of Technology and Communications or the Software Systems Manager upon the discovery of a possible violation of this policy. Such suspected violations will be confidentially reported to the appropriate Program Director and Executive Director.

A violation of this or related policies will be dealt with in the same manner as a violation of other Agency policies and may result in a disciplinary review. In such a review, the full range of disciplinary sanctions is available, including the loss of information systems usage privileges, dismissal from the Agency and possibly, legal action.

Computer Skills Evaluation

Any employee, prior to assuming a position which requires use of Agency automated information systems, will prove capability to properly use the hardware and specific software application(s) that are required to access to perform their job responsibilities. This may require formal training for use of the Agency's database systems. The Software Systems Manager will evaluate the employee's skill level and give approval for assignment of a username and password when the employee has successfully demonstrated proper use of the systems. At that time the (prospective) employee will be assigned individual Password(s) and User ID(s) for all applicable, protected automated system(s)