Data Security and Privacy Plan

As per Section 3 of the Supplemental Agreement, this plan must be completed by the Contractor within 10 days of the signing of said Addendum.

1. Exclusive Purposes for Data Use
    a. The exclusive purposes for which the Student Data and/or Principal or Teacher Data will be used by the Contractor are as follows

treatment, payment or healthcare operations of Ivy.

Initial _____

2. Data Accuracy/Correction Practices
    a. Parent, student, eligible student, teacher or principal may challenge the accuracy of the data by

submitting a written request to the clinic for review in accordance with Ivy's Amendment of PHI Policy.

Initial _____

3. Security Practices
    a. The security protection taken to ensure data will be protected include [*Insert (i) a description of where Student Data and/or Principal or Teacher Data will be stored, described in a manner to protect data security, (ii) a description of the security protections taken to ensure Student Data and/or Principal or Teacher Data will be protected and data security and privacy risks are mitigated; and (iii) a description of how the Student Data and/or Principal or Teacher Data will be protected using encryption while in motion and at rest.*

The following represents a high-level outline of data security and privacy practices as well as administrative, operational, and technical safeguards: -Data Security: Employee phishing testing and training, End-point protection solutions, Patch Management, Antivirus solution, Standardized Microsoft O365 email encryption, Access privileges, standard and advanced firewalls, Multi-Factor Authentication, Blocking of O365 login from multiple foreign countries, Standardized all company devices on Sophos Intercept X end-point protection, Periodic security updates, and more.

-Privacy: Ivy maintains and enforces over 25 HIPAA Privacy and Security Policies and Procedures as well as Incident Reporting Policy, Compliance Reporting, Compliance Hotline, Record Retention, etc. Ivy has a Privacy Officer.

-Electronic Medical Record (EMR)-specific: See Data Security and Privacy. EMR Password Protection and Multi-Factor Authentication.

See last page for more.

Initial _____

4. Contract Lifecycle Practices
   a. The agreement expires 6/30/2021
   b. When the agreement expires, the Student Data and/or Principal or Teacher Data will be

Data is maintained in an electronic medical record. In the event that Ivy determines that returning or destroying data is infeasible, Ivy shall extend the protections of data and limit further uses and disclosure of such data to those purposes that make the return or destruction infeasible, for so long as Ivy maintains data.

Initial

5. The Contractor will ensure that any and all subcontractors, persons or entities that the Contractor may share the Student Data and/or Principal or Teacher Data with will abide by the terms of the Agreement, the Supplemental Agreement, and the data protection and security requirements set forth in this Data Security and Privacy Plan, in accordance Education Law §2-d and Part 121 of the Regulations.

Yes

Initial

Ivy Rehab Physical Therapy PLLC

Company Name

Joseph Sullivan Regional Director

Print Name and Title

Signature of Provider

11/18/20

Date

Return to:
Amanda Kavanagh
Director of Instructional and Administrative Technology
Hewlett-Woodmere Public Schools
1 Johnson Place
Woodmere, NY 11598
akavanagh@hewlett-woodmere.net

Ivy Rehab enforces HIPAA compliant best practices and procedures to protect the personal information of students at all levels of the organization. This includes strong access control measures and computer system safeguards.

The Ivy Rehab systems that process student information are designed, built and maintained to effectively process PII/PHI. Student personal information is encrypted both at rest and in motion. This includes data protection backup of the data.

Any student information that is emailed is inspected and encrypted automatically based on system detected criteria. In addition to the automatic inspection, all Ivy Rehab teammates are trained to manually force encryption on emails containing sensitive information. Teammates are also regularly trained with monthly Information Security training videos and simulated phishing examples.

Secure user authentication protocols

- Unique strong passwords are required for all user accounts; each employee receives an individual user account.
- Passwords are required to be changed regularly.
- Server accounts are locked after 3 successive failed password attempts.
- Computer access passwords are promptly disabled upon termination of employment.
- User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.

Secure access control measures

- Access to specific files or databases containing Personal Information is limited to those employees who require such access in the normal course of their duties.

Files containing Personal Information transmitted outside of the Ivy Rehab network are encrypted.

The Information Security Officer performs regular internal network security checks to all server and computer systems to discover, to the extent reasonably feasible, possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Personal Information.

All Company-owned computers and servers are protected and regularly monitored.

Critical operating system patches and security updates are installed to all servers at least every 30 days.

Antivirus and anti-malware software is installed and kept updated on all servers and workstations. Virus definition updates are installed on a regular basis, and the entire system is tested and checked at least once per month.