Multi-State Billing Services, LLC
(DBA Educational Data Management Solutions LLC.)

Protected Information Security Policy

Table of Contents

.

1. Introduction

1.1 *Purpose*: This Policy governs the creation, receipt, acquisition, storage, maintenance, access, use, disclosure, transmission, transportation, destruction, and other matters concerning Protected Information. This Policy is intended to comply with Applicable Law, but does not simply restate that law. Thus, while this Policy guides the Company's conduct, the Security Officer may authorize deviations from this Policy to the extent necessary or appropriate and permitted by Applicable Law.

1.2 *Scope*: This Policy applies to all Protected Information that belongs to the Company, that is within the Company's possession, custody or control, or that is created, received, acquired, stored, maintained, accessed, used, disclosed, transmitted, transported, or destroyed by the Company, or an Employee or Business Associate acting on behalf of the Company. This Policy applies to the Company, all Employees and Business Associates of the Company, and all other Persons who have access to Protected Information of the Company.

2. Responsibilities of Employees and Business Associates

2.1 *General*: Employees and Business Associates may create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, dispose of, and destroy Protected Information only if and to the extent the Employee or Business Associate is expressly required or authorized to do so by the Security Officer or Applicable Law. If authorized to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, dispose of, or destroy Protected Information, Authorized Employees and Business Associates shall do so only in accordance with this Policy, directives of the Security Officer, or Applicable Law.

2.2 *Training and Awareness*: Employees and Business Associates shall cooperate with and participate in all necessary or appropriate training provided by the Company to safeguard the confidentiality, integrity and availability of Protected Information. Authorized Employees and Business Associates shall acquire and maintain an awareness about Protected Information, the types of Protected Information at the Company, the types of Protected Information they are authorized to access, and their authority and responsibility with respect to Protected Information under this Policy and Applicable law.

2.3 *Creation, Receipt, Access, Acquisition, Use, Storage and Maintenance of Protected Information*: Authorized Employees and Business Associates may create, access, acquire, use, store and maintain Protected Information only if and to the extent they are authorized to do so and doing so is necessary or appropriate to perform their duties for the Company. Authorized Employees and Business Associates shall create, access, acquire, use, store and maintain only the minimum amount of Protected Information necessary or appropriate to perform their duties for the Company. Authorized Employees and Business Associates shall not permit any Person to create, access, acquire, use, store or maintain Protected Information if that Person is not authorized to do so.

2.4 *Disclosure of Protected Information*: Authorized Employees and Business Associates may disclose Protected Information to, and make it accessible to, only the following Persons under the following circumstances: (a) other Authorized Employees and Business Associates if the Protected Information is necessary or appropriate for them to perform their duties for the Company; (b) if authorized by the Security Officer, the individual about whom the Protected Information pertains, but only Protected Information about that individual; (c) the

Person for whom the Company is providing services related to individuals about whom the Protected Information pertains, but only Protected Information about those individuals. The Security Officer may disclose and make accessible Protected Information to other Persons as permitted by Applicable Law, and as otherwise may be necessary or appropriate to fulfill the Security Officer's authority and responsibility under this Policy and Applicable Law.

2.5 *Use of Information Systems*: Authorized Employees may create, receive, acquire, store, maintain, access, use, disclose, transmit, and transport Protected Electronic Information only on Information Systems and Electronic Devices owned by the Company, and Business Associates shall do so only on the Information Systems and Electronic Devices owned by the Business Associate.

2.6 *Transmission of Protected Electronic Information*: Authorized Employees and Business Associates may transmit Protected Electronic Information by email, file transfer protocol or FTP, or other means of digital, analog, or electronic transmission only if (a) the transmission is necessary or appropriate to perform the Authorized Employee's or Business Associate's duties for the Company, (b) the entire transmission, or the Protected Electronic Information transmitted, is Encrypted in accordance with paragraph 4.13, and (c) the Person to whom the Authorized Employee or Business Associate transmits the Protected Electronic Information is authorized to receive it under paragraph 2.4.

2.7 *Transportation of Protected Electronic Information*: Authorized Employees and Business Associates may transport Protected Electronic Information only if (a) the Electronic Device used to do so, or the Protected Electronic Information on it, is Encrypted in accordance with paragraph 4.14, and (b) if transported by the Authorized Employee, the Electronic Device belongs to the Company or, if transported by the Business Associate, the Electronic Device belongs to the Business Associate.

2.8 *Laptops and External Drives*: Authorized Employees and Business Associates may create, receive, acquire, store, maintain, access, use, disclose, transmit, and transport Protected Electronic Information on a Laptop or External Drive only if (a) it is necessary or appropriate to have the Protected Electronic Information on the Laptop or External Drive to perform their duties for the Company, and (b) the entire Laptop or External Drive, or the Protected Electronic Information on it, is Encrypted in accordance with paragraph 4.14.

2.9 *Tablets and Smartphones*: Authorized Employees and that Business Associates may create, receive, acquire, store, maintain, access, use, disclose, transmit, and transport Protected Electronic Information on a Tablet or Smartphone only if (a) it is necessary or appropriate to have the Protected Electronic Information on the Tablet or Smartphone to perform their duties for the Company, and (b) the entire Tablet or Smartphone, or the Protected Electronic Information on it, is Encrypted in accordance with paragraph 4.14.

2.10 *Remote Access*: Authorized Employees and Business Associates may create, receive, acquire, access, and use Protected Electronic Information with an Electronic Device that is outside of the Company's firewall only if (a) the access occurs through the dual authentication virtual private network implemented by the Company, and (b) the transmission of the Protected Electronic Information is Encrypted in accordance with paragraph 4.13.

2.11 *Usernames, Passwords and Security Codes*: Employees and Business Associates shall not use the username, password, or security code of any other Person to activate or

deactivate the Company's security system or access the Company's facility, Information Systems or Electronic Devices, or to create, access, acquire, use, disclose, store or maintain Protected Information. Employees and Business Associates shall not permit any other Person to use their username, password, or security code to activate or deactivate the Company's security system or access the Company's facility, Information Systems or Electronic Devices.

2.12 *Printing and Storage of Protected Documentary Information*: Authorized Employees and Business Associates may print Protected Information or otherwise generate Protected Documentary Information only if and to the minimum extent doing so is necessary to perform their duties for the Company. Whenever Protected Documentary Information is not directly being used, Authorized Employees shall store it in a secure facility and locked equipment provided or designated by the Company, and a Business Associates shall do so only in such a facility and equipment provided or designated by the Company or the Business Associate.

2.13 *Transportation of Protected Documentary Information*: Authorized Employees and Business Associates may transport Protected Documentary Information only if (a) doing so is necessary or appropriate to perform their duties for the Company, and (b) if transported by an Authorized Employee, the Protected Documentary Information is transported in a locked container provided or designated by the Company appropriate to the nature of scope of the Protected Documentary Information being transported, and, if transported by a Business Associate, the Business Associates does so in a such locked container provided or designated by the Company or the Business Associate.

2.14 *Destruction and Disposal*: Authorized Employees and Business Associates shall dispose of Protected Documentary Information only in accordance with the Company's practices, procedures, policies, programs, systems and other measures for doing so under paragraph 5.5. Authorized Employees and Business Associates shall dispose of and destroy Protected Electronic Information and Information Systems that contain Protected Electronic Information only in accordance with the Company's practices, procedures, policies, programs, systems and other measures for doing so under paragraph 4.15.

2.15 *Breaches*: Employees and Business Associates shall not engage in any conduct that the Employee or Business Associate knows will or may result in an actual or threatened Breach of Protected Information. Employees and Business Associates shall inform the Security Officer (or, in the absence of the Security Officer, the IT Officer) if they have any reason to believe that an actual or threatened Breach of Protected Information has occurred, will occur, or may occur. Employees and Business Associates shall cooperate with and participate in investigations, remediations, processes and other measures to address an actual or threatened Breach of Protected Information.

2.16 *Questions and Concerns*: Employees and Business Associates shall inform the Security Officer or IT Officer of any question or concern they may about the confidentiality, integrity or availability of Protected Information.

2.17 *Cooperation and Participation in Security*: Employees and Business Associates shall cooperate and participate in all practices, procedures, policies, programs, systems and other measures under this Policy and otherwise implemented by the Company to safeguard the confidentiality, integrity and availability of Protected Information.

2.18 *Discipline and Consequences*: Employees shall be subject to discipline, up to and including termination of employment, and Business Associates shall be subject to adverse consequences, up to and including termination of their contract with the Company, for failing or refusing to comply with this Policy, Applicable Law, or any request or instruction from the Company, the Security Officer or the IT Officer.

3. Administrative Safeguards

3.1 *Security Officer*: The Security Officer has authority and responsibility to interpret, implement, enforce, modify and amend this Policy, to develop, implement and enforce existing, new, additional and supplemental information security practices, procedures and policies, and to generally ensure the Company's compliance with Applicable Law. The Security Officer has the discretion to assign portions of such authority and responsibility to other Employees, and to obtain the assistance of other Employees and outside professional services providers to fulfill such authority and responsibility, provided that the Security Officer shall retain ultimate authority and responsibility for those matters. To the extent any authority or responsibility is assigned directly to the IT Officer, the IT Officer shall have initial authority and responsibility for those matters, but the Security Officer shall retain ultimate authority and responsibility for those and all other matters under this Policy and Applicable Law.

3.2 *Authorized Employees and Business Associates*: The Security Officer shall determine which Employees and Business Associates are authorized to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, dispose of, and destroy Protected Information, and the scope of their respective authority and responsibility for such matters. The Security Officer shall prepare, maintain, periodically review, and make necessary or appropriate modifications to a list of such Authorized Employees and Business Associates.

3.3 *Risk Assessments and Policy Review*: The Security Officer annually initiates and directs an assessment of the Company's administrative, technical and physical safeguards to determine, under Applicable Law, what Protected Information the Company has, whether to modify or expand the scope of Protected Information, whether the Company is subject to any new, additional or reoccurring risks to the confidentiality, integrity or availability of Protected Information, whether the Company must or should implement or consider implementing any new or additional measures to mitigate such risks, and, if so, the measures that the Company must or should implement or consider implementing. Based on that risk assessment, the Security Officer shall take steps to implement the measures that the Company determines it must or should implement to mitigate such risks, and shall modify and amend this Policy if necessary or appropriate to do so. The Security Officer maintains records memorializing the risk assessments performed by the Company, and any other matters related to this Policy.

3.4 *Employee Training*: Upon the adoption of this Policy and no less than once every two years thereafter, the Company's attorneys shall train the Security Officer and the IT Officer concerning the Company's, the Security Officer's and the IT Officer's authority and responsibility under this Policy and Applicable Law. Upon the adoption of this Policy and no less than once every two years thereafter, the Security Officer shall train all Employees concerning their authority and responsibility under this Policy and Applicable Law. Within the first two weeks of employment of a new Employee and before any existing Employee becomes an Authorized Employee, the Security Officer shall train the Person concerning his/her authority

and responsibility under this Policy and Applicable Law. The Security Officer shall maintain records of all such trainings.

3.5 *Business Associates*: Before the Company retains any Person to be a Business Associate, the Security Officer determines whether and the extent to which the Company must or should conduct due diligence with respect to such Person given the nature and scope of the Person's anticipated access to Protected Information, and directs such due diligence. Before providing Protected Information to any Business Associate, the Security Officer ensures that the Company enters into an appropriate written agreement with the Business Associate requiring the Business Associate to comply with its responsibility under this Policy and Applicable Law.

3.6 *Availability of Protected Information to Individuals*: The Security Officer will address any request by an individual for access to, production of, or modification of Protected Information concerning that individual.

3.7 *Breach Response*: In the event of an actual or threatened Breach, the Security Officer (or, in the absences of the Security Officer, the IT Officer) initiates and directs a process to (a) determine if a Breach occurred and, if so, the nature and extent of Protected Information affected, (b) identify the individuals affected by the Breach and Persons that the Company must or should notify about the Breach, (c) determine if the Company must or should implement measures to mitigate any risk to the confidentiality, integrity or availability of Protected Information related to the Breach or any other risk discovered during the process and, if so, implement such measures, (d) determine if the Company must or should take any disciplinary or other action against an Employee or Business Associate arising out of or related to the Breach and, if so, take such action, (e) determine if the Company must or should modify this Policy or provide additional training about the confidentiality, integrity or availability of Protected Information and, if so, modify this Policy and provide such training, (f) determine if the Company must or should take any other action arising out of or related to the Breach and, if so, take such action, and (g) prepare and retain records memorializing the process and outcome.

3.8 *Record Retention*: The Security Officer ensures that the Company retains all records, logs and other documents that are required, necessary or appropriate to be retained under this Policy or Applicable Law for at least six years after creation of the record.

4. Technical Safeguards

4.1 *IT Officer*: The IT Officer has authority and responsibility to interpret, implement, and enforce the provisions of this Policy related to technical safeguards, to develop, implement and enforce existing, new, additional and supplemental security practices, procedures and policies related to technical safeguards, and to generally ensure the Company's compliance with Applicable Law with respect to technical safeguards.

4.2 *Access Limitations*: The Company limits access to Protected Electronic Information to only those Authorized Employees and Business Associates who need access to such information to perform their duties for the Company.

4.3 *Electronic Devices*: The Company provides Authorized Employees with the Electronic Devices necessary or appropriate to create, receive, acquire, store, maintain, access, use, disclose, transmit, and transport Protected Electronic Information, and requires Authorized Employees to do so only on the Company's Information Systems and Electronic Devices. The Company provides Laptops, External Drives, Tablets and Smartphones to Authorized Employees

who need to have Protected Electronic Information on such External Drives to perform their duties for the Company. The Company requires Employees to use usernames and passwords to access all of the Company's Information Systems and Electronic Devices pursuant to paragraph 4.5.

4.4 *Tablets and Smartphones*: The IT Officer shall implement technology that maintains Protected Electronic Information on Company Tablets and Smartphones in an Encrypted format.

4.5 *Usernames and Passwords*: Employees and Business Associates have unique usernames and passwords. Passwords used to access the Company's Information Systems, Laptop and External Drives have at least eight characters, including capitalized letters and either numbers or symbols. Passwords used to access the Company's Tablets and Smartphones have at least six characters. The IT Officer shall take steps to investigate and, if technologically, financially and operationally feasible, implement technology that requires Employees to change such passwords at least once every six months. The Company's Information Systems have software that requires the use of a password to access the Electronic Device being used to access the system if the device has not been used for 30 minutes or longer. Promptly after an Employee ceases to be employed by the Company or the Company's contract with a Business Associate ends, the Company revokes the username and password assigned to the Employee or Business Associate. The Company also revokes the username and password assigned to any existing or former Employee or Business Associates as soon as the Company becomes aware that the Employee or Business Associate presents a threat to the confidentiality, integrity or availability of Protected Electronic Information.

4.6 *Remote Access*: The Company has implemented and maintains a virtual private network with dual authentication that permits Authorized Employees and Business Associates to create, receive, acquire, access, and use Protected Electronic Information using an Electronic Device that is outside of the Company's firewall.

4.7 *Issuance and Inventory*: The IT Officer shall take steps to ensure that the Company creates and maintains an inventory of Electronic Devices issued to Employees and the usernames and passwords of Employees and Business Associates. The IT Officer shall take steps to ensure that, before issuing any Electronic Device to an Employee, all Protected Electronic Information is removed from the Electronic Device in accordance with National Institute of Standards and Technology Special Publication 800-88, if the removal of Protected Electronic Information is necessary or appropriate.

4.8 *Information Systems*: All servers, routers and other network infrastructure that support the Company's Information Systems and contain Electronic Personal Information are maintained either (a) in the Company's secure facility in Somersworth, New Hampshire, or (b) offsite with three Business Associates of the Company. The Security Officer and IT Officer shall take steps to ensure that the Company conducts appropriate due diligence and obtains an appropriate contract with such Business Associates in accordance with paragraph 3.5.

4.9 *Software Updates*: To the extent available and technologically, financially and operationally feasible, the Company uses the automatic updating functionality of commercially available software on the Company's Information Systems. If automatic updating functionality is not available, feasible, or used, the IT Officer ensures that, no less than once every three months, the Company manually updates commercially available software on its Information

Systems. At least annually and whenever the IT Officer is aware of a security threat, to the extent technologically, financially and operationally feasible, the IT Officer ensures that software proprietary to the Company, including Seaquell, is updated to address any known threats.

4.10 *Protective Software*: The Company has implemented and maintains up-to-date, commercially reasonable and available software and systems to protect the confidentiality, integrity and availability of Protected Electronic Information, including firewall, anti-virus, anti-malware, and anti-spyware software. The IT Officer shall investigate and, if technologically, financially and operationally feasible, implement commercially reasonable and available software and systems that detects multiple failed attempts to log-on to the Company's Information Systems and disables the account being used to attempt to log-on. To the extent available and technologically, financially and operationally feasible, the Company shall use the automatic notification functionality of such software and systems. If automatic notification functionality is not available, feasible or used, the IT Officer shall ensure that the Company monitors the security logs for such software and systems at intervals appropriate to the nature of the security risk, but in no event less than once every three months. The IT Officer shall take steps to have the Company develop, test and implement software that detects and alerts the Company in the event of multiple failed attempts to log-on to the Company's proprietary software program, Seaquell, and disables the account being used to attempt to log-on.

4.11 *Audit Logs*: The Company has implemented and maintains up-to-date, commercially reasonable and available software and systems that log the creation, receipt, access, use, modification, disclosure, transmission, and destruction of Protected Electronic Information. The IT Officer shall take steps to have the Company develop, test and implement software that does so for Company's proprietary software program, Seaquell. The IT Officer shall investigate and, if technologically, financially and operationally feasible, implement commercially reasonable and available software and systems that enable the Company to effectively and efficiently review user creation, receipt, access, use, modification, disclosure, transmission, and destruction of Protected Electronic Information on a periodic basis.

4.12 *Administrators and Software Installation*: Employees generally are not administrators of any of the Company's Information Systems and Electronic Devices. Only the Security Officer, IT Officer, and employees designated by one of them may be an administrator. Administrator usernames and passwords are provided to the Security Officer and IT Officer and, if stored electronically, are stored in an encrypted format. Employees, including administrators, are not authorized to download executable software to the Company's Information Systems and Electronic Devices without prior express approval of either the Security Officer or IT Officer.

4.13 *Transmission of Protected Electronic Information*: The Company has implemented and maintains technology that enables the transmission of Protected Electronic Information, including by email and by file transfer protocol or FTP, pursuant to National Institute of Standards and Technology Special Publication 800-52.

4.14 *Transportation of Protected Electronic Information*: The Company has implemented and maintains technology that enables the transportation of Protected Electronic Information on Laptops and External Drives pursuant to National Institute of Standards and Technology Special Publication 800-52. The IT Officer shall investigate and, if technologically, financially and operationally feasible, implement technology that enables transportation of

Protected Electronic Information on Tablets and Smartphones pursuant to National Institute of Standards and Technology Special Publication 800-52.

4.15 *Destruction of Protected Electronic Information*: The IT Officer shall ensure that, if the Company destroys Protected Electronic Information or Information Systems containing Protected Electronic Information, it does so pursuant to National Institute of Standards and Technology Special Publication 800-88. The IT Officer shall ensure that, if the Company retains a third party provider to destroy Protected Electronic Information or Information Systems containing Protected Electronic Information, it contractually requires the provider to do so in compliance with National Institute of Standards and Technology Special Publication 800-88.

4.16 *Disaster and Emergency*: The IT Officer shall investigate, implement, test, document, and maintain reasonable, commercially available software and systems that enable the Company to (a) create and maintain back-ups of exact copies of Protected Electronic Information, (b) restore and use Protected Electronic Information within a reasonable amount of time after a natural or other disaster affecting the Company's Information Systems, and (c) continue critical business operations involving Protected Electronic Information during and after an emergency or mass failure of the Company's Information Systems.

5. Physical Safeguards

5.1 *Facility Security*: The Company's only physical facility is in Somersworth, New Hampshire. The facility is protected by both a keyed and a keyless entry system both of which must be activated to access the facility to perform their duties for the Company. Promptly after an Employee ceases to be employed by the Company and a Business Associate ceases to have a business relationship with the Company, the Company revokes access previously assigned to the Employee and Business Associate. The Company also revokes access as soon as the Company becomes aware that the Employee or Business Associate presents a threat to the confidentiality, integrity or availability of Protected Information.

5.2 *Onsite Storage*: At its facility in Somersworth, New Hampshire, the Company generally maintains Protected Documentary Information in locked filing cabinets and in locable offices.

5.3 *Offsite Storage*: The company currently uses secure Iron Mountain for offsite storage of Protected Information and insures all Protected Information id stored at this secure facility.

5.4 *Transportation of Protected Documentary Information*: The Company transports Protected Documentary Information only in a secure container or other method of transportation appropriate to the nature and scope of the Protected Documentary Information being transported.

5.5 *Disposal and Destruction of Protected Documentary Information*: The Company provides Employees with receptacles for the disposal of Protected Documentary Information. The Company has retained a third party provider to destroy Protected Documentary Information, and contractually requires the provider to destroy that it in a manner that renders it essentially unreadable and indecipherable, such as by shredding, burning, pulping or pulverizing.

6. Definitions: The following definitions apply to this Policy. To the extent a term used in this Policy is not specifically defined here, the definitions in the Code of Federal Regulations, Section 45, Part 164, Section 304 may be used to interpret this Policy.

6.1 *Applicable Law*: "Applicable Law" means HIPAA and State Law.

6.2 *Authorized Employee*: "Authorized Employee" means an Employees who is authorized by the Security Officer or Applicable Law to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, dispose of, or destroy Protected Information, but only to the extent the Employee is authorized to do so by the Security Officer or Applicable Law.

6.3 *Company*: "Company" means Multi-State Billing Services, LLC and all of its Employees, officers, directors, managers, members, and owners, but not any Business Associate, independent contractor, or vendor of Multi-State Billing Services, LLC.

6.4 *Breach*: "Breach" means access to or acquisition, use or disclosure of Protected Information without authorization, beyond the scope of authorization, or in a manner or to an extent that compromises the confidentiality, integrity or availability of the Protected Information or that violates Applicable Law. A Breach shall not include access to or acquisition, use or disclosure of Protected Electronic Information that is Encrypted. A Breach also shall not include the unintended or good faith accessing, acquisition or use of Protected Information by an Authorized Employee related to fulfilling a duty for the Company, or the inadvertent disclosure of Protected Information by an Authorized Employee to another Authorized Employee or Business Associate, as long as the Protected Information is not otherwise further accessed, acquired, used or disclosed without authorization, beyond the scope of authorization, or in a manner or to an extent that compromises the confidentiality, integrity or availability of the Protected Information or that violates Applicable Law.

6.5 *Business Associate*: "Business Associate" means any Person, not an Employee, who (a) performs or assists in performing a function or activity for the Company involving the creation, receipt, acquisition, storage, maintenance, access, use, disclosure, transmission, transportation, disposal of, or destruction of Protected Health Information, or involving any other function or activity for the Company regulated by HIPAA, or (b) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to the Company that involve the use or disclosure of Protected Health Information.

6.6 *Electronic Device*: "Electronic Device" means any digital, analog, or electronic machine, device, system, account or service used to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, analyze, or manipulate computerized or electronic data, including the following: servers, routers, networks, hubs, desktop computers, Laptops, Tablets (*e.g.*, iPads and Droid tablets), handheld computers, smartphones (*e.g.*, iPhones, Droid phones, and Blackberries), cellphones, electronic readers (*e.g.*, Kindles), music players (*e.g.*, iPods, MP3 and MP4 players), internal and External Drives, USB drives (*e.g.*, flash, thumb and zip drives), digital cameras and video recorders, photo and video storage media, compact discs or CDs, digital video discs or DVDs, other data storage media, digital telephone and voicemail systems, photocopiers, calculators, cloud storage, social media, micro-blogs, and blogs.

6.7 *Employee*: "Employee" means a Person employed by the Company, but not a Business Associate, independent contractor, or vendor of the Company.

6.8 *Encrypt*: "Encrypt" means to transform data through use of an algorithmic process into a form where there is a low probability of assigning meaning to the data without the use of a confidential process, key, security code, access code, or password; provided that this term shall not include data acquired in combination with, or accessed or acquired using, the process, key,

security code, access code, or password that permits access to the data, or data acquired where the process, key, security code, access code, or password has been Breached.

6.9 *External Drive*: "External Drive" means a digital, analog, or electronic machine or device external to a computer used to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, analyze, or manipulate computerized or electronic data, including the following: external hard drives, USB drives (*e.g.*, flash, thumb and zip drives), photo and video storage media, compact discs or CDs, and digital video discs or DVDs.

6.10 *HIPAA*: "HIPAA" means the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic an Clinical Health Act of 2009; Code of Federal Regulations, Section 45, Parts 160, 162 and 164; and all amendments to the foregoing, administrative regulations promulgated pursuant to the foregoing, and published administrative and judicial interpretations of the foregoing.

6.11 *Information Systems*: "Information Systems" means a system of multiple Electronic Devices used to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, analyze, or manipulate computerized or electronic data.

6.12 *IT Officer*: "IT Officer" means the Employee designated by the Company to assume the authority and responsibility of the IT Officer under this Policy. The Employee initially designated to be the IT Officer is William Goodhue. The Company has the discretion to designate, at any time and for any reason, a different Employee to serve as the IT Officer, or an additional Employee or Employees to assist the IT Officer or serve as co-IT Officers.

6.13 *Laptop*: "Laptop" means a computer designed to be transported from place to place by the user or that the user routinely transports from place to place; provided that this term does not include the following: Tablets (*e.g.*, iPads and Droid tablets), handheld computers, Smartphones (*e.g.*, iPhones, Droid phones, and Blackberries), cellphones, electronic readers (*e.g.*, Kindles), music players (*e.g.*, iPods, MP3 and MP4 players), or External Drives.

6.14 *Person*: "Person" means any individual or entity, including a sole proprietorship, partnership, corporation, limited liability company, limited liability partnership, professional association, professional corporation, S corporation, and any other entity whatsoever.

6.15 *Policy*: "Policy" means this Protected Information Security Policy, as well as all predecessors, successors, additions, modifications, amendments, addendums and appendices to this Protected Information Security Policy.

6.16 *Protected Documentary Information*: "Protected Documentary Information" means Protected Information rendered into a tangible physical medium such as a document or other hard copy format.

6.17 *Protected Electronic Information*: "Protected Electronic Information" means Protected Information in digital, analog, computerized or electronic format.

6.18 *Protected Health Information*: "Protected Health Information" means (a) any information related to any physical or mental health or condition of an individual, the provision of health care to the individual, or the payment for health care for an individual, where (b) that information specifically identifies the individual, or there is a reasonable basis to believe that the information can be used to identify the individual; provided that this term does not include information related to a student maintained by an educational agency or institution or a person

acting for such an agency or institution, or information related to an Employee that the Company has in its role as the employer of the Employee.

6.19 *Protected Information*: "Protected Information" means Protected Health Information, Protected Personal Information, and any other information that the Security Officer designates as Protected Information. This term includes all Protected Electronic Information and all Protected Documentary Information.

6.20 *Protected Personal Information*: "Protected Personal Information" means (a) the last name of an individual, together with that individual's first name or the first initial of the first name, in combination with (b) any of the following for that individual (i) social security number, (ii) governmental identification number, including driver's license and non-drivers identification number, (iii) credit, debit, insurance, or other financial account number, with or without any username, password, personal identification number, or other code necessary to access or control such account, and (iv) password, personal identification number, or other code used to access or control any credit, debit, insurance, or other financial account, provided that (c) any information in sub-paragraph (b) shall alone constitute Protected Personal Information, even when not in combination with information in sub-paragraph (a), if the information would be sufficient to permit a Person to assume or attempt to assume the identity of the individual or if it is reasonable to believe that the information would be sufficient to identify the individual; provided that this term does not include any information that is generally publically available, including from any local, state or federal governmental records, as long as such information did not become generally publically available through the violation of a Person's obligation to maintain the confidentiality of that information, including pursuant to this Policy, Applicable Law, or an applicable contract.

6.21 *Security Officer*: "Security Officer" means the Employee designated by the Company to assume the authority and responsibility of the Security Officer under this Policy. The Employee initially designated to be the Security Officer is Rebecca Martin or, in the absence of Rebecca Martin, William Goodhue. The Company has the discretion to designate, at any time and for any reason, a different Employee to serve as the Security Officer, or an additional Employee or Employees to assist the Security Officer or to serve in as co-Security Officers.

6.22 *Smartphone*: "Smartphone" means a handheld digital, analog, or electronic device used to create, receive, acquire, store, maintain, access, use, transmit, transport, analyze, or manipulate computerized or electronic data, including iPhones, Droid phones, Blackberries and other cellphones; provided that this term does not include Laptops, External Drives or Tablets.

6.23 *State Law*: "State Law" means New Hampshire Revised Statutes Annotated, Chapter 359-C, Section 19 to 21; Massachusetts General Laws, Chapter 93H, Sections 1 to 6; Code of Massachusetts Regulations, Chapter 17.00, Section 17.01 to 17.05; Maine Revised Statutes, Title 10, Sections 1346 to 1350-B; Vermont Statutes, Title 9, Sections 2430 to 2435; and all amendments to the foregoing, administrative regulations promulgated pursuant to the foregoing, and published administrative and judicial interpretations of the foregoing.

6.24 *Tablet*: "Tablet" means a portable digital, analog, or electronic device used to create, receive, acquire, store, maintain, access, use, transmit, transport, analyze, or manipulate computerized or electronic data, including iPads, Droid tablets, and electronic readers (*e.g.*, Kindles); provided that this term does not include Laptops, External Drives or Smartphones.