

NON DISCLOSURE / DATA PROCESSING AGREEMENT
FOR SERVICES AND FUNCTIONS PROVIDED ON BEHALF OF THE BOE

This agreement (“Agreement”) is dated October 1, 2020 between
The Board of Education of the City of New York with an address at 52 Chambers Street, New York, New
York 10007 (“BOE”)
and
Somos Healthcare Inc. D/B/A Somos Community Care (“Vendor”) with an address at 519 Eighth Avenue,
14th Floor, New York, NY 10018

1. Definitions. “Biometric Record” means a record of one or more measurable biological or behavioral characteristics that can be used to recognize or identify an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

“NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, or any successor thereto.

“Process” or “Processing” means to perform any act, omission or operation on or with respect to data or information, such as accessing, adapting, altering, blocking, collecting, combining, delivering, deleting, destroying, disclosing, disseminating, erasing, generating, learning of, organizing, recording, releasing, retrieving, reviewing, sharing, storing, transmitting, using or otherwise making data or information available.

“Protected Information,” as it relates to BOE’s current, future and former employees, students, and their family members (together, “Subjects”), includes, but is not limited to (a) personal and family names, and any variation or abbreviation of a name; (b) physical and electronic addresses, telephone or mobile phone numbers, and geolocation; (c) Biometric Records; (d) personal identifiers, such as social security numbers, student identification numbers, staff identification numbers; (e) indirect identifiers, such as date of birth and place of birth; (f) health information relating to any Subject or their contacts; (g) any other information that, alone or in combination, is linked or linkable to a specific Subject that would allow a reasonable person in a school community, who does not have personal knowledge of the Subject or contact or the relevant circumstances, to identify or locate the Subject with reasonable certainty; or (h) information requested by a person who the Vendor or BOE reasonably believes knows the identity of the Subject or contact e to whom the information relates.

2. Confidentiality. In accordance with the Family Educational Rights and Privacy Act and its implementing regulations (respectively 20 U.S.C. 1232g and 34 C.F.R. Part 99 and together, “FERPA”), the Vendor agrees that it is conducting the services described in the Speciman Collection Agreement (the “Agreement”) dated, October 9, 2020, and attached hereto as Attachment A, on behalf of the BOE, and is acting as a “school official” pursuant to 34 C.F.R. 99.31(a)(1)(B). The Vendor agrees to hold and Process the Protected Information in strict confidence, and not to disclose Protected Information to, or otherwise permit the Processing of Protected Information by, any other parties, nor to Process such Protected Information for the benefit of another or for any use or purpose other than for providing the Services as required of Vendor as detailed within the Agreement. The confidentiality and data security obligations of the Vendor under this Agreement shall survive any termination of this Agreement. The Vendor agrees to conduct the Services in a manner that does not permit the personal identification of Subjects by anyone other than Authorized Users with legitimate interests in the Protected Information. Vendor agrees to not collect any Biometric Records of Subjects as part of the Services, except to the extent documents in Subjects’ handwriting (for example, on consent forms) are provided to or collected by Vendor.

3. Authorized Users. The Vendor shall only disclose Protected Information to its employees (hereinafter referred to as “Personnel”), and its nonemployee agents, assignees, consultants or subcontractor (hereinafter collectively referred to as “Non-Employee Vendors,” and together with Personnel, “Authorized Users”) who need to Process the Protected Information in order to carry out the Services and in those instances only to the extent justifiable by that need. The Vendor shall ensure that all such Authorized Users comply with the terms

of this Agreement. The Vendor agrees that upon request by the BOE, it will provide the BOE with the names and affiliations of the Non-Employee Vendors to whom it proposes to disclose, or has disclosed, Protected Information. The Vendor agrees and acknowledges that the data protection obligations imposed on it by state and federal law, as well as the terms of this Agreement, shall apply to any Non-Employee Vendor it engages to Process Protected Information of the BOE. The Vendor therefore The Vendor agrees to ensure that each Non-Employee Vendor is contractually bound by an agreement that includes confidentiality and data security obligations equivalent to, and no less protective than, those found in this Agreement. Vendor agrees and acknowledges that the data protection obligations imposed on it by state and federal law, as well as the terms of this Agreement shall apply to any Subcontractor it engages in providing the Services to the BOE.

4. Compliance with Law.

- (a) The Vendor agrees to hold all Protected Information it Processes in compliance with all applicable provisions of federal, state and local law, including but not limited to FERPA and New York Education Law §2-d and any applicable regulations promulgated thereunder. The Vendor understands that the disclosure of Protected Information to persons or agencies not authorized to receive it is a violation of United States federal law and New York state law, which may result in civil and/or criminal penalties under New York State and Federal laws.
- (b) In the event that disclosure of Protected Information (including Protected Information) is required of the Vendor under the provision of any law, judicial order or lawfully-issued subpoena, the Vendor will (a) promptly notify the BOE of the obligations to make such disclosure sufficiently in advance of the disclosure, if possible, to allow the BOE to seek a protective order or to make any notifications required by law, and (b) disclose such Protected Information only to the extent (i) allowed under a protective order, if any, or (ii) necessary to comply with the law or court order. Notwithstanding the foregoing, the BOE acknowledges that the Vendor is required under applicable federal and state law to report certain laboratory testing results, and shall not be required to notify BOE of any such mandatory reporting.

5. Mandatory N.Y. Education Law 2-d Requirements.

- (a) BOE Data Privacy and Security Policies. Vendor agrees that it will comply with the BOE's data privacy and security policies, including but not limited to New York City Department of Education Chancellor's Regulation A-820, and any successor thereto.
- (b) Subject Data Requests. If permitted by law, the Vendor agrees to notify the BOE of any requests it receives from Subjects or parties authorized by Subjects to amend, inspect, obtain copies of, or otherwise access Protected Information of such Subject in the possession or control of the Vendor, in advance of compliance with such requests. The Vendor shall defer to the judgment of the BOE in granting or denying such requests, and in confirming the identity of Subjects and the validity of any authorizations submitted to the Vendor. The Vendor agrees to assist the BOE in processing such requests in a timely manner, whether received by the Vendor or by the BOE. The Vendor shall amend any Protected Information in accordance with the BOE's decision and direction. Notwithstanding the foregoing, the Vendor shall not be required to notify the BOE if a Subject requests his or her laboratory testing records, and the BOE acknowledges that the Vendor is required under federal and state law to promptly provide such records to a requesting Subject.
- (c) Training. The Vendor shall ensure that all Authorized Users with access to the Protected Information are trained, prior to receiving such access and thereafter on a periodic basis, in their confidentiality and data security responsibilities under applicable law and understand the privacy and data security obligations of this Agreement.
- (d) Privacy and Security Plan; Additional Data Privacy and Security Protections. The Vendor shall neither retain nor incorporate any of the Protected Information into any database or any medium other than as may be required for it to provide the Services and as required under applicable federal and state law and regulations as well as laboratory accreditation and certification requirements. Vendor agrees to maintain appropriate administrative, technical and physical safeguards in accordance with industry best practices and applicable law to protect the security, confidentiality and integrity of Protected

Information in its custody. Vendor agrees to adhere to its data privacy and security plan and the BOE Information Security Requirements (together, the “Plan”), attached hereto as Attachment B. Vendor warrants and represents that (i) its technologies, safeguards and practices, as outlined in the Plan, align with the NIST Cybersecurity Framework, and include sufficient (A) data privacy protections, including processes to ensure that personally identifiable information is not included in public reports or other public documents; and (B) data security protections, including data systems monitoring, encryption of data in motion and at rest, an incident response plan, limitations on access to Protected Information, safeguards to ensure Protected Information is not accessed by unauthorized persons when transmitted over communication networks, and destruction of Protected Information when no longer needed; and (ii) that its Plan meets all additional requirements of New York Education Law 2-d. The Vendor agrees to use encryption technology to protect Protected Information both (i) while in motion or in transit and (ii) while stored, at rest or otherwise in its custody from unauthorized Processing using a technology or methodology specified by the United States Department of Health and Human services in guidance issued under Section 13402(H)(2) of Public Law 111-5. The Vendor acknowledges and agrees to conduct digital and physical periodic risk assessments and to remediate any identified security and privacy vulnerabilities in a timely manner. The BOE reserves the right to request information from Vendor regarding its security practices and compliance with the Plan, prior to authorizing any exchange of Protected Information. The BOE reserves the right to work with the Vendor to develop a risk mitigation plan to resolve any deficiencies in its compliance with the Plan. The BOE reserves the right to promptly terminate the Agreement with no further liability to the Vendor, in the event that the Vendor fails to comply with such risk mitigation plan or is unable to resolve its noncompliance with the Plan. The BOE may audit the Vendor’s Processing of the Protected Information for data privacy and data security purposes.

- (e) Parent Bill of Rights. The Vendor agrees to comply with the BOE Parents’ Bill of Rights for Data Privacy and Security, attached hereto as Attachment C. The Vendor shall complete the Supplemental Information section of Attachment C, and append it to this Agreement. The Vendor acknowledges and agrees that the BOE shall make Vendor’s Supplemental Information public, including but not limited to posting it on the BOE’s website.
- (f) Reportable Data Events. The Vendor shall promptly notify, without unreasonable delay, the BOE Office of Legal Services at 212-374-6888 and at AskLegal@schools.nyc.gov (to the attention of the Chief Privacy Officer) of any act, error or omission, negligence, misconduct, or breach (including any unauthorized release, use or disclosure of, access to Protected Information, whether by the Recipient, its Authorized Users or any other party that shall have gained access to the affected Protected Information) that compromises or is suspected to compromise the security, confidentiality, availability or integrity of Protected Information, including by compromising the physical, technical, administrative or organizational safeguards implemented by the Recipient (“Reportable Data Event”). In no event shall such notification occur more than seventy-two (72) hours after confirmation that a Reportable Data Event occurred. Moreover, to the extent (a) New York Education Law 2-d or any other law or regulation requires parties affected by the Reportable Data Event to be notified, and (b) the Reportable Data Event is not attributable to the acts or omissions of the BOE, the Vendor shall compensate the BOE for the full cost of any notifications that the BOE is required by law to make. Vendor agrees to assist and collaborate with the BOE in ensuring that required notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: (a) a brief description of the Reportable Data Event, the dates of the incident and the date of discovery, if known; (b) a description of the types of Protected Information affected; (c) an estimate of the number of records affected; (d) a brief description of the investigation or plan to investigate; and (e) contact information for representatives who can assist parents or adult students that have additional questions. The Vendor shall provide any records or other information the BOE requires to investigate the incident or to effectuate the notifications. The Vendor shall fully cooperate with and assist the BOE in investigating the Reportable Data Event, including, without limitation, by providing full access to persons or information necessary to determine the scope of the Reportable Data Event, such as all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the BOE.

(g) No Sale or Commercial Use. The Vendor agrees that it will not sell Protected Information; use, disclose or otherwise Process Protected Information for purposes of receiving remuneration, whether directly or indirectly; or use, disclose or otherwise Process Protected Information for marketing, commercial or advertising purposes (or facilitate its use, disclosure or other Processing by any other party for such purposes), or to develop, improve or market products or services to students, or permit another party to do so.

6. Right to Termination. The BOE shall have the right at its sole discretion to terminate the Vendor's access to the BOE's Protected Information upon fifteen (15) days written notice to the Vendor. The BOE shall have the right at its sole discretion to terminate the Vendor's access to the BOE's Protected Information immediately upon the Vendor's breach of any confidentiality obligations herein. No claim for damages will be made or allowed to the Vendor because of said termination.

7. Protected Information Retention, Transfer and Destruction. Whenever required by the BOE, and no later than upon termination of this Agreement, except for Protected Information which the Vendor is required to retain under applicable federal or state law and regulation as well as laboratory accreditation and certification requirements, the Vendor shall promptly (a) with respect to physical copies of Protected Information, surrender, or if surrender is not practicable, securely delete or otherwise destroy Protected Information and (b) with respect to digital and electronic Protected Information, securely delete or otherwise destroy Protected Information remaining in the possession of the Vendor and its Authorized Users, (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data). Vendor shall ensure that no copy, summary, or extract of Protected Information are retained on any storage medium whatsoever by Vendor or its Authorized Users, except as otherwise provided in this Agreement. Any and all measures related to the extraction, transmission, deletion, or destruction of Protected Information will be accomplished utilizing an approved, appropriate and secure method of destruction, including shredding, burning or certified/witnessed destruction of physical materials and verified erasure of electronic media. To the extent that the Vendor continues to be in possession of de-identified data, it agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party for re-identification. The Vendor agrees not to retain any de-identified Biometric Records. The Vendor shall certify, in writing, that all of the foregoing materials have been surrendered or destroyed (as applicable), except as otherwise provided in this Agreement, in accordance with this Agreement via the "Certificate of Records Disposal" form attached to this Agreement as Attachment D. Provider shall dispose of Protected Information when it is no longer needed to carry out the Services, except as otherwise provided in this Agreement, and shall submit the form found in Attachment D upon disposition. The obligations of this agreement shall apply for so long as Vendor maintains, or is responsible for maintaining, any Protected Information.

8. BOE Property. All Protected Information (a) created or collected by the Vendor, or (b) disclosed or transmitted to the Vendor, pursuant to this Agreement, shall remain the exclusive property of the BOE, or (as applicable) the Subjects. All rights, including the intellectual property rights in and to Protected Information contemplated per this Agreement shall remain the exclusive property of the BOE. Any reports or work product may not contain any Protected Information, unless required by the BOE or if necessary to carry out the Services.

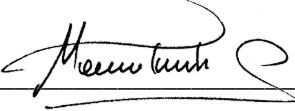
9. Other Agreements. The Vendor agrees that to the extent that any confidentiality or data security terms or conditions regarding the Services found in another agreement binding BOE employees, subcontractors, parents or students (together, "BOE Users,") including but not limited to any end-user license agreement, "click wrap," "click-through," "click and accept," "web-wrap," or other form of agreement requiring the individual user to accept terms in order to use or benefit from the Services, conflict with the terms found in this Agreement, the terms and conditions which afford more protection to BOE Users shall apply. Any subsequent agreements between the Vendor and the BOE with respect to the provision of the Services shall include confidentiality and data security obligations on the part of the Vendor at least as strict as set those forth in this Agreement. In the event a subsequent agreement fails to contain confidentiality and data security provisions with obligations at least as strict as this Agreement, the confidentiality provisions of this Agreement shall be deemed inserted therein, and shall continue to bind the Vendor, unless such subsequent agreement specifically references this Agreement by name and disclaims its obligations in writing.

10. Other Terms.

- (a) The Vendor agrees that money damages would be an insufficient remedy for breach or threatened breach of this Agreement by the Vendor. Accordingly, in addition to all other remedies that the BOE may have, the BOE shall be entitled to specific performance and injunctive or other equitable relief as a remedy for any breach of the confidentiality and other obligations of this Agreement.
- (b) Nothing in this Agreement obligates either party to consummate a transaction, to enter into any agreement or negotiations with respect thereto, or to take any other action not expressly agreed to herein.
- (c) The Vendor shall defend, indemnify and hold harmless the BOE and the City of New York from any and all claims brought by third parties to the extent arising from, or in connection with, any negligent acts or omissions of the Vendor and the Vendor's Authorized Users or any other representatives for whom the Vendor is legally responsible for, in connection with the performance of this Agreement.
- (d) No failure or delay (in whole or in part) on the part of either party hereto to exercise any right or remedy hereunder shall impair any such right or remedy, operate as a waiver thereof, or affect any right or remedy hereunder. All rights and remedies hereunder are cumulative and are not exclusive of any other rights or remedies provided hereunder or by law or equity. To the extent any provision of this Agreement is held to be unenforceable or invalid, the remainder of the Agreement shall be remain in full force and effect, and the Agreement shall be interpreted to give effect to the such provision to the maximum extent permitted by law.
- (e) This Agreement shall be governed by and construed in accordance with the law of the State of New York. The Federal or State Courts of New York City, New York will have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this Agreement. This Agreement constitutes the entire Agreement with respect to the subject matter hereof; it supersedes any other Vendor terms and conditions, all prior agreements or understandings of the parties, oral or written, relating to the Services and shall not be modified or amended except in writing signed by the Vendor and the BOE. The Vendor may not assign or transfer, without the prior written consent of the BOE, this Agreement. This Agreement shall inure to the benefit of the respective parties, their legal representatives, successors, and permitted assigns. This Agreement is effective upon execution of the Vendor.

Signed and Agreed to:

**Somos Healthcare Inc. D/B/A Somos
Community Care**

By: 

Date: 10/15/20

Name: Mario J. Paredes

Title: CEO

Vendor Acknowledgment

State of New York }
 } ss.:
County of New York }

On this ____ day of _____, 202__, before me, the undersigned, a Notary Public in and for said State, personally appeared one _____, personally known to me or proved to me on the basis of satisfactory evidence to be the individual whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her capacity, and that by his/her signature on the instrument, the entity or individual upon behalf of which the individual acted, executed the instrument.

_____ NOTARY PUBLIC

Attachment A:
Specimen Collection Agreement

SPECIMEN COLLECTION AGREEMENT

This Agreement (“Agreement”) is made as of October __, 2020 (the “**Effective Date**”) by and between **Somos Healthcare Providers Inc. D/B/A Somos Community Care** with offices at 519 Eighth Avenue, 14th Floor, New York, NY 10018 (“**Somos**”) and **NEW YORK CITY HEALTH AND HOSPITALS CORPORATION**, a New York public benefit corporation with offices at 125 Worth Street, New York, NY 10013 (“**H+H**”). Somos and H+H may each be referred to herein as a “**Party**” and together as the “**Parties.**”

WITNESSETH

WHEREAS, the City of New York (the “**City**”) acting by and through its Department of Education (“**DOE**”) wish to implement a system of testing its students and staff for COVID-19; and

WHEREAS, the City’s Department of Health and Mental Hygiene (“**DOHMH**”) has statutory responsibility for DOE school-based health programs; and

WHEREAS, DOHMH has designated H+H as its authorized agent and as its qualified representative for purposes of the activities contemplated herein;

WHEREAS, DOE and DOHMH have asked H+H to contract for the necessary testing services on their behalf; and

Whereas, Somos possesses the ability to arrange for the provision of professional services by and through its network of Medical Providers (“**Medical Providers**”) who have agreed with Somos to provide the professional services indicated herein to and for H+H; and

WHEREAS, the Parties wish to provide for Somos to obtain laboratory specimens (“**Swabbing**”) suitable for COVID-19 RT-PCR diagnostic testing (“**Diagnostic Tests**”) from DOE students (“**Tested Students**”) and DOE staff (“**Tested Staff**”) designated by H+H, which professional services are to be provided by and through those Medical Providers who have agreed with Somos to perform such Swabbing all under the terms and conditions of this Agreement; and

WHEREAS, H+H has separately contracted with BioReference Laboratories, Inc. (“**BRL**”) to perform Diagnostic Tests on specimens obtained by Somos hereunder as well as on specimens BRL itself obtains as well as to provide such other services related to BRL’s performance of its functions as outlined in the Agreement by and between BRL and H+H; and

WHEREAS, in view of DOHMH’ statutory authority, it will be appropriate for the results of the Diagnostic Tests to be communicated to DOHMH and H+H, as provided herein, as well as to the parents or guardians of Tested Students, to Tested Staff and to Tested Students who are over the age of 18.

NOW THEREFORE, in consideration of the foregoing premises and mutual promises, and intending to be legally bound, the parties agree as follows:

1. **Overview of NYC School System Student Testing Program.** Commencing on or about the Effective Date, Somos will commence Swabbing at the locations designated by H+H (the “**Collection Sites**”) as per Attachment “1” and perform the Swabbing for approximately 3,300 persons each month. The Collection Sites will all be in City public schools in School Districts 3, 5, 6, 9, 10, and 79.
2. **Consent to Testing and Authorization for Disclosure of Test Results.** H+H acknowledges that most of the Tested Students will be minors and therefore legally unable to consent to Swabbing and the Diagnostic Tests or authorize the disclosure of the Diagnostic Test results. H+H shall be responsible to obtain, or cause DOE to obtain, all necessary HIPAA appropriate consents and authorizations from the parents or other legal guardians of Tested Students who are under the age of 18, from Tested Staff and directly from Tested Students who are 18 years of age or older. The form of consent is attached as Attachment 3.
3. **Collection Sites; Schedules.** Swabbing for the Diagnostic Tests shall be performed at the Collection Sites during the days and times as agreed to by Somos to ensure every location is tested at least one time per month. Monthly, H+H will provide Somos a list of all individuals who are eligible for testing and a list 2 days prior to Somos’s arrival at a school to conduct Swabbing in order to know the specific individuals that are to be Swabbed. Included with such list, H + H shall provide the following information for each test subject: name; address; date of birth; parent/guardian’s name (if test subject is a minor); telephone for test subject’s parent/guardian, if test subject is a minor or for test subject if an adult; email address for subject’s parent/guardian, if test subject is a minor or for test subject if an adult and preferred language, if not English.. Somos will use that information to expedite the Swabbing by pre-registering and/or pre-accessioning all individuals expected to be tested prior to the arrival of the testing team at the scheduled school location. H+H shall ensure, through DOE, that adequate social distancing space is made available and maintained at the Collection Sites as required under applicable federal, state, and local law or as deemed advisable by Somos.
4. **Management of Collection Sites.** H+H has contracted with DOE to provide Collection Sites in its schools, to ensure that they are clean, to assist in the scheduling of individual DOE students and staff for specimen collection, to work to produce the individuals as scheduled for specimens to be taken for the Diagnostic Tests, to ensure students and/or staff scheduled to be tested have provided the legally required HIPAA consent for each individual to be tested and for the test results to be disclosed as herein provided, and to help to manage the flow of individuals at the Collection Sites and to clean such sites after each testing session.

5. **Specimen Collection.** Medical Providers shall perform the specimen collection for the Diagnostic Tests at the Collection Sites, in accordance with the schedule mutually agreed upon by the Parties. Somos shall be responsible for the costs associated with the Swabbing performed by the Medical Providers who shall be responsible for providing qualified personnel to conduct the Diagnostic Tests and for all required personal protective equipment. H+H shall cause BRL to supply the test kits required for the Swabbing which shall be delivered to Somos' offices. Somos shall be responsible for the removal and disposal of all personal protective equipment used in the collection process from the Collection Site. H+H shall cause BRL to collect from Somos the specimens obtained from Swabbing.
6. **Staffing.** Somos shall ensure that each collection site shall be staffed by those contracted Medical Providers who shall provide qualified staff ("Qualified Personnel") to collect specimens suitable for Diagnostic Tests at all assigned locations. Somos shall provide administrative personnel who shall be responsible for all the non-professional aspects of the Collection Site. A typical team is expected to include two persons who are the Qualified Personnel who are trained and able to perform the nasal swabs appropriate for the Diagnostic Tests as well as a non-professional administrative staff person to handle paperwork and assist in the administrative management of the Collection Site. Somos shall monitor reporting of Diagnostic Test results to monitor those test results which have not been reported for more than forty-eight (48) hours and will serve to *laissez* with the testing laboratory regarding those overdue results.
7. **Somos Representations and Warranties.** Somos represents and warrants to H+H as follows: (i) that it is properly organized and licensed to operate within the State of New York and is a legal not-for-profit entity; (ii) that the Medical Providers are all familiar with the terms of this Agreement; (iii) that each Medical Provider has explicitly agreed to be bound by the terms of the Agreement; (iv) that every representation Somos makes in this Agreement shall be understood to apply, where appropriate, to the Medical Providers; and (v) that Somos shall defend, indemnify and hold H+H harmless from and against any claim, suit, damage, cost or penalty that are brought against, suffered or incurred because of any failure of a Medical Provider to adhere to the terms of this Agreement and any failure of any representation made herein regarding a Medical Provider to be true.
8. **Fees.** H+H shall pay \$3,520.00 (the "Fee") to Somos for each three-person team per each Collection Site who shall work up to 8-hours per day which fee shall include Swabbing and the reporting of results as provided herein.
9. **Laboratory Results.** H+H shall cause BRL to report the results of the Diagnostic Tests to the Medical Provider who performed the Swabbing, H+H and to DOHMH.
10. **Reporting of Results.** Medical Providers who performed the Swabbing shall call parents or guardians of the Tested Students, Tested Students over 18 years of age and Tested Staff with their test results. An initial attempt must be made within one

business day after receipt of the laboratory results, if the first attempt is unsuccessful Somos shall make another attempt within the next day, and a third will be made within the next business day should the first two attempts fail.

11. Other Reporting. Somos will be responsible for providing H+H with the following reports:

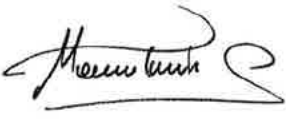
- a. Daily reports including the following each of which shall break out the numbers by each Collection Site:
 - i. Specimen collections scheduled per day
 - ii. Specimens per day actually collected
 1. Number pending
 2. Number cancelled/otherwise not resulted
 - iii. Number of results where Somos attempted notification within agreed upon timeframe (broken out by positive and negative). Report should also include the following aggregate information (does not need to be broken out by school):
 - iv. Status update on results beyond 48 hours
 1. Number of results beyond 48 hours
 2. Number that have been resulted: positive
 3. Number that have been resulted: negative
 4. Number still pending: 48-72 hours
 5. Number # still pending: 72-96 hours
 6. Number # still pending: 96+ hours

12. Term. This Agreement shall be in effect from the Effective Date until the first anniversary of the Effective Date; provided that either Party may terminate this Agreement at any time for its convenience on thirty days' notice.

13. H+H Terms and Conditions. H+H's Standard Terms and Conditions as attached hereto are hereby incorporated into the Agreement.


IN WITNESS HEREOF, the Parties have signed this Agreement as of the Effective Date.

SOMOS HEALTHCARE PROVIDERS INC. NEW YORK CITY HEALTH AND HOSPITALS CORPORATION

By: 

Name: Mario J. Paredes

Title: CEO

By: 

Name: PAUL A. AUSENTSON

Title: VP

**New York City Health and Hospitals Corporation's
Standard Terms and Conditions**

These terms and conditions ("Terms and Conditions") are entered into as of the ___ day of September, 2020 ("Effective Date") by and between New York City Health and Hospitals Corporation, located at 125 Worth Street, New York, New York 10013, ("NYC Health + Hospitals") and Somos Healthcare Providers Inc. D/B/A Somos Community Care with offices at 519 Eighth Avenue, 14th Floor, New York, NY 10018 ("Vendor"), each individually referred to as a party ("Party") and collectively referred to as the parties ("Parties").

Definitions

Agreement: the agreement between the Parties consists of these Terms and Conditions and the agreement made between the Parties this date ("Incorporated Document").

The City: The City of New York.

Diversity Vendor: a company that is generally recognized in the field of diversity contracting as diverse. Recognition of diversity may include, for example, an MWBE certification by New York State, the City, or by a third-party, such as the Women's Business Enterprise National Council (WBENC).

Goods: include tangible items, such as commodities (e.g., gloves, paper, furniture, pharmaceuticals, computers), equipment (e.g., x-rays, generators), and intangible items where most of the cost is not attributable to a service (e.g., stock software would be considered a Good whereas a custom developed interface would be considered a Service).

NYC Health + Hospitals: New York City Health and Hospitals Corporation, a public benefit corporation established by the laws of the State of New York.

Services: actions provided by a Vendor for the benefit of NYC Health + Hospitals, such as software support, equipment maintenance, professional services (e.g., legal), non-professional services (e.g., cleaning), consultations, and the like.

Vendor: the individual or entity providing Goods or Services directly or indirectly through its network of contracted Medical Providers or other associated entities under this Agreement.

Vendor Employee(s): owners, partners, members, officers, directors, employees, agents, or any other person under the reasonable control of Vendor.

Medical Provider: owners, partners, members, officers, directors, employees, agents, or any other person under the reasonable control of the licensed healthcare professional who have agreed to be responsible for the professional provision of services hereunder and under this Agreement.

Article I. Mandatory Terms and Conditions

1. Term and Extension of Term

Reserved.

2. Termination

This Agreement may be terminated at any time during the term of this Agreement in whole or in part (i) by NYC Health + Hospitals with or without cause upon thirty days written notice and without liability for any damages resulting therefrom, (ii) if either Party breaches this Agreement, and has failed to cure such breach within thirty days after receiving written notice from the non-breaching Party, provided, however, that if the breach is of such a nature that it cannot be cured within such thirty day period, the breaching Party shall be allowed a reasonable time within which to cure, provided that the breaching Party gives notice to the non-breaching Party within such thirty day period of its intention to cure and the manner in which it intends to cure, or (iii) immediately if a Party becomes insolvent, a Party has a proceeding under the federal or State Bankruptcy Act, either voluntarily or involuntarily, or a Party has a receiver appointed.

3. Order of Precedence

These Terms and Conditions shall prevail in the event of a conflict between these Terms and Conditions and any Incorporated Documents.

4. Governing Law

This Agreement shall be governed, construed and enforced in accordance with the laws of the State of New York without giving effect to its principles of conflicts of laws.

5. Legal Disputes

5.1 Pursuant to New York City Health and Hospitals Corporation Act, Chapter 1016-69, Section 20, all actions against NYC Health + Hospitals shall be brought in the City, in the county in which the cause of action arose, or if it arose outside of the City, in the City, County of New York. The Parties consent to the dismissal or transfer to any claims asserted inconsistent with this section. If Vendor initiates any action in breach of this section, Vendor shall promptly reimburse NYC Health + Hospitals for any attorneys' fees incurred to remove the action to the contractually agreed upon venue.

5.2 Actions against NYC Health + Hospitals by Vendor arising out of this Agreement must be commenced within six months of the expiration or termination of this Agreement.

5.3 Neither Party shall make a claim for personal liability against any individual, officer, agent or employee of the other, nor of the City, pertaining to anything done or omitted in connection with this Agreement.

6. New York State Law 10 NYCRR 400.4

Notwithstanding any other section of this Agreement, NYC Health + Hospitals shall remain responsible for ensuring that any Services provided pursuant to this Agreement complies with all pertinent federal, state and local statutes, rules and regulations, and shall comply with Chapter V of Title 10 of the NY Code of Rules and Regulations, entitled "Medical Facilities – Minimum Standards."

7. Nondiscrimination

NYC Health + Hospitals' adopted Chapter 56 of the New York City Charter, formerly Mayor's Executive Order 50, dated April 25, 1980, as amended ("Chapter 56"), and the rules and regulations promulgated thereunder. Vendor shall comply with all rules and regulations under Chapter 56, and shall not engage in any unlawful discrimination. This section applies to all Vendor subcontractors, and Vendor Employees. Violation of this section may be deemed a material breach of this Agreement, and may result in a declaration of non-responsibility with NYC Health + Hospitals or the City.

8. MacBride Fair Employment Principles

This section does not apply if Vendor is a not-for-profit corporation or governmental entity. Pursuant to the MacBride Fair Employment Principles (Section 165 of the New York State Finance Law), Vendor warrants that it (i) has no business operations in Northern Ireland, or (ii) shall take lawful steps in good faith to conduct any business operations in Northern Ireland in accordance with the MacBride Fair Employment Principles, and shall permit independent monitoring of compliance with such principles by NYC Health + Hospitals or the City.

9. Diversity Contracting

Reserved

10. Investigations

10.1 Vendor shall fully cooperate with any reasonable related investigation, audit or inquiry conducted by NYC Health + Hospitals, the City, or the State of New York that is empowered directly, or by designation to compel the attendance of witnesses to examine under oath for matters strictly related to the services provided under this Agreement.

10.2 If Vendor, an officer or director of Vendor, or any person under the reasonable control of Vendor, refuses to testify for a reason other than the assertion of his or her privilege against self-incrimination in an investigation, audit, or inquiry conducted by NYC Health + Hospitals, the City, the State of New York that is a party in interest in, and is seeking testimony concerning the award of, or performance under, any transaction, agreement, lease, permit, contract, or license entered into with NYC Health + Hospitals, the City, the State of New York, any political subdivision thereof or local development, then NYC Health + Hospitals may convene a hearing, upon not less than five days written notice to the parties involved, to determine if any penalties shall attach for the failure of such person to testify.

10.3 The penalties that may attach after a final determination may include but shall not exceed: (i) the disqualification of Vendor for a period not to exceed five years from the date of an adverse determination for any person or any entity of which such person was a member at the time the testimony was sought, from submitting bids for, or transacting business with, or entering into or obtaining any contract, lease, permit or license with or from NYC Health + Hospitals or the City, and/or (ii) the cancellation or termination of any and all such existing NYC Health + Hospitals or City contracts, leases, permits, or licenses that the refusal to testify concerns and that have not been assigned as permitted hereunder, nor

the proceeds of which pledged, to an unaffiliated and unrelated institutional lender for fair value prior to the issuance of the notice scheduling the hearing, without NYC Health + Hospitals or the City incurring any penalty or damages on account of such cancellation or termination. Any monies lawfully due for goods delivered, work done, or fees accrued prior to the cancellation or termination shall be paid by NYC Health + Hospitals or the City, as applicable. As used in this paragraph license or permit shall be defined as a license, permit, franchise, or concession not granted as a matter of right.

11. Audit

11.1 At NYC Health + Hospitals' reasonable request made upon reasonable notice, Vendor shall make available all records and books pertaining to this Agreement during normal business hours for audit, inspection and/or investigation by NYC Health + Hospitals, the City, acting through its Comptroller, the U.S. government or any other persons authorized by NYC Health + Hospitals. Such audit, inspection and/or investigation may include examination and review of the source and application of all funds from NYC Health + Hospitals, the City, the State of New York, the federal government, private sources, or any other source. If an audit, inspection, or investigation is commenced as set forth in this section, NYC Health + Hospitals may withhold payment hereunder until Vendor provides the cooperation required hereunder.

11.2 Vendor shall maintain accurate books and records in accordance with generally accepted accounting principles. Vendor shall retain such documents for six years after the final payments, expiration or termination of this Agreement, whichever is later.

12. Fair Practices

12.1 Vendor warrants that no Vendor Employee is an elected official, officer or employee of NYC Health + Hospitals or the City.

12.2 Vendor, Vendor Employees shall not directly or indirectly give any gift in any form, including but not limited to money, service, loan, travel, entertainment to members of NYC Health + Hospitals' Board of Directors, Community Advisory Boards, officers, employees, or personnel.

12.3 Vendor shall not represent any party other than NYC Health + Hospitals related, or substantially related, to the Services to be performed under this Agreement without NYC Health + Hospitals' advance written consent.

12.4 Vendor warrants that neither Vendor nor any Vendor Employee has any conflict of interest relating to the performance of this Agreement which is materially adverse to NYC Health + Hospitals or the City and shall not acquire such conflict of interest during the term of this Agreement.

12.5 Any violation of the representations or warranties set forth in this section shall constitute a material breach of this Agreement, and NYC Health + Hospitals shall have the right to immediately terminate this Agreement as to Vendor or to an individual Medical Provider who provides Services hereunder without liability for any damages resulting therefrom.

13. HIPAA

13.1 If at any time NYC Health + Hospitals determines that a business associate agreement compliant with the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) ("HIPAA") is required to be executed to comply with HIPAA, Vendor shall comply with such requirement. Failure to comply with this section shall constitute a material breach of this Agreement and NYC Health + Hospitals shall have the right to immediately terminate this Agreement without liability for any damages resulting therefrom.

13.2 NYC Health + Hospitals is a Hybrid Entity and Organized Health Care Arrangement as defined under the HIPAA Privacy Rule. NYC Health + Hospitals' Correctional Health Services division does not engage in electronic transactions as defined in 45 CFR and was removed from HIPAA applicability at NYC Health + Hospitals' option pursuant to CFR 164.105(a)(2)(iii)(D). Any agreement exclusively for its Correctional Health Services division shall not require a business associate agreement.

14. Excluded Providers

14.1 Vendor represents and warrants that Vendor and Vendor Employees are not individuals or entities excluded from participation in federal or state health care programs. Vendor shall ensure the eligibility of Vendor and Vendor Employees to participate in federal and state health care programs and further warrants that it will notify NYC Health + Hospitals in writing if Vendor become excluded from such participation during the term of this Agreement. NYC Health + Hospitals may terminate this Agreement immediately without liability for any damages resulting therefrom should Vendor or Vendor Employees be excluded from participation in federal or state health care programs.

14.2 Vendor warrants that it is not currently a party to a Corporate Integrity Agreement or Certification of Compliance Agreement with any state or federal governmental agency. Vendor shall promptly notify NYC Health + Hospitals if it becomes a party to such agreement during the term of this Agreement.

15. Principles of Professional Conduct

If Vendor, Vendor's Employees, or any Vendor subcontractors, provide billing or coding functions, furnish health care services or items, or monitor the health care provided by NYC Health + Hospitals, then each such party shall comply with NYC Health + Hospitals' Principles of Professional Conduct ("POPC"), and shall (i) adopt the POPC or their own code of conduct that includes the POPC's core objectives or substantially similar compliance goals, (ii) not violate the POPC or their own similar code, (iii) not engage in unprofessional conduct as defined in the POPC, (iv) timely report to NYC Health + Hospitals in writing any violation of the POPC of which it becomes aware, and (v) fully cooperate, to the extent applicable, with any investigation by NYC Health + Hospitals, the City or by any governmental agency arising out of this Agreement.

16. Vendex

16.1 Vendor represents and warrants that any questionnaires submitted as part of the Vendex process have been, or will be, fully answered in accordance with the requirements set forth by the New York City Mayor's Office of Contract Services. The veracity of the information submitted is a material inducement to NYC Health + Hospitals' execution of this Agreement.

16.2 If clearance from the City's Office of Inspector General cannot be obtained prior to execution of this Agreement and if subsequent to the execution of this Agreement NYC Health + Hospitals receives information from the Office of the Inspector General of the kind that would typically lead to a finding that a vendor is not responsible to receive a contract from NYC Health + Hospitals, then NYC Health + Hospitals may terminate this Agreement immediately without liability for any damages resulting therefrom.

16.3 Vendor must submit new Vendex questionnaires every three years from the date of its last submission of Vendex questionnaires so long as this Agreement is in effect.

17. Vendor Responsibility

17.1 NYC Health + Hospitals may require Vendor to participate in its vendor credentialing system and Vendor shall comply with all such requirements of such system. If NYC Health + Hospitals receives information from its vendor credentialing system that leads to a finding that Vendor or Vendor's Employees are not responsible, then NYC Health + Hospitals shall have the right to immediately terminate this Agreement without liability for any damages resulting therefrom. Failure to comply with such program shall constitute a material breach of this Agreement and NYC Health + Hospitals shall have the right to immediately terminate this Agreement without liability for any damages resulting therefrom.

17.2 Vendor and Vendor Employees hereby waive all rights of recovery against NYC Health + Hospitals and its officers, employees, agents, and representatives for losses resulting from any disclosure of information as part of the vendor credentialing process. This section shall survive the termination or expiration of this Agreement.

18. Joint Commission Standards

If this Agreement falls within the scope of Joint Commission Standard LD.04.03.09 (the Goods or Services are directly related to patient care) then Vendor shall work in good faith with NYC Health + Hospitals to set forth specific key performance indicators in an attachment to this Agreement against which the performance of Vendor under this Agreement can be meaningfully measured on a regular periodic basis. Such attachment shall become part of this Agreement.

Article II. General Terms and Conditions

1. Independent Contractor

Vendor's relationship to NYC Health + Hospitals and the City are that of an independent contractor and not that of an employee. Vendor covenants that neither it nor any Vendor Employees will hold themselves out as, nor claim to be, employees of NYC Health + Hospitals or the City, and that they will not make any claim, demand, or application to or for any right or privilege applicable to an employee of NYC Health + Hospitals or the City including, but not limited to, Workers' Compensation, benefits, pension, payroll taxes, or Social Security.

2. Subcontractors

2.1 Vendor is not permitted to subcontract, in whole or in part, performance of any obligation under this Agreement, except as specifically indicated herein and within the Services Agreement, without the prior written consent of NYC Health + Hospitals. Approval by NYC Health + Hospitals of subcontractors specifically set forth in an approved Diversity Vendor Utilization Plan shall be considered prior written consent by NYC Health + Hospitals.

2.2 If NYC Health + Hospitals authorizes in writing Vendor's use of a subcontractor, then Vendor shall not be relieved of any obligation under this Agreement and shall ensure all work performed by such subcontractor is in accordance with this Agreement. Upon request, a copy of each proposed subcontract shall be provided to NYC Health + Hospitals.

3. Indemnification

3.1 Vendor shall defend and indemnify NYC Health + Hospitals and the City, their respective agents and employees from and against all actions, proceedings, claims, damages, losses, and expenses, including reasonable attorney fees, arising out of Vendor's performance, or failure to perform, under this Agreement except to the extent caused by the negligence or wrongful acts of NYC Health + Hospitals or the City or their agents or employees.

3.2 The foregoing right of indemnification is exclusive of any other rights to which NYC Health + Hospitals may be entitled hereunder and shall survive the expiration or termination of this Agreement.

4. Limitation of Liability

4.1 NYC Health + Hospitals' liability to Vendor arising out of this Agreement shall not exceed the amount that is unpaid to Vendor at the time such liability accrued.

4.2 Neither Party, nor their respective employees or agents, shall be liable to the other for indirect, punitive, exemplary or consequential damages. Neither Party's officers, directors, agents or employees shall have personal liability to the other Party under this Agreement except in cases of fraud.

5. Notices

5.1 All notices or communications required or permitted to be given hereunder shall be in writing and if to NYC Health + Hospitals shall be sent to 125 Worth Street, Room 527, New York, New York 10013, Attn: General Counsel and if to Vendor at the address specified below. Notices may be sent by hand delivery, U.S. Postal Service certified mail return receipt requested or by nationally recognized courier next business day delivery. Notices shall be deemed given upon delivery if delivery is made by hand, within three business days if sent by certified mail and on the next business day if sent by recognized courier with next business day delivery specified.

5.2 Notices to Vendor shall be sent to:

SOMOS Community Care
519 Eighth Avenue, 14th Floor
New York, NY 10018
Attention: Lidia Virgil, Chief Operating Officer

With a copy to Philip Kuszel, Esq.
via email at philaw2@aol.com

With a copy to Mario J. Paredes CEO
via email at mparedes@somoscommunitycare.org

6. Compliance with Law

Vendor shall comply with all applicable laws, rules and regulations, including New York State and the City's wage laws. Each and every provision of law required to be inserted in this Agreement shall be and is deemed to be included.

7. Criminal Background Checks

7.1 Vendor shall perform a criminal background check of each Vendor Employee performing under this Agreement and such check shall include a search of New York State Office of Court Administration's records for all New York counties, and a search through the records for any other state in which the person resided in the last three years (a "Background Check"), and shall be conducted prior to the effective date of this Agreement, unless such a Background Check was conducted on the Vendor Employee within the past year. A Background Check shall be conducted annually thereafter for the duration of this Agreement for each of Vendor's Employees performing under this Agreement.

7.2 NYC Health + Hospitals may require Vendor to perform a more extensive background check on Vendor Employees that will have direct contact with mentally ill or minor patients, provide nursing home or home health care services or in certain other situations.

7.3 Vendor shall notify NYC Health + Hospitals in writing if a Vendor Employee has (i) been convicted of, or was placed in a pre-trial diversion program for, any crime involving dishonesty or breach of trust including but not limited to, drug trafficking, forgery, theft, perjury, fraud, money laundering, or (ii) been convicted of any sex, weapons or violent crime including but not limited to homicide, attempted homicide, rape, child molestation, extortion, terrorism or terrorist threats, kidnapping, assault, battery, or illegal weapon possession, sale or use. Any such Vendor Employee shall not perform under this Agreement without the express written consent of NYC Health + Hospitals.

7.4 NYC Health + Hospitals may audit Vendor's records to verify compliance with this section.

7.5 Failure to comply with this section shall constitute a material breach of this Agreement and NYC Health + Hospitals shall have the right to immediately terminate this Agreement without liability for any damages resulting therefrom.

8. Payment

8.1 Vendor shall invoice NYC Health + Hospitals for all Goods or Services provided under this Agreement and NYC Health + Hospitals shall pay all undisputed invoices within thirty days of receipt of invoice. NYC Health + Hospitals shall not pay penalties or interest charges on any late payments. NYC Health + Hospitals shall not pay any amounts in advance unless otherwise expressly agreed to in writing. In the event of a dispute of invoice amount the time to pay an invoice shall be tolled until said dispute is resolved. Vendor

shall upon NYC Health + Hospitals' request, submit documentation and justification supporting the amounts charged.

8.2 NYC Health + Hospitals represents that it is exempt from the payment of sales and excise taxes and will provide Vendor documentation of such exemption upon request.

9. Intellectual Property Infringement

9.1 Vendor warrants warrant that the sale and use of Goods or Services provided shall not give rise to any claim of infringement of any third-party patent, copyright, trademark, or trade secret rights.

9.2 Notwithstanding any other section of this Agreement, Vendor shall indemnify and defend NYC Health + Hospitals and the City, their respective directors, officers, employees and agents, from and against any and all losses, liabilities, judgments, awards and costs (including legal fees and out-of-pocket expenses reasonably incurred) arising out of or related to any claim that NYC Health + Hospitals' or the City's use of the Services or Goods infringes, induces the infringement of, or violates and any third-party's intellectual property rights.

9.3 If, as a result of any such claim, NYC Health + Hospitals is enjoined from use of any Services or Goods, or if Vendor believes that NYC Health + Hospitals is likely to become the subject of such a claim, Vendor, at its option and expense shall (i) procure the right for NYC Health + Hospitals to continue to use the Services or Goods, (ii) modify the Services or Goods so that they are not infringing, while remaining functionally equivalent to the Services or Goods to have been provided, or (iii) provide a refund to NYC Health + Hospitals for the infringing Services or Goods.

10. Intellectual Property

10.1 Any intellectual property in any format developed by Vendor under this Agreement constitutes "work made for hire" under the copyright laws of the United States and shall be the property of NYC Health + Hospitals. NYC Health + Hospitals is the sole owner of the "work made for hire," and all the underlying rights to the "work made for hire," worldwide and in perpetuity. If for any reason any such intellectual property does not qualify as "work made for hire" under the copyright laws of the United States, Vendor hereby assigns all of its right, title and interest in and to such intellectual property to NYC Health + Hospitals worldwide and in perpetuity.

10.2 Any discovery or invention arising out of this Agreement shall be promptly and fully reported to NYC Health + Hospitals in writing and Vendor hereby irrevocably assigns to NYC Health + Hospitals worldwide and in perpetuity without additional consideration, any right, title or interest in any such discovery or invention immediately as of the vesting of such right, title or interest in Vendor. Vendor hereby appoints NYC Health + Hospitals as its attorney-in-fact to execute and deliver any such assignments or other documents on Vendor's behalf.

11. Use of NYC Health + Hospitals' Marks

The prior written approval of NYC Health + Hospitals is required before Vendor or any Vendor Employee may (i) use NYC Health + Hospitals or any of its facilities' names, logos, marks, seals, insignia, symbols or brands or the like in any material for publication through any media of communication, or (ii) make any statement to the press or issue any material for publication through any media of communication relating

to this Agreement. The foregoing restriction does not prohibit Vendor from using any such name in direct communications (including marketing materials that contain a list of Vendor's customers) with current or identified prospective customers (such as in a response to a solicitation or another direct communication).

12. Insurance

12.1 Vendor shall not commence performing under this Agreement unless and until all insurance required by this Agreement is in effect and satisfactory proof of such insurance (such as certificates of insurance, amendatory endorsements, additional insured endorsement where applicable, or copy of the declarations and endorsements page) has been provided to and approved by NYC Health + Hospitals. All insurance shall be primary with respect to Vendor and the additional insureds and issued by an insurer with an A.M. Best rating of A-, Class VII or better. All insurance policies must be issued by insurance companies authorized to do business in New York State. Such insurance shall waive any right of subrogation against NYC Health + Hospitals. The limits of coverage for all insurance required under this Agreement shall be the greater of (i) the minimum limits set forth herein or (ii) the limits available to Vendor under all primary, excess, and umbrella policies. NYC Health + Hospitals reserves the right to increase the minimum acceptable limits of coverage depending upon the scope of services and the potential risk exposures involved in this Agreement. Vendor's failure to maintain any of the insurance required by this Agreement shall constitute a material breach of this Agreement.

12.2 There shall be no self-insurance program or self-insured retention in excess of \$25,000 with regard to any insurance required under this Agreement unless approved in writing by NYC Health + Hospitals. Any self-insurance program shall provide NYC Health + Hospitals with all rights that would be provided by traditional insurance.

12.3 Vendor shall provide NYC Health + Hospitals with a copy of any policy required under this Agreement upon the demand for such policy by NYC Health + Hospitals.

12.4 Any subcontract shall conform to the insurance requirements set forth in this Agreement.

12.5 Vendor shall maintain occurrence based commercial general liability insurance with limits no less than \$2,000,000 per occurrence, \$4,000,000 in the aggregate. Such insurance shall name (i) "New York City Health and Hospitals Corporation, its officials, and employees" and (ii) "The City of New York, its officials and employees" as additional insureds. Such insurance shall cover claims for property damage, bodily injury, including death, products liability, and ongoing and completed operations liability. Such insurance shall state that coverage shall not be canceled except with notice to the additional insureds.

12.6 If professional services are rendered, then Medical Provider providing the professional services hereunder shall maintain its professional liability insurance with limits no less than \$1,000,000 per occurrence \$2,000,000 in the aggregate. Any policy that is claims-made shall have at least a three-year reporting period.

12.7 If Vendor uses vehicles under this Agreement, then Vendor shall maintain business automobile liability insurance with limits no less than \$2,000,000 and at least as broad as the current ISO form CA0001. Such insurance shall name (i) "New York City Health and Hospitals Corporation, its officials, and employees" and (ii) "The City of New York, its officials and employees" as additional insureds. Such

insurance shall state that coverage shall not be canceled except with notice to the additional insureds. If vehicles are transporting hazardous materials, the insurance shall be endorsed to provide pollution liability broadened coverage for covered vehicles (endorsement CA 99 48) as well as proof of MCS-90.

12.8 Vendor shall maintain statutory limits of Worker's Compensation insurance and employer's liability insurance with limits no less than the statutory requirements.

13. Entire Agreement

This Agreement contains the entire understanding of the Parties with respect to the subject matter hereof and supersedes all prior or contemporaneous oral or written communications or agreements with respect to such matters.

14. Amendments

This Agreement may not be modified or amended except in writing and signed by both Parties.

15. Assignment

15.1 Neither Party shall assign, subcontract, transfer or otherwise dispose of this Agreement or any interest herein without first obtaining the other Party's prior written consent; if a Party does so without consent of the other Party ("non-consenting Party") it shall constitute a material breach of this Agreement and the non-consenting Party shall have the right to immediately terminate this Agreement without liability for any damages resulting therefrom.

15.2 Should this Agreement be assigned, all rights, benefits and obligations shall be binding upon and inure to the benefit of the Parties, and their respective successors and permitted assigns.

16. Severability

If any section of this Agreement is held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining sections shall remain in full force and effect.

17. Waiver

The failure to enforce any right or remedy under this Agreement or at law shall not constitute a waiver of such right or remedy.

18. Execution

This Agreement may be executed in one or more counterparts, each of which when executed shall be deemed to be an original, and when taken together shall constitute one and the same agreement. Electronic, facsimile or PDF image signatures shall be treated as original signatures.

19. Delay

19.1 The time of delivery of Goods or performance of Services may be extended in the following ways and with the following consequences:

19.1.1 If delivery or performance by Vendor is delayed by an act or omission of NYC Health + Hospitals, Vendor shall be allowed a corresponding extension of time for performance.

19.1.2 If delivery or performance by Vendor is delayed by a force majeure event such as war, civil insurrection, strikes, weather, etc., Vendor shall promptly give notice to NYC Health + Hospitals of the circumstances and the anticipated delay duration, and Vendor shall be allowed a corresponding extension of time.

19.1.3 Should a delay necessitate NYC Health + Hospitals to purchase Goods or Services from a third-party, NYC Health + Hospitals may do so without liability to Vendor and NYC Health + Hospitals shall be relieved of the obligation to purchase such Goods or Services from Vendor.

20. Confidentiality

Each Party has materials and information that have been or might be made available to the other in connection with this Agreement and may consist of confidential and proprietary information ("Confidential Information") of the other Party. Confidential Information shall include any information relating to the Services, identity of customers or patients, business practices, trade secrets, business opportunities, pricing terms, and financial information. Only those employees or consultants requiring the use of Confidential Information in the performance of this Agreement shall receive such Confidential Information and only if such employees or consultants are bound by a confidentiality agreement as protective as this section. Neither Party shall be liable to the other with regard to any Confidential Information that: (i) was publicly known at the time it was disclosed, (ii) was legally known to the receiving party at the time of disclosure, (iii) was disclosed pursuant to law or court order, or (iv) was disclosed with the prior written approval of the disclosing party. This section shall survive the termination or expiration of this Agreement.

Article III. Terms and Conditions Specific to Goods

The following shall apply if Vendor provides Goods under this Agreement.

Reserved

Article IV. Terms and Conditions Specific to Services

The following shall apply if Vendor provides Services under this Agreement.

1. Warranty for Services

Vendor warrants that the Services will be performed (i) in a diligent, professional and workmanlike manner in accordance with the highest applicable industry standards, (ii) in accordance with the requirements under this Agreement, and (iii) by experienced, qualified and properly trained and appropriately licensed personnel. If Vendor fails to meet the specifications as set forth herein, Vendor will, without additional compensation, promptly correct or revise any errors or deficiencies in the Services provided.

Article V. Information Security

1. Change in Ownership

Vendor shall notify NYC Health + Hospitals of any changes in its ownership or any significant change to its information security environment that will negatively impact its effectiveness or ability to comply with the provisions of this Agreement.

2. IT Security Point Person

Vendor shall identify a person responsible for information security and related governance matters.

Name: John Dionisio
Title: Chief Information Officer
Email: jdionisio@somoscommunitycare.org
Phone: 646-931-5708

3. Security Questionnaire

Vendor shall complete the NYC Health + Hospitals Vendor Information Security Risk Assessment Questionnaire and provide relevant documentation as requested to substantiate responses to the questionnaire.

4. Compliance with law

Vendor shall, upon request of NYC Health + Hospitals, demonstrate its ability to comply with all applicable laws and regulations that apply to this Agreement by making audit reports available (e.g. HIPAA, SSAE 16, etc.), including any required security accreditations.

5. Compliance with Security Standards

Vendor shall, upon request of NYC Health + Hospitals, provide evidence of on-going compliance with industry standard security controls related to:

5.1 Access Control, including identity and access management policies, practices, and technologies that support and ensure authorization, secure authentication, role-based access, auditable access, and timely access termination, as well as Vendor policies and procedures related to access control and identity management. For the solution delivered to the System, Vendor will additionally ensure standard federation or integration protocols are used for Active Directory (AD) authentication.

5.2 Asset management, including Vendor's policies and procedures for "bring your own device" and personal device management procedures, and for data inventory, data flow, data classification, data labeling, and data handling (including disposal).

5.3 Business continuity and disaster recovery, including Vendor's policies and procedures regarding data availability, data backup, data recovery, data retention and disaster recovery service levels, physical and environmental security to ensure that data center utilities are in optimal condition, secure, safeguarded against risks, monitored, maintained, redundant, and regularly tested.

The policies and procedures shall ensure that the Vendor:

5.3.1 operates a mirror system at a hardened data center facility in the United States that is geographically remote from the primary system on which the subscription services are hosted (the "Secondary Backup Facility").

5.3.2 conducts periodic backup of NYC Health + Hospitals data and stores such backup data in the Secondary Backup Facility.

5.4 Data protection, including Vendor's policies and procedures that ensure that:

5.4.1 applications and programming applications and interfaces are designed, developed, deployed, and tested in accordance with leading industry standards and adhere to applicable legal, statutory, or regulatory compliance obligations;

5.4.2 data input and output integrity routines (i.e., reconciliation and edit checks) have been implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse, including encryption, penetration testing, vulnerability management, malicious code execution and data management solutions employed to ensure controlled access to data, to secure data while at rest, in transit and in use;

5.4.3 baseline security configurations are implemented along with documentation that demonstrates annual testing of same;

5.4.4 physical and logical architecture and configuration safeguards against unauthorized access of, intentional, or unintentional alteration of information technology resources; and

5.4.5 data can be provided in a structured and unstructured format in accordance with industry standards.

5.5 Incident management, including Vendor's policies and procedures for incident management, including evidence of forensic procedures that support the ability to provide evidence to support discovery of potential legal action after a security incident.

5.6 Information security management, including documentation that demonstrates Vendor's implementation of an information security management program and a control framework that is reviewed at least annually.

5.7 Vendor's risk management and compliance policies and procedures, including audit plans, effectiveness of implemented security operations, and supported via independent audits that are performed at least annually.

5.8 Vendor's service delivery program, including information technology governance and service management model that meet industry standards, as well as change control and configuration management policies and procedures that meet industry standards.

5.9 Vendor's personnel security controls, including acceptable use policy, personnel screening and separation practices, sanction policy for Vendor Employees who have violated security policies and procedures, and a personnel security awareness training program.

6. Risk Assessment

6.1 Vendor shall permit NYC Health + Hospitals to perform, no more than once annually and upon reasonable notice, and at its own cost, a risk assessment of Vendor's information technology infrastructure and information security controls and processes and to perform relevant tests to ensure compliance with applicable regulations.

6.2 Vendor shall participate in NYC Health + Hospitals' risk assessment activities and shall be required to mitigate any identified significant risks.

6.3 Vendor shall provide evidence of an independent, third-party information technology security assessment or audit upon request by NYC Health + Hospitals.

7. Training

Vendor shall complete required training as deemed necessary by NYC Health + Hospitals, which may include HIPAA Privacy & Security Training, Information Security Awareness Training, training related to the use of specific information systems the vendor has access to, and facility specific life safety.

8. Incident Reporting

Vendor shall immediately report suspected or confirmed information security incidents to the NYC Health + Hospitals' vendor management liaison.

9. Insurance

Vendor shall maintain cyber liability insurance with limits no less than \$1,000,000 per claim. Such insurance shall name (i) "New York City Health and Hospitals Corporation, its officials, and employees" and (ii) "The City of New York, its officials and employees" as additional insureds.

IN WITNESS WHEREOF, the Parties have agreed to the foregoing, intending to be legally bound hereby.

**New York City Health and Hospitals
Corporation**

By: 

Paul A. Albertson

Vice President

Somos Healthcare Providers Inc.

By: 

Name: Mario J. Paredes

Title: Chief Executive Officer

Attachment B

**Information Security Requirements
For Contractors**

**Office of Information Security
Division of Instructional and Information Technology
NYC Department of Education**

CLASSIFICATION: PUBLIC.

This document may be distributed without restriction.

1. Information Security Policies

- A. Contractor must have, and upon request by the DOE shall promptly provide the DOE with copies of its, information security policies that cover the following elements:
1. Data classification and privacy
 2. Security training and awareness
 3. Systems administration, patching and configuration
 4. Application development and code review
 5. Incident response
 6. Workstation management, mobile devices and antivirus
 7. Backups, disaster recovery and business continuity
 8. Regular audits and testing
 9. Requirements for third-party business partners and contractors
 10. Compliance with information security or privacy laws, rules, regulations or standards
 11. Any other information security policies
- B. Policy Requirements: In addition to addressing the elements set forth above:
1. Contractor must indicate in their policies the date of the most recent revision.
 2. Contractor must include a certification from its Chief Operating Officer, or individual with an equivalent title with authority to represent the Contractor, asserting that all of the above elements are addressed in the Contractor's security policies, and that such policies are at least as rigorous as the policies set forth in this document and the NYC Citywide Information Security Policies issued by the NYC Cyber Command, in cooperation with DoITT (Cyber Policies). If Contractor cannot make such certification for any reason (e.g. Contractor's policies do not address an element listed above), Contractor must notify the DOE of the deficiency and explain how Contractor will remedy such deficiency.
 3. Contractor shall comply with such policies and, unless the Contractor receives the DOE's prior written approval, Contractor shall not make any changes to such policies that would result in (i) not addressing one or more elements set forth above or (ii) not being as rigorous as the policies set forth in this document or the NYC Cyber Policies.

2. Privacy & Confidentiality

In accordance with the Agreement, Contractor must hold Protected Information in strict confidence and not disclose it to any third parties nor make use of such data for its own benefit or for the benefit of another, or for any use other than the permitted purpose agreed.

- A. The Contractor shall use commercially reasonable efforts to secure and defend any system housing Protected Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System.
- B. The Contractor shall protect and secure all Protected Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer.
- C. The Contractor shall maintain all copies or reproductions of Protected Information with the same security it maintains the originals. At the point in which the Protected Information is no longer necessary for its primary or retention purposes, as authorized by DOE, Contractor must destroy such data, making it unusable and unrecoverable. If Contractor determines at such point that destruction of the Protected Information is infeasible, Contractor will provide DOE with a reasonable explanation and will cease any access or use of the Protected Information.
- D. For all Application screens, front pages of any reports and landing pages of web Applications that contain Protected Information, Contractor must include prominent confidentiality notices in legible-sized font on each page (e.g. a prominent notice that the information on such screen or report is confidential on the

bottom of a web screen or the footer of a report page).

- E. All web Application screens that contain Protected Information must be non-cacheable.
- F. Protected Information should not appear in URLs.
- G. Contractor's development, test and QA environments shall not use actual Protected Information unless additional safeguards are put into place to protect the confidentiality of the information.
- H. Contractor must comply with any additional requirements set forth in its data use agreement, non-disclosure agreement, or any similar contract or agreement with the DOE that is related to the subject matter to which these requirements apply

3. Application Development

- A. Where applicable, Contractor shall have a comprehensive secure development lifecycle System in place consistent with industry standard best practices, including policies, training, audits, testing, emergency updates, proactive management, and regular updates to the secure development lifecycle System itself.
- B. Where applicable, Contractor must review and test all application code for security weaknesses and backdoors prior to deployment with DOE. All high-risk findings and exploitable vulnerabilities must be resolved before the Application is released. A development manager of Contractor must certify in writing to the DOE that a security review has been conducted and that all risks are acceptable before every release. For further information, please refer [National Institute of Standards and Technology \("NIST"\) Special Publication 800-64 Revision 2](#).
- C. Contractors that handle Protected Information must respond to and resolve security-related reports, inquiries and incidents in a timely and professional manner. The Contractor must notify the DOE within 24 hours of when Contractor becomes aware of any such incident or suspected incident that poses a potential risk to the Protected Information. The Contractor shall send the notification to studentprivacy@schools.nyc.gov.

4. Authentication & Identity Management

- A. If an application requires Single Sign-On (SSO) integration with the DOE, the Contractor must support authentication for DOE Users as specified in the DIIT SAML Integration Guidelines
 1. Contractor will not have the ability to make any changes to the DOE Identity Management Systems.
 2. If new DOE Users need to be enrolled or registered in order to use a Contractor's System, The NYCDOE Office of Information Security must receive and agree upon the plan for the registration process and ownership of identity management in writing.
 3. Follow DIIT OpenId and SAML Integration guidelines if application requires Single Sign-on.
- B. If the Contractor maintains its own identity management system for its users, it must:
 1. Enforce a one user, one account policy in which shared/ group accounts and duplicate accounts are not permitted
 2. Be free of testing, development and non-production accounts.
 3. Maintain accurate legal name, address, phone number information for all users who are permitted to access Protected Information, and upon request from the DOE, produce lists of users who will have access to Protected Information.
 4. Enforce a strong password policy of eight characters minimum, with mixed case and at least one number or special character.
 5. Store all passwords in non-reversible one-way cryptographic hash.
 6. Log all successful and failed authentication attempts, including date, time, IP address, and username.
 7. Offer a secure password reset feature, including verification of identity, email or text notification and a one-time-use password link that expires after 24 hours.
 8. Automatically de-provision accounts for terminated employees of Contractor and DOE.
 9. Temporarily lock accounts with repeated failed login attempts and provide support to affected users.
 10. Keep attributes and group structures that support authorization accurate.
 11. Don't hardcode credentials

12. Use a password Reset Tool whenever possible
13. Implement account lockout against brute-force attacks
14. Don't disclose too much information in error messages
15. Store database credentials securely
16. Encrypt credentials in transit
17. Password must expire in 90 days
18. Applications that use non-standard authentication solutions require approval from Office of Information Security

5. Protected Information Authorization

- A. Applications that handle Protected Information must have explicitly defined authorization controls that prevent users from exceeding their authorized privileges.
- B. Any applications must perform authorization checks before performing any action that creates, views, updates, provides access to, transmits or deletes Protected Information. Authorization logic must be highly configurable and alterable without code changes.
- C. Authorization checks must verify the user is authorized to perform the requested action, including the scope of the action. Scope authorization checks should reference DOE location codes, student-teacher-class linkage, parent-student linkage and other data sources.
- D. Any non-DOE accounts that are managed locally by the Contractor must follow the principal of "Least Privileged Access" whereby those user accounts are provided the most restrictive access necessary to perform the required business function. "Super users" (i.e. application administrators) must be avoided unless absolutely necessary due to a legitimate administrative or educational need for such access in order to provide the Services.

6. Incident Response

- A. Contractor must have a plan for compliance with all applicable breach notification laws, including but not limited to New York State Education Law § 2-d and the New York State Data Breach Notification Act (General Business Law §899-aa and New York State Technology Law § 208, as appropriate).
- B. The DOE must be notified in writing within 24 hours of the earliest indication or report of a potential breach or unintended disclosure of Protected Information or a system that supports it.
- C. Response actions to incidents that might affect Protected Information or systems must be conducted quickly and with ample resources. Contractor will hire a professional third-party incident response team if in-house resources do not have sufficient skill or availability.
- D. DOE shall have the right to view all incident response evidence, reports, communications and related materials upon request.
- E. If requested by the DOE, or if required by law, the Contractor shall notify in writing all persons affected by the incident, at its own cost and expense, or shall compensate the DOE for the cost and expense of notifications it makes.
- F. Contractor's IT security program includes a security incident response policy and procedure. The incident response procedure defines incident types, risk levels, step by step procedure for responding to each event type, contact personnel, management, internal and external communication procedures, local law enforcement agency information, etc.

7. Audit & Inspection

- A. The Contractor shall allow DOE, upon reasonable notice, to perform security assessments or audits of Systems that handle or support Protected Information related to the subject matter to which these requirements apply. Such an assessment shall be conducted by an independent 3rd party agreed upon by

the Contractor and the DOE, and at the DOE's own expense, *provided* that the Contractor cooperate with any such assessment/audit and shall, at its own expense, provide all necessary support, personnel and information needed to ensure the successful completion of the assessments or audits.

- B. The Contractor shall provide DOE, upon DOE's request, with a SSAE 16 or similar report as agreed to by DOE for critical business processes relating to protection of Protected Information and safeguards implemented in its organization.
- C. Contractor must engage an independent third party annually to assess the practical security of Contractor's Systems. These reviews must include penetration tests from the perspective of an external attacker and an internal user with common privileges. The penetration tests must include all Systems exposed to the internet and any Systems, internal or external, that Handle Protected Information. Such annual assessment shall be at Contractor's sole expense.
- D. Any Contractor housing Protected Information must have for the duration of the contract an independent third-party Contractor specializing in continuous monitoring and reporting on Information Security events. The reports and or electronic access must be made available to DOE Information Security personnel at any time.
- E. Audit logs must be implemented for all systems that handle Protected Information. All attempted violations of system security must generate an audit log. Audit logs must be secured against unauthorized access or modification.
- F. In the event of adverse findings through a DOE or Contractor audit, the Contractor shall cooperate with the DOE in remediating any risks to Protected Information, including complying with request to temporarily taking the system offline or otherwise limiting access to the system, and any other follow up actions reasonably necessary to secure the Protected Information.

8. Availability

- A. Contractor Systems that handle Protected Information shall be available and fully functional 24x7x365 with 99.9% uptime, unless otherwise agreed upon in writing with the DOE. Contractor shall make plans for colocation, backups and any other systems necessary to ensure continuity.
- B. Contractor must notify and obtain agreement from the DOE for any planned interruptions in service related to the agreement to which these requirements apply, with the exception of emergency security updates. Contractor must notify the DOE immediately of any unintended service interruption.

9. Encryption

- A. All systems that handle Protected Information must encrypt the DOE data that include Protected Information in transit in a manner consistent with the most recent NIST guidelines.
- B. For HTTP and other protocols that use SSL/TLS, Contractor shall use the TLS 1.2 or later protocol with 128-bit or larger key size, and shall make previous protocols and smaller keys unavailable.
- C. Contractor shall utilize a third party provider that is a recognized and trusted authority in the industry to generate any certificates that are used for authentication between two parties (e.g., Contractor and the DOE or Contractor and any other party).
- D. Web Applications that contain Protected Information must be available only over Transport Layer Security ("TLS"). Attempts to use the Application without encryption shall be rejected. Encrypted and non-encrypted content shall not be mixed.
- E. Data at rest that is stored outside of hardened Application or database production Systems must be protected by encryption consistent with NIST recommendations.
- F. The Contractor shall keep private keys confidential, implement key lifecycle management and protect all keys in storage or in transit.

- G. The Contractor shall choose keys randomly from the entire key space and ensure that encryption keys allow for retrieval for administrative or forensic use.
- H. Encryption of the DOE data in production databases is *not* required. Any database encryption system must be approved by the DOE, which approval shall not be unreasonably withheld. The DOE must be provided with a complete set of decryption keys. All DOE data must be recoverable.
- I. Contractor will not store DOE data outside of the United States. In the event that Contractor will store DOE data outside of the United States at a later date, Contractor shall notify the DOE of the locations outside the U.S. by providing notice either in its contract or proposal to a RFP/RFB if known by Contractor prior to award, or if known after award, to studentprivacy@schools.nyc.gov; *provided* that the DOE reserves the right to require that the use, storage, or handling of DOE data occur within the contiguous United States or similar regional boundary as defined by the DOE, which, if applicable, shall be specified in the contract or RFP/RFB.
- J. Disable HTTP access for all SSL enabled resources
- K. Use the Strict-Transport-Security header
- L. Store user passwords using a strong, iterative, salted hash
- M. Securely exchange encryption keys
- N. Setup a secure key management processes
- O. Disable weak SSL ciphers on servers
- P. Use valid SSL certificates from a reputable CA
- Q. Disable data caching using cache control headers and autocomplete
- R. Limit the use and storage of sensitive data.

10. Data retention/destruction

- A. Contractor may be required to support retention of Protected Information as per [NYSED Education Data Retention Schedule ED-1](#).
- B. If applicable, retention requirements for DOE data may be specified in a contract or RFP/RFB. If applicable, the Contractor must acknowledge in its proposal to a RFP/RFB that it can meet the requirements and, upon request by the DOE, demonstrate that retention requirements are implemented.
- C. Record retention systems must comply with all security and privacy controls set forth in this document.
- D. Whenever required by the BOE, and upon termination of this agreement, and except as noted below, the Contractor will promptly (a) with respect to physical copies of Protected Information, surrender, or if surrender is not practicable, securely delete or otherwise destroy Protected Information and (b) with respect to digital and electronic Protected Information, securely delete or otherwise destroy Protected Information remaining in the possession of the Contractor. This will include all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data. The Contractor will ensure that no copy, summary, or extract of Protected Information is retained on any storage medium whatsoever by Contractor, except as noted below. Contractor will accomplish all measures related to the extraction, transmission, deletion, or destruction of Protected Information utilizing an approved, appropriate and secure method of destruction. This may include shredding, burning or certified/witnessed destruction of physical materials and verified erasure of electronic media. To the extent that the Contractor continues to be in possession of de-identified data, it will not attempt to re-identify de-identified data and not to transfer de-identified data to any party for re-identification. The Contractor will not retain any de-identified biometric records. The Contractor will certify, in writing, that all of the foregoing materials have been surrendered or destroyed (as applicable), except as noted below.
- E. The provisions noted in section D above will not apply to Protected Information which the Contractor is required to retain under applicable federal or state law and regulation as well as laboratory accreditation and certification requirements. However, the Contractor will continue to abide by the confidentiality and data security terms of its agreement with the DOE while it retains Protected Information, or causes it to be retained.

11. System Configuration & Maintenance

- A. All operating systems, servers, and network devices that support DOE systems or Protected Information must be kept hardened and patched.
- B. All Contractor systems that are used to host, transfer, or otherwise interact with Protected Information must enforce strict separation from any non-DOE systems. This may be achieved through physical and/or logical separation. The separation must be auditable and able to be proven at the request of the DOE.
- C. Contractor must maintain technical best security practices configuration guidelines for all such systems and update them at least twice per year.
- D. All security-related patches must be installed on systems within a reasonable timeframe. Contractor will maintain a testing lab in order to support this.
- E. Establish a rigorous change management process
- F. Define security requirements
- G. Conduct a design review
- H. Perform code reviews
- I. Perform security testing
- J. Harden the infrastructure
- K. Define an incident handling plan
- L. Keep browser updated with latest version.

12. Subcontractors

- A. Contractor has represented that it will not utilize sub-contractors to perform testing, but may use a third party to assist with Help Desk customer service. However, should it do so, in addition to the subcontracting provisions in the agreement with the DOE (which require DOE approval of all subcontractors), in the event that a Contractor utilizes subcontractors to support a system that handles Protected Information (each a “subcontractor”), such subcontractors shall be subject to, and Contractor must require that each subcontractor comply with, the requirements set forth herein.

13. New York City Parents’ Bill of Rights for Data Privacy and Security (“PBOR”)

- A. Contractor shall comply with the requirements of the PBOR in every respect. As detailed in its agreement with the DOE, it will not sell Protected Information or release it for any commercial purposes. It will facilitate the parents’ right to inspect and review their children’s Protected Information in the custody of the Contractor. As detailed in the previous sections of this document, it shall maintain safeguards to protect Protected Information when it is stored or transferred, and represents that these safeguards meet industry standards and best practices. Contractor shall respond appropriately to complaints parents make about possible breaches of Protected Information. It has agreed to the DOE’s full PBOR as part of this agreement and provided the supplemental information required of it for public posting on the DOE’s website, pursuant to New York Education Law 2-d.

14. Training

Employees go through a background check as well as drug screening prior to employment. New hires go through an orientation program where employees are educated on federal and state laws governing confidentiality and security of healthcare data. On an ongoing basis, compliance and security awareness events are conducted for employee education and awareness.

Attachment C: BOE Parents' Bill of Rights for Data Privacy and Security

Both state and federal laws protect the confidentiality of information about your child that identifies him or her. Such information, which includes student-specific data, is known as “personally identifiable information.” Under New York state’s education law, if you are a parent of a child in the New York City public school district (the NYC DOE), you have the following rights regarding the privacy and security of your child’s personally identifiable information and data.

(1) Your child’s personally identifiable information cannot be sold or released for any commercial purposes.

(2) If your child is under age 18, you have the right to inspect and review the complete contents of your child’s education records.

(3) Safeguards must be in place to protect your child’s personally identifiable data when it is stored or transferred. These safeguards must meet industry standards and best practices. Examples of such safeguards include encryption, firewalls and password protection.

(4) You have the right to make complaints about possible breaches of student data and to have such complaints addressed. Complaints to the SED 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. Complaints to the NYC DOE should be directed via email to data-security@schools.nyc.gov, or in writing to the Office of the Chief Information Officer, the Division of Instructional and Information Technology, New York City Department of Education, 335 Adams Street, Brooklyn NY 11201.

(5) You have additional rights as a parent, including additional privacy rights under federal law. They are found in the NYC DOE’s Parents’ Bill of Rights and Responsibilities, available here: <https://www.schools.nyc.gov/school-life/policies-for-all/parents-bill-of-rights>

(6) You can find a complete list of all of the types of student data that the New York State Education Department (SED) collects at this web-link: <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>

You may also 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.

Attachment C: BOE Parents' Bill of Rights for Data Privacy and Security: Supplemental Information

Entity Name: **Somos Healthcare Inc. D/B/A Somos Community Care**

New York Education Law §2-d requires the New York City Department of Education (NYC DOE) to supplement its Parents' Bill of Rights for Data Privacy and Security with additional information concerning agreements under which personally identifiable student information (Protected Information) is disclosed. In accordance with these provisions, it is necessary for you to provide the following. If an item is not applicable to your agreement, please explain why.

(1) The exclusive purposes for which Protected Information will be used, and how students and staff members will benefit from the Vendor's services:

Protected Information will be used by Vendor, as such is defined within the Agreement, for the sole purpose of performing COVID-19 testing under its contractual agreement with New York City Health and Hospitals Corporation.

(2) How you will ensure that the Vendor or other authorized persons or entities that you will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements required by your written agreement with the NYC DOE:

Vendor will provide the Services as detailed within the Specimen Collection Agreement and will only report COVID-19 test results to parents or guardians of the Tested Students, Tested Students over 18 years of age and Tested Staff, as required or permitted by law and will further ensure that all personnel involved in the specimen collection and reporting comply with all confidentiality and privacy obligations equivalent to and no less protective than those found within this Agreement.

(3) When the written agreement with the NYC DOE starts and ends and what happens to Protected Information upon expiration of the agreement:

This Agreement is effective October 1, 2020 and will continue for so long as the Contractor will be providing the NYC DOE services with respect to COVID-19 testing. Somos abides by NIST 800-53 controls to as well as applicable New York state laws and regulations to safeguard Protected Information. BioReference Laboratories ("BRL") under its Agreement with H+H will be required to retain test orders and requisitions, consents to testing, and test results. This Protected Information will be retained in the same secure manner as BRL retains information for the approximately 60,000-70,000 tests that it performs daily. Vendor shall retain any PHI it receives from BRL in accordance with all law and regulation.

(4) 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:

Pursuant to its contractual obligations, Vendor will work collectively with the NYC DOE in processing requests for copies of student Protected Information, and challenges to the accuracy of student data in the custody of the Vendor. Any received requests will be directed to studentprivacy@schools.nyc.gov. However, if a parent of a student who was tested wishes to obtain a copy of their child's laboratory testing records, the request should be directed to BRL through its portal at patientportal@bioreference.com.

(5) Whether the Protected Information will be stored in the US or outside of the US (and if outside of the US, where), and the security protections taken to ensure such data will be protected (described in such a manner as to protect data security):

The Protected Information is stored in the US. Please see question #3 above.

(6) How the data will be encrypted (described in such a manner as to protect data security):

Vendor employs industry standard encryption method and strength for data at rest and in transit.

Attachment D: Certificate of Records Disposal

CERTIFICATE OF RECORDS DISPOSAL			
<input type="checkbox"/> The information described below was destroyed in the normal course of business pursuant to organizational retention schedule destruction policies and procedures, and/or written agreement.			
Description of Information Disposed Of/Destroyed:			
<input type="checkbox"/> Noted in Attachment			
PERSON PERFORMING SANITIZATION			
Name:		Title:	
Organization:	Location:	Phone:	
MEDIA INFORMATION			
Make/Vendor:		Model Number:	
Serial Number(s)/Property Numbers:			
Media Type:		Source (i.e., user name/property #):	
Data Classification:	Data Backed up?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> Unknown
Backup Location (if applicable):			
SANITIZATION DETAILS			
Method Type:	<input type="checkbox"/> Clear	<input type="checkbox"/> Purge	<input type="checkbox"/> Damage <input type="checkbox"/> Destruct <input type="checkbox"/> Other:
Method Used:	<input type="checkbox"/> Degauss	<input type="checkbox"/> Overwrite	<input type="checkbox"/> Block Erase <input type="checkbox"/> Crypto Erase <input type="checkbox"/> Other:
Method Details:			
Tool Used (include version):			
Verification Method:	<input type="checkbox"/> Full	<input type="checkbox"/> Quick Sampling	<input type="checkbox"/> Other:
Post-Sanitization Classification:			
Notes:			
MEDIA DESTINATION			
<input type="checkbox"/> Internal Reuse	<input type="checkbox"/> External Reuse	<input type="checkbox"/> Recycling Facility	<input type="checkbox"/> Manufacturer <input type="checkbox"/> Other (specify in Details)
Details:			
SIGNATURE			
<input type="checkbox"/> I attest that the information provided on this Certification of Destruction and Sanitization is accurate to the best of my knowledge.			
Signature:		Date:	
VALIDATION			
Name:		Title:	
Organization:	Location:	Phone:	
Signature:		Date:	