Terms and Conditions Relating to Protected Health Information ("City PHI Terms")

Revised and Effective as of January 4, 2023

(a) Definitions. Capitalized terms used but not defined in these City PHI Terms have the same meaning as those terms are given in the HIPAA Rules (as defined below). For purposes of these City PHI Terms and notwithstanding anything in the Contract to the contrary, the terms enumerated in this Section (a) are defined as follows:

(1) Applicable Law. "Applicable Law" means all applicable present and future federal, state, or local laws, ordinances, executive orders, rules, regulations and all court orders, injunctions, decrees and other official interpretations thereof of any federal, state, or local court, administrative agency or governmental body, including the City, the Commonwealth of Pennsylvania, and the United States of America. Applicable Law includes, without limitation, all specific laws and regulations referred to in these City PHI Terms. Any reference to a statute or regulation in these City PHI Terms shall refer to the statute or regulation referenced, as may be amended or superseded from time to time.

(2) Breach. "Breach" means a "breach" as defined in 45 CFR §164.402 that involves City PHI.

(3) City PHI. "City PHI" means Individually Identifiable Health Information of the City that is received, accessed, created, maintained, retained, modified, or transmitted by Provider (or its agents or Subcontractors) in the course of providing the Services. City PHI excludes information regarding a person who has been deceased for more than 50 years, in education records covered by FERPA (20 U.S.C. 1232g), in student records described at 20 U.S.C. 1232g(a)(4)(B)(iv), or in employment records held by the City in its role as employer.

(4) City PHI Terms. "City PHI Terms" means these Terms and Conditions Relating to Protected Health Information.

(5) Contract. "Contract" means a professional services contract, purchase order, procurement contract from a competitive bid process, or any other agreement of the parties including any and all documents and exhibits incorporated therein by reference or attached thereto and any and all amendments or changes thereto in accordance with the Contract.

(6) Covered Unit. "Covered Unit" means a health care component designated by the City in accordance with 45 CFR §164.105(a)(2)(iii)(D). A current list of the City's Covered Units is posted at www.phila.gov/privacypolicy.

(7) Designated Record Set. As defined in 45 CFR §164.501.

(8) Discovery of an Incident. Consistent with 45 CFR §164.410 (a)(2), "Discovery of an Incident" means that Provider or an employee, officer, or other agent of Provider knows of an Incident or by the exercise of reasonable diligence should have known of an Incident.

(9) Electronic Protected Health Information. "Electronic Protected Health Information" or "EPHI" means City PHI that is transmitted or maintained in Electronic Media.

(10) HHS. “HHS” means the U. S. Department of Health and Human Services.

(11) HIPAA. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH”), and all applicable implementing regulations as amended from time to time.

(12) HIPAA Rules. “HIPAA Rules” means the Privacy, Security, Breach Notification, and Enforcement Rules set forth in 45 CFR Part 160 and Part 164.

(13) Incident. “Incident” means (a) any successful Security Incident involving City PHI; (b) any use or disclosure of City PHI not authorized by these City PHI Terms; or (c) any acquisition, access, use, or disclosure of City PHI in a manner not permitted by the Privacy Rule.

(14) Individual. “Individual” means the person who is the subject of City PHI or a person who is qualified to act as a personal representative of such subject in accordance with 45 CFR §164.502(g).

(15) Other Privacy Laws. "Other Privacy Laws” means The Pennsylvania Mental Health Procedures Act (50 P.S. §7111 et seq.), Pennsylvania Mental Health Treatment Regulations (55 Pa. Code §5100.31 et seq.), Pennsylvania Confidentiality of HIV-Related Information Act (35 P.S. §7601 et seq.), federal substance abuse treatment confidentiality law and regulations codified as 42 USC 290dd-2 and 42 CFR Part 2, Pennsylvania Drug and Alcohol Abuse Control Act and related regulations (71 P.S. §1690.101 et seq. and 4 Pa. Code §255.5), Pennsylvania Breach of Personal Information Notification Act (73 P. S. §2301 et seq.), Identity Theft Prevention Rules under 16 CFR §681.1, and any other Pennsylvania and federal laws that protect the privacy, confidentiality, integrity, and security of individually identifiable health information.

(16) Person. “Person” means any individual, sole proprietorship, associate, company, firm partnership, limited partnership, joint venture, corporation, limited liability company, or other form of entity or association recognized by law.

(17) Privacy Rule. "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information set forth in 45 CFR Parts 160 and 164 (Subparts A and E).

(18) Provider. “Provider” means the Person providing Services to the City.

(19) Security Incident. As defined in 45 CFR §164.304.

(20) Security Rule. “Security Rule” means the Security Standards for the Protection of Electronic Protected Health Information set forth in 45 CFR Parts 160 and 164 (Subparts A and C).

(21) Services. “Services” means the functions to be performed and services to be provided by Provider as specified in the Contract.

(22) Subcontractor. Notwithstanding anything to the contrary in the Contract, the term “Subcontractor” when used in these City PHI Terms means a Person who under a contract or other arrangement with Provider performs or assists in the performance of some part of the Services.

(23) Unsecured City PHI. "Unsecured City PHI" means City PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of HHS in the guidance issued under section 13402(h)(2) of Public Law 111-5 (available on the HHS website).

(24) Unsuccessful Security Incident. "Unsuccessful Security Incident" means a Security Incident that does not result in unauthorized access, use, disclosure, modification, or destruction of City PHI (including, for example, pings on Provider's firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks that do not result in the system being taken off-line, or malware such as worms or viruses).

(b) Permitted Uses and Disclosures by Provider.

(1) Uses and Disclosures Authorized by the Contract. The City authorizes Provider to create, use, receive, and disclose the minimum City PHI necessary to perform the Services. Provider may not use, disclose, or request City PHI in a manner that would violate the Privacy Rule, or Other Privacy Laws if done by the City, except for the specific uses set forth in Sections (b)(2) and (b)(3) below.

(2) De-Identified Information, Limited Data Sets, and Data Aggregation Services. Provider shall only use City PHI to create de-identified information in accordance with the specifications in 45 CFR §164.514(b) to perform services for the City or as otherwise permitted in writing by the City. As requested by and subject to such limitations as may be imposed by the City in writing from time to time, Provider may use City PHI to create a limited data set that meets the specifications in 45 CFR §164.514(e)(2), or to provide data aggregation services as permitted in 45 CFR §164.504(e)(2)(i)(B).

(3) Internal Uses by Provider. Provider may use City PHI to the extent necessary for its proper management and administration or to carry out its legal responsibilities, provided that such uses are permitted by Applicable Law. For clarity, Provider's proper management and administration does not include any Research or Marketing activities.

(4) Required by Law. Provider may use or disclose City PHI as Required by Law.

(5) Minimum Necessary. Provider shall use, disclose, or request only the minimum City PHI necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with 45 CFR §164.502(b).

(c) Obligations and Activities of Provider.

(1) Limitation on Use and Disclosure. Provider shall not access, use, disclose, or maintain City PHI other than as expressly authorized or required by these City PHI Terms or as Required By Law.

(2) Safeguards. Provider shall use appropriate safeguards, and shall comply with the Security Rule with respect to EPHI, to prevent the use or disclosure of City PHI other than as

permitted in these City PHI Terms. Provider shall: (i) maintain written policies, procedures, and documentation evidencing its compliance with the Security Rule; (ii) review its security measures on an annual basis and modify its security measures as needed to continue providing reasonable and appropriate protection of City PHI; and (iii) cooperate in good faith in response to City's request to discuss, review, inspect, or audit Provider's safeguards.

(3) Compliance with Privacy Rule. To the extent Provider is to carry out one or more of the City's obligations under the Privacy Rule, Provider shall comply with the requirements of the Privacy Rule that apply to the City in the performance of such obligation(s).

(4) Subcontractors. Provider shall ensure that any Subcontractors that access, create, receive, maintain, or transmit City PHI, in any format, on behalf of Provider: (i) agree to the same restrictions, conditions, and requirements that apply to Provider with respect to such information; (ii) enter into a business associate agreement or other written agreement that complies with 45 CFR §164.504(e) and 45 CFR §164.314(a); and (iii) implement reasonable and appropriate safeguards to protect City PHI.

(5) No Off-Shore Activities. Provider shall not disclose, transmit, or permit access to City PHI in any form or medium to any third party beyond the boundaries and jurisdiction of the United States (e.g. "Offshoring") without express written authorization from the City HIPAA Privacy Officer.

(6) Requests by Individuals.

(i) Restrictions on Use or Disclosure. Upon written notice from City that it has agreed to any restrictions requested by an Individual pursuant to 45 CFR §164.522, Provider shall comply with such restrictions to the extent they affect Provider's use or disclosure of City PHI.

(ii) Access to Records. To the extent Provider maintains City PHI that the City has determined to be part of its Designated Record Set, Provider shall, within five (5) business days of written request from the City, make available such City PHI in the form and format specified by the City as necessary for City to satisfy its obligations under 45 CFR §164.524 and other Applicable Law.

(iii) Amendment of Records. To the extent Provider maintains City PHI that the City has determined to be part of its Designated Record Set, Provider shall, within five (5) business days of written request from the City, make any amendments to City PHI as directed or agreed to by the City pursuant to 45 CFR §164.526, or take other measures as necessary for City to satisfy its obligations under 45 CFR §164.526.

(iv) Accounting of Disclosures. Provider shall identify and document, and require any agents and Subcontractors to identify and document, all disclosures of City PHI that are subject to the Individual's right to receive an accounting as set forth in 45 CFR §164.528. Provider shall, within twenty (20) business days of written request from the City, provide adequate documentation of such disclosures as necessary for City to satisfy its obligations under 45 CFR §164.528.

(v) Forwarding Requests. In the event Provider receives directly from an Individual any written request of the nature described in paragraphs (i) through (iv) above, Provider shall forward such request to the City HIPAA Privacy Officer within five (5) business days. This requirement shall not apply to the extent Provider responds directly to such requests as set forth in paragraph (vi) below.

(vi) Delegation to Provider. If the City has directed Provider in writing to act on behalf of the City with respect to Individuals' requests for access to records, amendment of records, and/or accounting of disclosures, Provider shall respond directly to Individuals in a time and manner that meets the City's obligations under the Privacy Rule (including, but not limited to, 45 CFR §§ 164.524, 164.526, and 164.528), any applicable guidance issued by HHS (for example, as posted at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html), and any other Applicable Law. In no event shall Provider charge any fees in excess of the amount the City would be permitted to charge under 45 CFR §164.524(c)(4), related HHS guidance, or any other Applicable Law. Provider shall maintain written records of such requests and retain such documentation as required by the HIPAA Rules and other Applicable Law.

(7) Notice of Complaints. If Provider receives a complaint from an Individual regarding Provider's use or disclosure of City PHI, Provider shall provide a copy of the complaint to the City HIPAA Privacy Officer within five (5) business days after Provider receives it.

(8) Inspection of Books and Records.

(i) HHS. Provider shall make its internal practices, books, and records relating to the use and disclosure of City PHI available to the Secretary of HHS for purposes of determining the City's or Provider's compliance with HIPAA. Provider shall promptly notify the City HIPAA Privacy Officer of communications with HHS regarding City PHI.

(ii) City. Provider shall make available to City and its authorized agents, at Provider's place of business during normal business hours, all facilities, systems, procedures, records, books, agreements, and policies relating to the use and/or disclosure of City PHI for purposes of enabling City to determine Provider's compliance with these City PHI Terms.

(9) Judicial and Administrative Proceedings. In the event Provider receives a subpoena, discovery request, or request from a governmental agency that may potentially require the disclosure of City PHI, Provider: (i) shall promptly forward a copy to the City HIPAA Privacy Officer; and (ii) shall not disclose the requested City PHI without written authorization from the City HIPAA Privacy Officer.

(10) Compliance with Electronic Transactions and Code Set Standards. If Provider conducts any Standard Transaction for, or on behalf of, the City, Provider shall comply, and shall require any Subcontractor conducting such Standard Transaction to comply, with each applicable requirement of 45 CFR Part 162.

(d) Incident Reporting and Management.

(1) Incident Reporting. Provider shall give written notice of any Incident to the City HIPAA Privacy Officer and the HIPAA Privacy Officer of each Covered Unit whose information was potentially affected as follows:

(i) Initial Report. As soon as possible, but no later than five (5) business days after Discovery of an Incident, an initial Incident report shall be provided that includes: a description of the Incident; the number (or estimated number) of people potentially affected; the date of occurrence and the date of discovery; the nature and extent of City PHI involved; and whether the Incident involved Unsecured City PHI.

(ii) Full Report. As soon as possible, but no later than fifteen (15) business days after Discovery of an Incident, an updated Incident report shall be provided that includes: Provider's conclusion of whether the Incident constitutes a Breach of Unsecured City PHI and basis for such conclusion; and, for any Breach of Unsecured City PHI, the information specified in 45 CFR §164.410(c). Provider shall promptly supplement such report with additional information as it becomes available, even if such information becomes available after Individuals have been notified of a Breach.

(2) Cooperation with the City. Provider shall cooperate with the City in investigating any Incident and shall promptly provide additional information related to the Incident as requested by the City. As between City and Provider, City shall have the final authority to determine whether a Breach of Unsecured PHI has occurred and whether notifications are required under HIPAA or other Applicable Law. If the City determines that HHS, affected Individuals, or others must be notified, the City shall provide such notifications unless otherwise agreed to in writing by the City and Provider. Provider shall provide to the City full and timely assistance in preparing and providing such notifications.

(3) Corrective Actions. In addition to the obligations set forth above, Provider shall promptly: (i) take corrective action to remedy any Incident; (ii) mitigate, to the extent practicable, any harmful effect of any Incident; and (iii) take any other action required by the City pertaining to such Incident (e.g. establishment and staffing of a toll-free telephone contact number, credit monitoring, mail individual notifications, etc.).

(4) Report of Unsuccessful Security Incident. The parties acknowledge and agree that this Section (d)(4) constitutes notice by Provider to the City of the ongoing existence and occurrence of Unsuccessful Security Incidents. The foregoing notwithstanding, Provider shall, upon the City's written request, provide a report that: (i) identifies the categories of Unsuccessful Security Incidents; (ii) states whether Provider believes its current defensive security measures are reasonable and appropriate to address Unsuccessful Security Incidents, given the scope and nature of such attempts; and (iii) if the security measures are not reasonable and appropriate, identifies measures Provider will implement to address the security inadequacies.

(5) Indemnification. To the extent an Incident occurs involving Unsecured City PHI under the custody or control of Provider or its Subcontractor or agent, then, in addition to any other obligation of Provider under the Contract, and notwithstanding any other provision in the Contract

to the contrary, Provider will indemnify the City for: (i) all costs and expenses the City incurs to investigate an Incident and, if the City determines that a Breach has or may have occurred, to comply with the notification and mitigation requirements of the HIPAA Rules or other Applicable Law; and (ii) any fees, fines, penalties, costs, expenses, and other liabilities incurred by the City as a result of the Incident.

(e) Obligations of City to Inform Provider of Privacy Practices and Restrictions.

(1) The City shall notify Provider of any limitation(s) in the City's notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect Provider's use or disclosure of City PHI.

(2) The City shall notify Provider of any changes in, or revocation of, permission by an Individual to use or disclose City PHI, to the extent that such changes may affect Provider's use or disclosure of City PHI.

(3) The City shall notify Provider of any restriction on the use or disclosure of City PHI that has been requested by an Individual and agreed to by the City in accordance with 45 CFR §164.522, to the extent that such restriction may affect Provider's use or disclosure of City PHI.

(f) Termination.

(1) Termination for Cause. In addition to and without limiting any other termination rights or remedies of the City provided for in the Contract, the City shall have the right to terminate the Contract immediately if the City determines that Provider has failed to cure a material breach of these City PHI Terms within ten (10) business days after the City notifies Provider of such breach.

(2) Disposition of City PHI Upon Termination. Upon termination of the Contract for any reason, Provider shall, and shall ensure its Subcontractors and agents that possess City PHI fulfill one of the following options with respect to such City PHI:

(i) Return the City PHI to the City in whatever form or medium that Provider received from or created on behalf of the City, or, if so directed by the City in writing, destroy the City PHI using technology or a methodology that renders it unusable, unreadable, or undecipherable to unauthorized individuals in accordance with the most recent guidance issued by HHS. Provider shall not retain any City PHI in any electronic, paper, or other form, format, or medium. Within thirty (30) business days after the termination of the Contract, Provider shall certify in writing to the City that such return or destruction has been completed.

(ii) To the extent required by Applicable Law or directed by the City in writing, retain City PHI after the termination of the Contract. Provider shall extend the protections of these City PHI Terms to any retained City PHI and shall limit further uses and disclosures strictly to those purposes that are required by Applicable Law or directed by the City in writing. At such time as Applicable Law and the City no longer require Provider to retain the City PHI, Provider shall return or destroy the City PHI in accordance with paragraph (i) above.

(g) Miscellaneous.

(1) Notices. Notwithstanding anything to the contrary in the Contract, any notification given to the HIPAA Privacy Officer of a Covered Unit pursuant to these City PHI Terms shall be in a writing delivered by fax or email with a copy delivered by 1st class mail to the addresses below, or such other address(es) as the City may provide in a written notification to Provider.

Health and Welfare Benefits
Attn: HIPAA Privacy Officer
City of Philadelphia, Office of Human Resources
2 Penn Center Plaza - 16th Floor
Philadelphia, PA 19102
Fax: 215-686-0610

Ambulatory Health Services
Attn: HIPAA Privacy Officer
Philadelphia Department of Public Health
500 South Broad St - Suite 360
Philadelphia, PA 19146
Fax: 215-685-6732

Emergency Medical Services
Attn: HIPAA Privacy Officer
Philadelphia Fire Department, EMS Administration
240 Spring Garden Street
Philadelphia, PA. 19123
Fax: 215-685-4207

Public Health Laboratory
Attn: HIPAA Privacy Officer
Philadelphia Department of Public Health
500 South Broad St, 3rd Floor
Philadelphia, PA 19146
Fax: 215-545-7297

Office of Behavioral Health and Intellectual disAbility Services
Attn: HIPAA Privacy Officer
City of Philadelphia, OBHIDS
1101 Market St. 7th floor
Philadelphia, PA 19107
Fax: 215-685-5563

STD Control Program
Attn: HIPAA Privacy Officer
Philadelphia Department of Public Health
1930 S. Broad Street, Unit 30
Philadelphia, PA 19145
Fax: 215-545-8362

Notification to the City HIPAA Privacy Officer shall be in a writing delivered by email with a copy delivered by 1st class mail to the address below:

City of Philadelphia Law Department
Attn: City HIPAA Privacy Officer
1515 Arch Street, 15th Floor
Philadelphia, PA 19102
E-mail: HIPAAPrivacy@phila.gov

(2) Order of Precedence. Provider and City agree that these City PHI Terms shall supersede any provisions in the Contract to the contrary.

(3) Privacy Law Modifications Notice. Notwithstanding anything to the contrary in the Contract, the Provider and the City agree that these City PHI Terms shall be deemed automatically modified as the City deems necessary from time to time to ensure continued compliance with the requirements of HIPAA and other Applicable Law, such modification to be effective upon the City posting the modified Terms and Conditions Relating to Protected Health Information on the City's website (at https://philawx.phila.gov/econtract/ under the "About" link).

(3) Survival. In addition to and without limiting the survival of any other rights, obligations, or liabilities provided for in the Contract, the obligations of Provider set forth in these City PHI Terms shall be enforceable with respect to any City PHI retained by Provider or its Subcontractors or agents after the expiration or termination of the Contract.

(4) Interpretation. Any ambiguity in these City PHI Terms shall be resolved to permit the City and require Provider to comply with HIPAA and other Applicable Law.