

RESOLUTION NO. RS2020 - 247

A resolution approving a data sharing agreement between The Metropolitan Government of Nashville and Davidson County, acting by and through the Metropolitan Board of Health, and the Tennessee Department of Health, to share drug overdose data for program planning and public health intervention.

WHEREAS, it is to the mutual benefit of the Tennessee Department of Health and the Metropolitan Government of Nashville and Davidson County, acting by and through the Metropolitan Board of Health, to share drug overdose data for program planning and public health intervention; and,

WHEREAS, the Tennessee Department of Health and the Metropolitan Government of Nashville and Davidson County, acting by and through the Metropolitan Board of Health, have entered into a data sharing agreement, attached hereto and incorporated herein, to share drug overdose data for program planning and public health intervention; and,

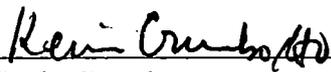
WHEREAS, it is to the benefit of the citizens of The Metropolitan Government of Nashville and Davidson County that this data sharing agreement be approved.

NOW, THEREFORE, BE IT RESOLVED BY THE COUNCIL OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY:

Section 1. That the data sharing agreement between the Tennessee Department of Health and The Metropolitan Government of Nashville and Davidson County, acting by and through the Metropolitan Board of Health, to share drug overdose data for program planning and public health intervention, a copy of which is attached hereto and incorporated herein, is hereby approved.

Section 2. That this resolution shall take effect from and after its adoption, the welfare of The Metropolitan Government of Nashville and Davidson County requiring it.

APPROVED AS TO AVAILABILITY
OF FUNDS:



Kevin Crumbo
Finance Director

INTRODUCED BY:

Member(s) of Council

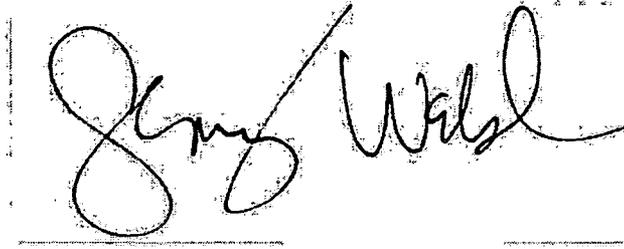
APPROVED AS TO FORM
AND LEGALITY:

A handwritten signature in cursive script, appearing to read "Dennis C. Smith", is written over a horizontal line.

Assistant Metropolitan Attorney

Electronic Signature Page

(Attach to Legislation Pursuant to Rule 8 of the Council Rules of Procedure)

A handwritten signature in black ink, appearing to read "Ginny Welsch". The signature is written in a cursive style with a large initial "G" and a long horizontal stroke at the end. It is positioned above a horizontal line.

Ginny Welsch
Council Member, District 16

**DATA SHARING AGREEMENT
BETWEEN THE STATE OF TENNESSEE,
DEPARTMENT OF HEALTH
AND
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

This Data Sharing Agreement (Agreement), by and between the State of Tennessee, Department of Health, hereinafter referred to as the "State" or "TDH" and Metropolitan Government of Nashville and Davidson County, hereinafter referred to as the "Metro" or "Contractor," (individually and collectively "Party" or the "Parties") is for the purposes of sharing drug overdose data, as further defined in the "SCOPE OF SERVICES."

WHEREAS, pursuant to Tenn. Code Ann. § 68-11-314 and Tenn. Comp. R. & Regs. 1200-14-01-.02, TDH collects data from healthcare facilities across the State on patients with discharge diagnoses that include drug poisonings ("Overdose(s)");

WHEREAS, healthcare facilities transmit data to TDH at a regular frequency and manner as defined by the State, and include information on the individual experiencing the Overdose as well as the diagnosis codes available in the electronic health record and disposition of the patient ("Overdose Data");

WHEREAS, the purpose of the Overdose Data is to conduct surveillance on drug Overdoses across the State for the purposes of program planning and public health interventions;

WHEREAS, Metro conducts surveillance and responds to public health emergencies at the local level as part of its duties as a public health department and access to available Overdose Data is essential to these activities.

NOW, THEREFORE, the Parties agree as follows:

A. SCOPE:

- A.1. TDH shall make available to Metro patient level Overdose Data relevant to the Metro.
- a. Overdose Data elements shall include at a minimum:
 1. patient name and address
 2. diagnostic codes associated with the overdose
 3. reporting healthcare facility
 4. dates of service
 - b. TDH will make available the Overdose Data on at least a biweekly basis.
 - c. TDH will make available the Overdose data using secure methods, with specific method of transfer, file formatting and encryption methods to be determined by the Parties.
- A.2. Metro shall use this Overdose Data only for its surveillance and public health duties, including responding to public health emergencies.
- a. Overdose data is highly sensitive and confidential information. Only Metro employees engaged in activities directly related to Overdose surveillance, prevention, and programs shall have access to the Overdose Data, including employees studying Overdose related comorbidities. Metro shall provide these employees with the minimum data necessary to

achieve purposes specified in this section.

- b. Metro employees shall obtain TDH Institutional Review Board approval for research using the Overdose Data.
- c. Metro will require that all employees with access to the Overdose Data complete and maintain current training in the management, storage, and use of HIPAA protected data prior to access to Overdose Data.
- d. Metro shall not share Overdose Data with any third parties, including, but not limited to, law enforcement, external agencies and partners, contractors and media. Media requests for Overdose Data shall be directed to the TDH Public Information Officer. All other requests and Inquiries related to Overdose Data shall be directed to the Director of the Office of Informatics and Analytics.
- d. Metro shall not disclose names nor other identifying information from the Overdose Data dataset either during this Agreement or hereafter to any persons others than Metro employees engaged in activities directly related to Overdose surveillance, prevention, and programs.
- e. Metro level Overdose Data shall not be made publicly available, even in aggregate, without express written permission and in coordination with the Office of Informatics and Analytics at TDH.
- f. If Metro would like TDH to provide additional Overdose Data elements, Metro shall make a request for the additional data in writing to TDH. TDH approved data element additions shall be reflected in a written amendment to this Agreement which shall be signed by both Parties.
- g. Metro will designate a single contact person who is authorized to coordinate transfer of the Overdose Database to Metro and who is responsible for granting access to Metro employees.
- h. Metro shall maintain an audit trail of Overdose Data access authorizations for its Employees, and provide a report of authorizations on a quarterly basis.

B. TERM OF AGREEMENT:

- B.1. This Agreement shall be effective on April 1, 2019 ("Effective Date"), and extend for a period of three (3) years after the Effective Date ("Term"). The State shall have no obligation for goods or services provided by the Metro prior to the Effective Date.
- B.2. Renewal Options. This Agreement may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to two (2) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.

C. PAYMENT TERMS AND CONDITIONS:

There shall be no cost to either Party for the performance of services under this Agreement.

D. STANDARD TERMS AND CONDITIONS:

- D.1. Required Approvals. The State is not bound by this Agreement until it is signed by the Parties and approved by appropriate officials in accordance with applicable Tennessee laws and regulations (depending upon the specifics of this Agreement, said officials may include, but are

not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).

- D.2. Modification and Amendment. This Agreement may be modified only by a written amendment signed by all parties hereto and approved by both the officials who approved the base contract and, depending upon the specifics of the contract as amended, any additional officials required by Tennessee laws and regulations (said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).
- D.3. Termination for Convenience. This Agreement may be terminated by either Party by giving written notice to the other, at least thirty (30) days before the effective date of termination. Said termination shall not be deemed a breach of Agreement. Upon such termination, neither the State nor the Contractor shall have a right to any actual general, special, incidental, consequential, or any other damages whatsoever of any description or amount.
- D.4. Termination for Cause. If the Contractor fails to properly perform its obligations under this Agreement in a timely or proper manner, or if the Contractor violates any terms of this Agreement, the State shall have the right to immediately terminate the Agreement. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any breach of this Agreement by the Contractor.
- D.5. Subcontracting. The Contractor shall not assign this Agreement or enter into a subcontract for any of the services performed under this Agreement without obtaining the prior written approval of the State. If such subcontracts are approved by the State, each shall contain, at a minimum, sections of this Agreement below pertaining to "Conflicts of Interest," "Nondiscrimination," and "Records" (as identified by the section headings). Notwithstanding any use of approved subcontractors, the Contractor shall be the prime contractor and shall be responsible for all work performed.
- D.6. Conflicts of Interest. The Contractor warrants that no amount shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed relative to this Agreement.
- D.7. Nondiscrimination. The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Agreement or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, color, religion, sex, national origin, or any other classification protected by Federal, Tennessee State constitutional, or statutory law. The Contractor shall, upon request, show proof of such nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.
- D.8. Records. The Contractor shall maintain documentation of services rendered under this Agreement. The books, records and documents of the Contractor, insofar as they relate to work performed under this Agreement, shall be maintained for a period of three (3) full years from the final date of this Agreement and shall be subject to audit, at any reasonable time and upon reasonable notice, by the State, the Comptroller of the Treasury, or their duly appointed representatives.
- D.9. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Agreement shall be subject to monitoring and evaluation by TDH, the State, the Comptroller of the Treasury, or their duly appointed representatives.
- D.10. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested.

- D.11. Strict Performance. Failure by any party to this Agreement to insist in any one or more cases upon the strict performance of any of the terms, covenants, conditions, or provisions of this Agreement shall not be construed as a waiver or relinquishment of any such term, covenant, condition, or provision. No term or condition of this Agreement shall be held to be waived, modified, or deleted except by a written amendment signed by the parties hereto.
- D.12. Independent Contractor. The parties hereto, in the performance of this Agreement, shall not act as employees, partners, joint venturers, or associates of one another. It is expressly acknowledged by the parties hereto that such parties are independent contracting entities and that nothing in this Agreement shall be construed to create an employer/employee relationship or to allow either to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever.

The Contractor, being a Tennessee governmental entity, is governed by the provisions of the Tennessee Government Tort Liability Act, *Tennessee Code Annotated*, Sections 29-20-101 *et seq.*, for causes of action sounding in tort. Further, no contract provision requiring a Tennessee political entity to indemnify or hold harmless the State beyond the liability imposed by law is enforceable because it appropriates public money and nullifies governmental immunity without the authorization of the General Assembly.

- D.13. State Liability. The State shall have no liability except as specifically provided in this Agreement.
- D.14. Force Majeure. The obligations of the parties to this Agreement are subject to prevention by causes beyond the parties' control that could not be avoided by the exercise of due care including, but not limited to, natural disasters, riots, wars, epidemics, or any other similar cause.
- D.15. State and Federal Compliance. The Contractor shall comply with all applicable State and Federal laws and regulations in the performance of this Agreement.
- D.16. Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Tennessee. The Contractor agrees that it will be subject to the exclusive jurisdiction of the courts of the State of Tennessee in actions that may arise under this Agreement. The Contractor acknowledges and agrees that any rights or claims against the State of Tennessee or its employees hereunder, and any remedies arising therefrom, shall be subject to and limited to those rights and remedies, if any, available under *Tennessee Code Annotated*, Sections 9-8-101 through 9-8-407.
- D.17. Completeness. This Agreement is complete and contains the entire understanding between the parties relating to the subject matter contained herein, including all the terms and conditions of the parties' agreement. This Agreement supersedes any and all prior understandings, representations, negotiations, and agreements between the parties relating hereto, whether written or oral.
- D.18. Severability. If any terms and conditions of this Agreement are held to be invalid or unenforceable as a matter of law, the other terms and conditions hereof shall not be affected thereby and shall remain in full force and effect. To this end, the terms and conditions of this Agreement are declared severable.
- D.19. Headings. Section headings of this Agreement are for reference purposes only and shall not be construed as part of this Agreement.

E. SPECIAL TERMS AND CONDITIONS:

- E.1. “Confidential State Data” is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:
- E.1.a. The Contractor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of the backup data.
- E.1.b. The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard (“FIPS”) 140-2 validated encryption technologies.
- E.1.c. The Contractor and the Contractor’s processing environment containing Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization (“ISO”) 27001; (ii) Federal Risk and Authorization Management Program (“FedRAMP”); or (2) be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants (“AICPA”) for a System and Organization Controls for service organizations (“SOC”) Type II audit. The State shall approve the SOC audit control objectives. The Contractor shall provide proof of current ISO certification of FedRAMP authorization for the Contractor and Subcontractor(s), or provide the State with the Contractor’s and Subcontractor’s annual SOC Type II audit report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. The Contractor shall submit corrective action plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Contractor or Subcontractor.

If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Contractor must provide the State a letter from the Contractor or Subcontractor stating whether the Contractor or Subcontractor made any material changes to their control environment since the prior audit and, if so, whether the changes, in the opinion of the Contractor or Subcontractor, would negatively affect the auditor’s opinion in the most recent audit report.

No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Maximum Liability of this Contract.

- E.1.d. The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. “Processing Environment” shall mean the combination of software and hardware on which the Application runs. “Application” shall mean the computer code that supports and accomplishes the State’s requirements as set forth in this Contract. “Penetration Tests” shall be in the form of attacks on the Contractor’s computer system, with the purpose of discovering security weaknesses which have the potential to gain access to the Processing Environment’s features and data. The “Vulnerability Assessment” shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Contractor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.
- E.1.e. Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State.
- E.1.f. Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of the National Institute of Standards and Technology (“NIST”) Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

E.2 Minimum Requirements

- E.2.a. The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the State's Enterprise Information Security Policies as amended periodically. The State's Enterprise Information Security Policies document is found at the following URL: <https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html>.
- E.2.b. The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.
- E.2.c. If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

- E.3. Comptroller Audit Requirements. Upon reasonable notice and at any reasonable time, the Contractor and Subcontractors agree to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Contractor and all Subcontractors used by the Contractor. Contractor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Contract. Contractor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives' access to Contractor and Subcontractor(s) personnel for the purpose of performing the information technology control audit.

The information technology control audit may include a review of general controls and application controls. General controls are the policies and procedures that apply to all or a large segment of the Contractor's or Subcontractor's information systems and applications and include controls over security management, access controls, configuration management, segregation of duties, and contingency planning. Application controls are directly related to the application and help ensure that transactions are complete, accurate, valid, confidential, and available. The audit shall include the Contractor's and Subcontractor's compliance with the State's Enterprise Information Security Policies and all applicable requirements, laws, regulations or policies.

This audit may include interviews with technical and management personnel, physician inspection of controls, and review of paper or electronic documentation.

For any audit issues identified, the Contractor and Subcontractor(s) shall provide a corrective action plan to the State within 30 days from the Contractor or Subcontractor receiving the audit report.

Each party shall bear its own expenses incurred while conducting the information technology controls audit.

- E.4. Personally Identifiable Information. While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other

applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify or ensure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within twenty-four (24) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law.

- E.5. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Agreement, these special terms and conditions shall control.
- E.6. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Agreement shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by EMAIL or facsimile transmission with recipient confirmation. Any such communications, regardless of method of transmission, shall be addressed to the respective party at the appropriate mailing address, facsimile number, or EMAIL address as set forth below or to that of such other party or address, as may be hereafter specified by written notice.
- E.7. Metro acknowledges and agrees that all security and confidentiality requirements in Section E hereunder are required by the State. To the extent that Metro does not or cannot meet those specifications, Metro shall maintain the highest standards possible and available to it. Metro further acknowledges and agrees that it remains responsible for the security and confidentiality of the data shared hereunder regardless of its ability to meet the standards. The State shall not be responsible for the Metro's technical limitations.

The State:
 Valerie Nagoshiner
 Chief of Staff
 Department of Health
 Andrew Johnson Tower, 5th Floor
 710 James Robertson Parkway
 Nashville, TN 37243
 Email Address: Valerie.Nagoshiner@tn.gov
 Telephone: (615) 532-5895

Metro:
 Director of Health
 Metro Public Health Department
 2500 Charlotte Avenue
 Nashville, TN 37209

All instructions, notices, consents, demands, or other communications shall be considered effectively given upon receipt or recipient confirmation as may be required.

- E.8. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State shall be regarded as confidential information in accordance with the provisions of applicable state and federal law, state and federal rules and regulations, departmental policy, and ethical standards. Such confidential information shall not be disclosed, and all necessary steps shall be taken by the Contractor to safeguard the confidentiality of such material or information in conformance with applicable state and federal law, state and federal rules and regulations, departmental policy, and ethical standards.

The Contractor's obligations under this section do not apply to information in the public domain; entering the public domain but not from a breach by the Contractor of this Agreement; previously possessed by the Contractor without written obligations to the State to protect it; acquired by the Contractor without written restrictions against disclosure from a third party which, to the Contractor's knowledge, is free to disclose the information; independently developed by the Contractor without the use of the State's information; or, disclosed by the State to others without restrictions against disclosure. Nothing in this paragraph shall permit Contractor to disclose any information that is confidential under federal or state law or regulations, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties.

It is expressly understood and agreed the obligations set forth in this section shall survive the termination of this Contract.

- E.9. HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations.
- a. Contractor warrants to the State that it is familiar with the requirements of HIPAA and its accompanying regulations, and will comply with all applicable HIPAA requirements in the course of this Contract.
 - b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by HIPAA and its regulations, in the course of performance of the Contract so that both parties will be in compliance with HIPAA.

- c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by HIPAA and that are reasonably necessary to keep the State and Contractor in compliance with HIPAA. This provision shall not apply if information received by the State under this Contract is NOT "protected health information" as defined by HIPAA, or if HIPAA permits the State to receive such information without entering into a business associate agreement or signing another such document.

IN WITNESS WHEREOF, the parties have by their duly authorized representatives set their signatures.

METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

Janni Crespo
Interim Director, Metro Public Health Department

02/13/2020
Date

Alan Johnson
Chair, Board of Health

2/13/2020
Date

APPROVED AS TO AVAILABILITY OF FUNDS:

Kennie Crumby/ste
Director, Department of Finance K

2/21/2020
Date

APPROVED AS TO RISK AND INSURANCE:

TCW
Director of Risk Management Services

2/26/20
Date

APPROVED AS TO FORM AND LEGALITY:

David C. Smith
Metropolitan Attorney

2/27/2020
Date

ATTEST:

Metropolitan Clerk

Date

DEPARTMENT OF HEALTH:

Lisa Piercey, MD, MBA, FAAP,
Commissioner

Date