DATA USE AGREEMENT
BETWEEN
THE STATE OF TENNESSEE DEPARTMENT OF HEALTH
AND
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY
[VITAL STATISTICS]

This Data Use Agreement ("Agreement" or "DUA") is by and between the State of Tennessee Department of Health ("State" or "TDH"), and the Metropolitan Government of Nashville and Davidson County ("Recipient"). TDH agrees to provide Recipient with TDH Data, as more fully described below, for the uses described in this Agreement.

Recipient is a: Tennessee Local Government Entity.

Recipient Principal Place of Business:

Metro Public Health Department
2500 Charlotte Avenue
Nashville, Tennessee 37209

HIPAA Status:

TDH program providing data is *not* a HIPAA covered component.
Recipient's Program, its Metro Public Health Department, is a HIPAA hybrid entity.

NOW, THEREFORE, TDH and Recipient agree:

A. Scope – Background

A.1. TDH operates the Office of Vital Statistics ("TDH Program"), which reviews, registers, amends, issues and maintains the original certificates of births, deaths, marriages and divorces that occur in Tennessee in accordance with Tennessee law. *See:* Tenn. Code Ann. §§ 68-3-101 *et seq.*

A.2. Recipient, on behalf of its Metro Public Health Department desires to receive; certain data, as more fully described below, to support its public health surveillance and response, as more fully described below ("Purpose").

A.3. The TDH Program, by its State Registrar, is permitted to release certain data pursuant to Tenn. Comp. R. & Regs. 1200-07-01-.11.

a. The State Registrar may permit the use of data from vital records for research purposes. No data shall be furnished from records for research purposes until the State Registrar has prepared, in writing, the conditions under which the records or data will be used and has received an agreement signed by a responsible agent of the research organization agreeing to meet with and conform to such conditions.

b. The State Registrar may disclose data ***which is not confidential*** from vital records to any federal, state, county or municipal agencies, courts, or law enforcement agencies which request such data in the conduct of their official duties. The Social Security numbers of the parent(s) as listed on the child's birth certificate may be disclosed for the purpose of child support enforcement. ***[Emphasis added].***

A.4. TDH and Recipient recognize the need to set forth and define the terms under which TDH will provide TDH Data, including Confidential State Data, to Recipient for the Purpose,

approved by the Tennessee State Registrar as provided by Tenn. Comp. R. & Regs. 1200-07-01-.11, confirmed by the execution of this Agreement by the State Registrar.

A.5. Recipient acknowledges all data requested must be evaluated for confidentiality and comply with any applicable Federal and State laws, rules, and regulations.

B. Scope - Definitions

B.1. "Authorized Persons" means Recipient's employees and contractors who have used the Data for its Purpose, and who are bound by confidentiality obligations sufficient to protect TDH Data in accordance with the terms and conditions of this Agreement and applicable laws, rules, and regulations.

B.2. "Confidential State Data" means data deemed confidential by State or Federal statute or regulation. *All TDH Data provided under this Agreement is Confidential State Data.*

B.3. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as amended, including HITECH, and regulations.

B.4. "IRB" means the State of Tennessee Department of Health Institutional Review Board. Additional information. Data Governance

B.5. "Individually Identifiable Health Information" is information that is a subset of health information, including demographic information collected from an individual as defined by HIPAA, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

B.6. "Personal Identifiable Information" (PII) is any information as defined by HIPAA and/or Tennessee law that may be used to identify an individual.

B.7. "Protected Health Information" (PHI) is all individual identifiable health information as defined by HIPAA, including demographic data, medical histories, and test results.

B.8. "Purpose" means the Recipient's purpose(s) for the use of the data received under this Agreement. "Research" means a systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to generalized knowledge.

B.9. "TDH Data" means health records and information held, collected, or maintained by TDH or TDH contractors.

B.10. "TDH Program Personnel" means TDH employees or TDH contractors responsible for data systems and data sets.

C. Scope - Data Use & Recipient Obligations

C.1. The following Data Set(s) will be provided by TDH to Recipient:

Vital Statistics Files	Years
Finalized Birth	2022-2030
Finalized Death	2022-2030
Finalized Fetal Death	2022-203
Finalized Linked Birth Infant Death	2021-2029

Note: Under no circumstances will any data be provided under this Agreement for Sexually Transmitted Infection(s) as required by Tenn. Code Ann. § 68-10-113.

a. Modification of Vital Records Data. Recipient acknowledges that the Office of Vital Records data contained in the final Statistical Files is static and does not represent changes to records occurring after the finalization process. Vital Records may be modified for up to One Hundred (100) years.

C.2. Purpose.

a. For all Confidential State Data received under this Agreement, the Recipient's Purpose is research and conduct of official duties as set forth in Tenn. Comp. R. & Regs. 1200-07-01-.11(8).

b. Recipient will provide TDH with reports on the use of the TDH Data provided under this Agreement as more fully set forth below.

C.3. Restriction on Recipient Use & Release of Data; Prohibited Uses.

a. Recipient shall only use this Data Set for the stated Purpose.

b. TDH makes no representation or warranty as to the accuracy or completeness of the TDH Data provided to Recipient.

c. Recipient may release TDH Data provided under this Agreement *only in aggregate form.* No cell containing a value less than 11 (eleven) may be displayed, and no use of percentages or other mathematical formulas may be used if they result in the display of a cell with a value of less than 11 (eleven).

d. Recipient may request written permission to release individual level data sets from the TDH data from the State Registrar.

e. Recipient is expressly forbidden to use the TDH Data provided under this Agreement to contact any individual(s) identified in the TDH Data. Failure to comply with this provision is a breach of this Agreement and will result in immediate termination.

f. Recipient may request linkage for any individual in the TDH Data to another data set by contacting TDH. Approval of the State Registrar is required for each such requested linkage.

g. Any use of the TDH Data provided under this Agreement contrary to the provision of this Section

C.4. If Recipient is a breach of this Agreement, and TDH may, in its sole discretion:

a. Immediately terminate this Agreement;

b. Require Recipient to return the TDH data or delete the TDH Data and provide written confirmation of deletion.

C.5. Reporting.

a. *Semi-Annual Disclosure Report.* During the term of this Agreement, Recipient shall provide to TDH, a semi-annual report of disclosures on July 1 and February 1 ("Semi- annual Disclosure Report") for the previous calendar year no later than March 1st of the following year.

(1) Recipient(s);
(2) Purpose;
(3) Date of Disclosure; and
(4) Data Provided.

b. *Expiration/Termination Disclosure Report.* Within thirty (30) days following the expiration or termination of this Agreement, Recipient shall provide to TDH a report of all disclosures made under this Agreement ("Expiration/Termination Disclosure Report"). The provisions of this Section C.5. survive the termination of this Agreement for any reason.

C.6. The method of data delivery for use will be agreed to by TDH and Recipient and meet the requirements of TDH to assure the security of the data in transit.

C.7. Research. Recipient shall obtain *separate* TDH IRB approval for any research or official duties not described in this DUA but using TDH Data provided under this Agreement.

C.8. Unauthorized Access/Potential Disclosure. Recipient shall report to the State any instances of unauthorized access to, or potential disclosure of, P II in the custody or control of Recipient ("Unauthorized Disclosure") that comes to Recipient's attention. Any such report shall be made by Recipient within twenty-four (24) hours after the Unauthorized Disclosure is known by Recipient. Recipient shall take all necessary measures to halt any further Unauthorized Disclosures.

If Recipient and TDH agree that the risk of harm requires notification of potentially affected individuals of the disclosure or security breach, Recipient will provide notification. Recipient and TDH may agree that additional remedies are appropriate and such remedies will be without cost to TDH, including, no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. 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 DUA or otherwise available at law. The obligations set forth in this Section shall survive the termination of this DUA.

C.9. Breach Reporting/Data Loss Reporting. Recipient shall report any breach of PII from the TDH Data, loss of this data, and uses or disclosures that are in violation of this DUA to the TDH Privacy Officer and the Recipient Privacy Officer within twenty-four (24) hours of Recipient's discovery of such disclosure, and Recipient shall cooperate fully in the security incident process.

TDH Privacy Officer:
TDH Privacy Officer
Andrew Johnson Tower, 5th Floor
710 James Robertson Parkway
Nashville, TN 37243
Phone: 615-741-1969
privacy.health@tn.gov

With copy to:
State Registrar
710 James Roberston Parkway
Nashville, TN 38243
615-532-2678
Gray.Bishop@tn.gov

Recipient's Privacy Officer:
Shannon Heath
2500 Charlotte Avenue
Nashville, TN 37209
Phone: 615-340-5677
Shannon.Health@nashville.gov

C.10. Improper Use/Disclosure. In the event TDH determines or has a reasonable belief that Recipient has or may have made a use, reuse, or disclosure of TDH Data that is not authorized by this Agreement or another written authorization from the TDH, TDH, in its sole discretion, may require Recipient to:

a. promptly investigate and report to TDH, Recipient's determinations regarding any alleged or actual unauthorized use, reuse, or disclosure;

b. promptly resolve any problems identified by the investigation;

c. submit a formal response to an allegation of unauthorized use, reuse, or disclosure; or

d. submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses, or disclosures; and return data files to TDH or destroy the data files it received from TDH under this DUA.

C.11. Unauthorized Use. If TDH determines or reasonably believes that unauthorized uses, reuses, or disclosures have taken place, TDH may, in its sole discretion, *immediately* suspend or discontinue release of further data to Recipient and require Recipient to return/destroy any Data Set provided under this Agreement.

D. Term; Termination

D.1. This Agreement shall be effective as of the date of the last signature on this Agreement ("Effective Date") and extend for a period of three (3) years after the Effective Date ("Term").

D.2. Term Extension. This Agreement may be extended for two (2) additional one (1) year terms, at the sole discretion of TDH. The Parties will execute a written amendment to this Agreement to exercise such Term Extension(s). In no event, however, shall the maximum Term, including all extensions or renewals, exceed a total of sixty (60) months.

D.3. Termination for Convenience. This Agreement may be terminated by TDH or by Recipient by giving THIRTY (30) days' written notice to the other Party. Said termination shall not be deemed a breach of this Agreement. Upon such termination, neither TDH nor Recipient 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 Breach. If Recipient is in breach of any term or condition of this Agreement, TDH may immediately:

a. Terminate this Agreement; and

b. Require Recipient to return and/or delete the subject Data Sets and provide confirmation of such deletion.

E. Compensation. This is a No Cost Contract. TDH, by its Interim Commissioner and the State Registrar, have agreed, as evidence by their signatures on this Agreement, to waive applicable fees.

E.1. Information Technology Security Requirements (State Data, Audit, and Other Requirements).

a. The Recipient shall protect State Data as follows:

(1) The Recipient shall ensure that all State Data is housed in the continental United States, inclusive of backup data. All State data must remain in the United States, regardless of whether the data is processed, stored, in-transit, or at rest. Access to State data shall be limited to US-based (onshore) resources only.

All system and application administration must be performed in the continental United States. Configuration or development of software and code is permitted outside of the United States. However, software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary, which the U.S. Secretary of Commerce acting pursuant to 15 CFR 7 has defined to include the People's Republic of China, among others are prohibited. Any testing of code outside of the United States must use fake data. A copy of production data may not be transmitted or used outside the United States.

(2) The Recipient shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 or 140-3 (or current applicable version) validated encryption technologies.

(3) The Recipient shall implement and maintain privacy and security controls that follow the guidelines set forth in NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," or NIST 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," as amended from time to time. Recipient shall meet annually, or as otherwise agreed, with the State to review the implementation of this Section. A "System Security Plan (SSP)" is required regardless of the type of third-party Controls Audit the Recipient obtains.

No additional funding shall be allocated for these examinations as they are included in the Maximum Liability of this Contract.

(4) The Recipient must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment per the NIST 800-115 definition. "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 Recipient shall provide a letter of

attestation on its processing environment that penetration tests and vulnerability assessments has been performed on an annual basis and taken corrective action to evaluate and address any findings. The Recipient must provide a letter of attestation that includes a penetration testing and vulnerability assessments report that outlines risk exposure of the critical, high, and moderate risks and how they were mitigated, within 30 days of receiving the results.

In the event of an unauthorized disclosure or unauthorized access to State data, the State Strategic Technology Solutions (STS) Security Incident Response Team (SIRT) must be notified and engaged by calling the State Customer Care Center (CCC) at 615-741-1001. Any such event must be reported by the Recipient within twenty-four (24) hours after the unauthorized disclosure has come to the attention of the Contractor.

(5) If a breach has been confirmed a fully un-modified third-party forensics report must be supplied to the State and through the STS SIRT. This report must include indicators of compromise (IOCs) as well as plan of actions for remediation and restoration. Recipient shall take all necessary measures to halt any further Unauthorized Disclosures.

(6) Upon State request, the Recipient shall provide a copy of all Confidential State Data it holds. The Recipient shall provide such data on media and in a format determined by the State

(7) Upon termination of this Agreement and in consultation with the State, the Recipient shall destroy, and ensure all subcontractors shall destroy, all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Recipient shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

b. Minimum Requirements

(1) Recipient and all data centers used by the Recipient to host State data, including those of all Subcontractors, must comply with the most current version of NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," or NIST 800- 171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," with the State to review the implementation of this Section. The State must have proof of compliance with NIST 800-53 or NIST 800-171 in the form of a third-party audit at a minimum every two years or upon request. Davidson County Information Security Management Policies are located at: https://www.nashville.gov/departments/information-technology-services/information-security/information-security-policies

(2) Recipient 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.

(3) If the Application requires middleware or database software, Recipient shall maintain middleware and database software versions that are always fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

(4) In the event of drive/media failure, if the drive/media is replaced, it remains with the State and it is the State's responsibility to destroy the drive/media, or the Recipient shall provide written confirmation of the sanitization/destruction of data according to NIST 800-88. All work undertaken by Recipient and any person acting under direction or control on the TDH Data shall take place on Recipient's premises and under no circumstances shall Recipient, or persons acting under the Recipient's direction or control remove confidential or identifiable data, whether in hard copy or electronic medium from Recipient's premises.

F. Comptroller Audit Requirements

When requested by the State or the Comptroller of the Treasury, the Recipient must provide the State or the Comptroller of the Treasury with a detailed written description of the Recipient's information technology control environment, including a description of general controls and application controls. The Recipient must also assist the State or the Comptroller of the Treasury with obtaining a detailed written description of the information technology control environment for any third or fourth parties used by the Recipient to process State data and/or provide services under this Agreement.

Recipient will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Agreement, including all information technology logging and scanning conducted within the Recipient's information technology control environment. Upon reasonable notice and at any reasonable time, the Recipient grants the State or the Comptroller of the Treasury with the right to audit the Recipient's information technology control environment, including general controls and application controls. The audit may include testing the general and application controls within the Recipient's information technology control environment and may also include testing general and application controls for any third or fourth parties used by the Recipient to process State data and/or provide services under this Agreement. The audit may include the Recipient's compliance with NIDT 800-53 or 800-171 and all applicable requirements, laws, regulations, or policies.

Upon reasonable notice and at any reasonable time, the Recipient agrees to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Recipient. Recipient will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Recipient personnel for the purpose of performing the information technology control audit. The audit may include interviews with technical and management personnel, physical or virtual inspection of controls, and review of paper or electronic documentation.

The Recipient must have a process for correcting control deficiencies that were identified in the State's or Comptroller of the Treasury's information technology audit. For any audit issues identified, the Recipient shall submit a corrective action plan to the State or the Comptroller of the Treasury which addresses the actions taken, or to be taken, and the anticipated completion date in response to each of the audit issues and related recommendations of the State or the Comptroller of the Treasury. The corrective action plan shall be provided to the State or the Comptroller of the Treasury upon request from the State or Comptroller of the Treasury and within 30 days from the issuance of the audit report or communication of the audit issues and recommendations. Upon request from the State or Comptroller of the Treasury, the Recipient shall provide documentation and evidence that the audit issues were corrected.

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

F.1. TDH shall retain ownership of any rights it may have in the TDH Data, and Recipient does not obtain any rights in TDH Data and shall not disclose, release, sell, rent, or otherwise grant access to TDH Data without TDH's prior written consent.

F.2. Recipient shall not use or otherwise grant access to the data referenced in this DUA except as specified in this DUA, Appendix to this DUA, or as otherwise required by law. Recipient shall require any individual acting under its direction or control for the purpose of carrying out the study or project for which the data has been disclosed to Recipient to abide by the terms of this DUA.

F.3. TDH and Recipient shall comply with all applicable federal and state laws, rules, and regulations regarding handling of TDH Data, including, but not limited to applicable obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act (collectively the "Privacy Rules").The obligations set forth in this Section shall survive the termination of this Agreement.

a. Recipient warrants to TDH that it is familiar with the requirements of the Privacy Rules and will comply with all applicable requirements.

b. Recipient warrants that it will cooperate with TDH, including cooperation and coordination with TDH privacy officials and other compliance officers required by the Privacy Rules, during performance of the Agreement so that both Parties comply with the Privacy Rules.

c. Recipient will execute any additional agreements, including but not limited to business associate agreements, as and if required by the Privacy Rules, that are reasonably necessary to keep TDH and Recipient in compliance with the Privacy Rules.

d. To the extent that some or all the Privacy Rules do not apply to information received or delivered by the parties under this Agreement, that information is NOT "protected health information" as defined by the Privacy Rules. Similarly, if the Privacy Rules permit the Parties to receive or deliver the information without entering into a business associate agreement or signing another document, no action is required under this subsection.

e. The Recipient will indemnify the State and hold it harmless for any violation by the Recipient or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.

f. HIPAA Compliance: Recipient must execute a business associate agreement ("BAA") if: (a) the contracting TDH Division is a "covered entity" as defined by the Privacy Rules; and (b) Recipient will provide services to TDH that involve Recipient's access to protected health information ("PHI") as defined by the Privacy Rules. Recipient must execute a BAA with a subcontractor if the subcontractor creates, receives, maintains, or transmits PHI on behalf of the Recipient.

G. Standard Terms

G.1. Communications and Contacts. All instructions, reports, notices, consents, requests, demands, or other communications required or contemplated by this Agreement shall be by email or other appropriate method. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address:

Tennessee Department of Health:
Alyson Holland, Director
Office of Vital Statistics
710 James Robertson Parkway
Nashville, TN 37243
Phone: 6156-532-5515
Email: Alyson.Holland@tn.gov

With Copy to:
TDH Privacy Officer
710 James Robertson Parkway, 5th Floor
Nashville, TN 37243
Phone: 615-741-1969
Email:privacy.health@tn.gov

Recipient:
Metro Public Health Department
Abraham Mukolo, Director Epidemiology Division
2500 Charlotte Avenue
Nashville, TN 37209
Desk: 615-340-8620
Email: Abraham.Mukolo@nashville.gov

G.2. Modification and Amendment. This Agreement may be modified only by a written amendment signed by all Parties.

G.3. State Liability. To the extent permitted by applicable law, the State shall have no liability except as specifically provided in this Agreement.

IN WITNESS WHEREOF:

Recipient: Metropolitan Government of Nashville and Davidson County on behalf of its Metro Public Health Department		
Address: 2500 Charlotte Avenue		
Nashville	State: TN	Zip Code: 37209
Signature: Signed by: Sanmi Areola 0872295CD81A4B1...	Date: 1/15/2026	
Title: Director of Health	Print Name: Sanmi Areola, Ph.D.	

State of Tennessee Department of Health		
Address: 710 James Robertson Parkway, Andrew Johnson Tower		
City: Nashville	State: TN	Zip Code: 37243
Signature:	Date:	
Title: Interim Commissioner	Print Name: Dr. John Dunn	

State of Tennessee Department of Health Office of Vital Statistics/State Registrar		
Address: 710 James Robertson Parkway, Andrew Johnson Tower		
City: Nashville	State: TN	Zip Code: 37243
Signature:	Date:	
Title: State Registrar	Print Name: Edward G. Bishop, III	