**UTAH DEPARTMENT OF HEALTH AND HUMAN SERVICES**
**DATA SHARING AGREEMENT**

This data sharing agreement ("Agreement") is by and between the Utah Department of Health and Human Services (DHHS) ("Department") and San Juan County Public Health Department ("Recipient"). This Agreement establishes conditions, safeguards, and requirements under which the Department agrees to disclose data ("Data" as defined below) to the Recipient and to ensure the confidentiality and security of all such Data.

The purpose of this Agreement is to authorize the Department to share Data with Recipient through a shared technology platform ("Shared Environment") to be used for the public health activities defined below. The Recipient is the public health agency responsible for monitoring the health of San Juan County. Recipient is a member of the Utah Association of Local Health Departments and is recognized by the Utah Department of Health and Human Services.

## 1. AUTHORIZING STATUTE:

The Department is authorized to disclose data to recipient by Utah State Code Title 26B and the data sharing authorities therein. The Department will maintain separately from this Agreement a list of data sources and data elements to be included in the Shared Environment, along with their associated record series and statutes authorizing their disclosure.

## 2. DEFINITIONS:

"Data" means information about individuals, identifiable and non-identifiable, within the Department's possession, custody, or control, and any data that the Department has disclosed to Recipient.

"Shared Environment" means a database in which the department will load approved Data which can be accessed by the Recipient to access and download the Data subject to the terms and conditions of this Agreement.

## 3. PERMITTED USES AND DISCLOSURES:

3.1. Recipient shall only access, use, or disclose Data for public health activities. The Recipient may not use the Data for any other purpose without prior approval of the Department. The Recipient may only access, use, or disclose the Data to analyze, calculate, trend, and monitor:

- 3.1.1. population outlooks;
- 3.1.2. infant health and mortality;
- 3.1.3. newborn screenings;
- 3.1.4. prenatal and maternal care;
- 3.1.5. causes of death;
- 3.1.6. disease surveillance;
- 3.1.7. overdose and suicide deaths;

3.1.8. location and other circumstances of deaths; and

3.1.9. data quality and validation.

3.2. Recipient shall ensure any access to, or use of Data is limited to authorized individuals within its organization who need to access or use the Data in the performance of Recipient's duties under this Agreement. This includes requiring users to only access the Shared Environment and data using their employee credentials.

3.3. Unless specified otherwise, Recipient shall not disclose or distribute any information from the Data that identifies or shall be used to identify an individual to any other organizations or persons. If the Data does not include sufficient information to allow a person to identify the individual described in it or an organization that supplied the Data, Recipient may not attempt to identify an individual whose information is included in the Data through linkage to other databases or through any other methods or process without the prior written approval by the Department. Recipient may not attempt to identify or contact an individual whose information is included in the Data

3.4. Any public release of the Data by Recipient shall only be made in aggregate and with cell suppression in place compliant with the Department's standards posted on the IBIS website.

4. **METHOD OF DATA TRANSMISSION:** All transmissions or exchange of Data between parties shall be performed using a secure transfer method.

The Department agrees to make a Shared Environment available to the Recipient, with appropriate safeguards, protections, and access controls. The Department shall load all approved Data into and provision access for authorized users to the Shared Environment. Recipient's access to the Shared Environment will be granted once the Agreement is signed by both parties. Current files may be uploaded on a recurring schedule at a frequency determined by the Department.

This Data is classified as restricted and requires protection. The Recipient agrees to transfer the Data out of the Shared Environment using a method that protects the Data in transit and at rest that employ cryptographic modules that are not deprecated and are currently validated under the FIPS 140 publications (e.g. TLS 1.2 and 1.3 with validated ciphers).

**5. SAFEGUARDING THE DATA:**

5.1. Recipient shall implement and maintain administrative, technical, and physical safeguards necessary to protect the confidentiality, integrity, and availability of the Data and to prevent unauthorized use or access. Such safeguards include, as appropriate and without limitation: (i) securing Recipient's facilities, data centers, paper files, servers, back-up systems and computing equipment, including all mobile devices and other equipment with information storage capability; (ii) implementing network, device application, database and platform security; (iii) securing information transmission, storage and disposal; (iv) implementing authentication and access controls within media, applications, operating systems and equipment; (v) encrypting identifiable Data stored

on any mobile media and devices and computers/servers that allow remote access; (vi) encrypting identifiable Data transmitted over public or wireless networks; (vii) strictly segregating identifiable Data from information of other unauthorized customers so that Department Data is not commingled with any other types of information where required; (viii) implementing appropriate personnel security and integrity procedures and practices; (ix) providing appropriate privacy and information security training to Recipient's employees; and (x) any other measures reasonably necessary to prevent unauthorized use or access.

5.2. Recipient shall report as soon as possible, but not later than 72 hours after discovery, to the Department any unauthorized access, use, disclosure, modification, or destruction of the Data or any interference with system operations in a system that involves Data of which it becomes aware. Recipient agrees to take reasonable steps to mitigate any effects of such incident and limit any further use or disclosure of the Data. Upon the Department's request, Recipient agrees to consult and cooperate with the Department regarding appropriate steps for remediation and any applicable reporting requirements.

5.3. Recipient agrees that no Data will be stored, transmitted or disposed of outside of the United States.

5.4. Recipient shall not enter any Data received under this Agreement into any generative artificial intelligence tool or website.

5.5. Recipient agrees to only access, retrieve, and use the minimum necessary Data from the Shared Environment needed to complete the task for which the Data is being retrieved.

5.6. Recipient agrees to notify the Department as soon as is reasonably possible after an employee with access to the Shared Environment leaves employment with Recipient or for another reason no longer needs access.

6. **DATA OWNERSHIP:** The Department retains all ownership rights to the Data. Recipient does not obtain any right, title, or interest in any Data furnished by the Department. For purposes of the Agreement, Data does not cease to be the Department's Data solely because it was transferred or transmitted beyond the Department's immediate possession, control, or custody. The Department makes no representation or warranty, either expressed or implied, with respect to the accuracy of any Data disclosed to Recipient.

7. **ACCESS TO BOOKS AND RECORDS REGARDING DATA:** Upon reasonable request by the Department, Recipient shall allow the Department to perform a review of the facilities, systems, books, records, agreements, policies and procedures relating to the access, use, or disclosure of Data to determine Recipient's compliance with the Agreement. The Department may require Recipient to conduct a risk assessment that addresses administrative, technical, and physical risks, if reasonable and appropriate.

8. **TERM AND TERMINATION:** The Agreement is effective upon the signatures of all parties until April 30, 2031. Either party may terminate the Agreement with or without cause upon thirty (30) days' prior written notice to the other party. The Department may terminate the Agreement at any time if deemed necessary because of requirements of law or policy, upon determination by

any party that there has been a breach of system integrity or security by Recipient, or by a failure of Recipient to comply with the Agreement.

9. **DISPOSITION OF DATA:** Upon termination of the Agreement, Recipient shall securely return or destroy all Data, including all copies, compilations, or derivatives in any form or medium, and at any location such information resides in accordance with the disposition guidance from NIST SP 800-88. If such return or destruction is not feasible, Recipient shall promptly notify the Department of the reasons for such in writing. Recipient shall extend the protections and limitations agreed to in the Agreement and shall limit further uses and disclosures to those purposes that make the return or destruction of the Data infeasible. This provision shall survive termination of the Agreement.

10. **INDEMNIFICATION:**

10.1. If Recipient is a governmental entity, the parties mutually agree that each party assumes liability for the negligent and wrongful acts committed by its own agents, officials, or employees, regardless of the source of funding for the Agreement. Notwithstanding the foregoing or anything to the contrary, neither party waives any rights or defenses otherwise available under the Governmental Immunity Act.

10.2. If Recipient is a non-governmental entity, Recipient shall be fully liable for the actions of its agents, employees, officers, partners, and Subcontractors. Contractor shall fully indemnify, defend, and save harmless the Department and the state of Utah from all claims, losses, suits, actions, damages, and costs of every name and description arising out of Recipient's performance of the Agreement caused by any intentional act or negligence of Recipient, its agents, employees, or subcontractors, without limitation; provided, however, that Recipient shall not indemnify for that portion of any claim, loss, or damage arising hereunder due to the sole fault of the Department.

11. **NOTICE:** Any notice or other communications required or permitted to be given under this Agreement shall be sent to:

If to the Department:

Kyle Lunt
Division of Data, Systems & Evaluation director, DHHS
288 North 1460 West
Salt Lake City, Utah 84114
385-332-1578
kylelunt@utah.gov

If to Recipient:

Mike Moulton
Interim Health Officer, Operations Manager
735 S 200 W, Suite 2, Blanding, UT 84511

(435) 587-3838
mmoulton@sanjuancountyut.gov

IN WITNESS WHEREOF, the parties have caused the Agreement to be signed and entered into by their authorized representative.

| For the Department: | For Recipient: |
| --- | --- |
| Signature | Signature |
| Name | Name |
| Title | Title |
| Date | Date |