UTAH DEPARTMENT OF HEALTH AND HUMAN SERVICES
INTERNAL OVERDOSE SURVEILLANCE DASHBOARD FOR LOCAL HEALTH DISTRICTS
SAN JUAN COUNTY PUBLIC HEALTH DEPARTMENT
DATA SHARING AGREEMENT

This data sharing agreement is by and between the Utah Department of Health and Human Services (DHHS), Violence and Injury Prevention Program ("Department") and San Juan County Public Health Department ("Recipient"). The purpose of this agreement is to establish conditions, safeguards, and requirements under which the Department agrees to disclose data to the Recipient and to ensure the confidentiality and security of all such data.

The Department is committed to providing the Recipient access to the Department's Internal Overdose Dashboard to ensure the Recipient has access to reliable and accurate drug overdose data in order to inform public health policy and interventions.

1. AUTHORIZING STATUTE:

The Department is authorized to disclose the data to the Recipient pursuant to Utah Code 26B - 8-406(2) which allows the data to be shared with a governmental entity so long as the data is used for the purpose which it was collected and the Recipient enters into a written agreement.

2. DESCRIPTION OF DATA:

"Data" means all records and information created, received, maintained, or transmitted by the Department which is accessed or used by, or disclosed to, Recipient in connection with the purpose of this agreement including but not limited to information about individuals, whether identifiable and non-identifiable, within the Department's possession, custody, or control, and any data that the Department has disclosed to Recipient.

The Data, which is part of record series # 31316 made available through the Internal Overdose Surveillance Dashboard is aggregated data with the ability to filter the data to look at the data by age group, sex, geographic location (county or LHD boundary), month, and year without low count data suppression applied to the data where low counts exist.

The Department agrees to disclose the following data to the Recipient:

2.1. Syndromic Surveillance data --- drug overdose related encounters from hospitals, emergency departments, urgent care centers, and other ambulatory care outpatient clinics that report syndromic surveillance data to DHHS.

2.2. Office of Medical Examiner (OME) Death data --- suspected drug overdose deaths.

2.3. Office of Vital Records (OVRS) Death data --- confirmed drug overdose deaths.

2.4. Utah Public Health Laboratory (UPHL) Biosurveillance data --- standardized panel of drug test results gathered from leftover biological specimens obtained from non-fatal drug overdose emergency department visits.

2.5. Bureau of Emergency Medical Services (EMS) and Preparedness EMS data --- drug related and suspect drug overdose EMS events.

3. PERMITTED USES AND DISCLOSURES:

3.1. Recipient shall only access, use, or disclose Data for surveillance, response, planning and/or prevention purposes. The Recipient may not use the Data for any other purpose without prior approval of the Department.

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.

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 or contact 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.

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

3.5. Recipient shall not store, transmit, dispose or access the data outside of the United States.

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 provide aggregated data via the Internal Overdose Dashboard. Data is accessed by an authorized user within San Juan County Public Health Department via user authentication and secure login to the Internal Overdose Dashboard. The individual user securely logs in to the Internal Overdose Dashboard using a Utah Master Directory (UMD) account to access syndromic surveillance data, death data (OME and OVRS), and biosurveillance data. The EMS data is accessed by a separate secure login on the Biospatial platform <https://app.biospatial.io/login >.

5. STORAGE OF THE DATA:

Recipient must obtain Department approval to store data in another location. Recipient shall not store data outside of the United States.

6. SAFEGUARDING THE DATA:

6.1. Only authorized LHD users shall access the Internal Overdose Dashboard. The LHD is responsible to ensure that only authorized LHD users access the Internal Overdose Dashboard and that the Permitted Uses of Internal Overdose Dashboard data specified in section 3. above are followed. The LHD must report security breach or unauthorized use of the data to the Department within three (3) business days of becoming aware of such an incident.

6.2. The recipient shall identify a single point of contact to serve as an Internal Overdose Dashboard Super User. The Super User has the following responsibilities:

6.2.1. Work with the Department to coordinate and set up individual LHD user access to the Internal Overdose Dashboard. Provide the Department with the Super User's name and contact information (phone number and email).

6.2.2. Communicate to the Department in the event that the person serving as the Super User changes. Provide the Department with the new Super User's name and contact information (phone number and email).

6.2.3. Document which LHD users have access to the Internal Overdose Dashboard. The following information shall be maintained for each LHD user with access to the Internal Overdose Dashboard:

6.2.3.1. Name (First and Last)

6.2.3.2. UMD email (this is the email address associated with the LHD user's UMD account.

6.2.3.3. Official work email address

6.2.4. Communicate to the Department immediately when an individual user no longer needs access to the Internal Overdose Dashboard so the Department can remove that users' access.

6.3. The Department shall identify a point of contact to serve as the Internal Overdose Dashboard User Access Contact. The Department Internal Overdose Dashboard Contact has the following responsibilities:

6.3.1. Work, coordinate, and communicate with the LHD Super User to set up individual LHD user access to the Internal Overdose Dashboard.

6.3.2. Work, coordinate, and communicate with the LHD Super User to ensure that the Internal Overdose Dashboard user access list is up to date with the correct LHD users who should have access to the Internal Overdose Dashboard.

6.4. Recipient shall implement and maintain administrative, technical, and physical safeguards necessary to protect the confidentiality 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.

6.5. Recipient shall promptly report 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.

7. 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.

8. 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.

9. TERM AND TERMINATION:

The Agreement is effective upon the signatures of all parties. The term of the agreement is from effective date to August 31, 2030. 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.

10. DISPOSITION OF DATA:

Upon termination of the Agreement, Recipient shall securely return or destroy all data in accordance with reasonable industry standards (e.g. DoD 5220.22, NIST SP 800-88), including any and all copies, compilations, or derivatives in any form or medium, and at any location such information resides. 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.

11. INDEMNIFICATION:

11.1. 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. Neither party waives any rights or defenses otherwise available under the Governmental Immunity Act.

11.2. 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.

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

If to the Department:

Blair Crickmore
Violence and Injury Prevention Program
288 North 1460 West
P.O. Box 142106
Salt Lake City, Utah 84114-2106
385-272-9917
bcrickmore@utah.gov

If to Recipient:

Rebecca Benally
San Juan County Public Health Department
735 South 200 West
Suite 2
Blanding, Utah 84511
435-587-3838
rbenally@sanjuancounty.org

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

For the Department:	For Recipient:
Kyle Lunt (Dec 3, 2025 17:28:39 MST)	Silvia Stubbs (Dec 2, 2025 20:42:19 MST)
Signature	Signature
Kyle Lunt	Silvia Stubbs
Name	Name
Data, Systems & Evaluation director	Commissioner Chair
Title	Title
12/03/2025	12/02/2025
Date	Date