DATA SHARING AGREEMENT
FOR
VITAL STATISTICS
BETWEEN
COWLITZ COUNTY HEALTH & HUMAN SERVICES
AND
COLUMBIA COUNTY ELECTIONS OFFICE

1. Purpose of Agreement. This Data Sharing Agreement (the "**Agreement**") documents the conditions under which Cowlitz County Health & Human Services ("**Health**") shares vital statistics with Columbia County Elections Office (the "**Elections Office**). This Agreement is by and between Health and the Elections Office. The existence of this Agreement is required by the Washington State Department of Health and Chapter 70.58 RCW for Cowlitz County agencies to share this information.

2. Contact Information. The contact information for the Health representative who will send the vital statistic information and the representative of the Elections Office who will receive the vital statistic information is as follows:

Health	Elections
*DaNicia Sheldon	*Don Clark
*Diane Miollis	*Debbie Klug
*Jessica Bischoff	
*Jamie Drake	
*Marie Dang	
*Amanda Foshaug	

3. Definitions. This Agreement hereby incorporates by reference the definitions provided in RCW 70.58A.010.

4. Type of Data Needed and How Data Will Be Used. Health will disclose a person's name, age, date of death, and where the person lived to the Elections Office so that the Elections Office can update its internal records in the performance of its public responsibilities.

5. Methods Used to Protect the Confidentiality and Security of Data.

A. *Confidentiality*

The Elections Office agrees to:

- Follow all Washington State Department of Health guidelines on confidentiality.
- Limit access and use of the information:
  1. To the minimum amount of information.
  2. To the fewest people.
  3. For the least amount of time required to do the work.
- Assure that all people with access to the information understand their responsibilities regarding it.
- Assure that every person (e.g., employee or agent) with access to the information signs and dates a Use and Disclosure of Confidential Information Form before accessing the information.

- Retain a copy of the signed and dated form for each user as long as this Agreement remains in effect.
- Upon request, forward a copy of the signed and dated form for each user to Health or the Washington State Department of Health.

The Elections Office acknowledges the obligations in this section survive completion, cancellation, expiration or termination of this Agreement.

B. *Security*

The Elections Office assures that its security practices and safeguards meet Washington State Office of the Chief Information Officer (OCIO) security standard 141.10 Securing Information Technology Assets.

For the purposes of this Agreement, compliance with the HIPAA Security Standard and all subsequent updates meets OICIO standard 141.10 "Securing Information Technology Assets."

The Elections Office agrees to adhere to the Data Security Requirements in Appendix B.

6. Re-Disclosure of Information. Both Parties agree that the vital statistics data provided under this agreement is confidential and exempt from public disclosure. Accordingly, the Elections Office agrees not to re-disclose the vital statistics data received under this agreement to the general public or other county departments or government agencies.

7. Amendments. This Agreement may be amended by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

8. Termination. The Elections Office acknowledges that unauthorized use or disclosure of the data/information or any other violation of this Agreement may result in the immediate termination of this Agreement. Otherwise, either party may terminate this Agreement upon 30 days prior written notification to the other party. If this Agreement is so terminated, the parties shall be liable only for performance rendered or costs incurred in accordance with the terms of this Agreement prior to the effective date of termination.

9. Governing Law. This Agreement is governed by the laws of the State of Washington.

10. Period of Performance/Effective Date. This Agreement shall be effective from March 1, 2026 through December 31, 2026.

COLUMBIA COUNTY ELECTIONS	COWLITZ COUNTY HEALTH & HUMAN SERVICES
Debbie Klug	Carole Harrison
Debbie Klug, County Clerk	Carole Harrison, Director
Date 2/27/2026	Date 2/27/2026

CONTRACT HAS BEEN APPROVED AS TO
FORM BY COWLITZ COUNTY
PROSECUTING ATTORNEY

APPENDIX A
USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

People with access to the information must sign and date this "Use and Disclosure of Confidential Information Form" (Appendix A) before accessing the information.

The Elections Office must retain a copy of the signed and dated form for each user as the Agreement remains in effect.

People with access to confidential information are responsible for understanding and following the laws, policies, procedures, and practices governing it, as provided in the Agreement. By signing below, the user certifies that he or she has reviewed and will abide by the terms of the Agreement.

Print Name	Don Clack
Signature	
Date	2/27/2026
Email Address	Donald.clack@columbiacountyor.gov
Phone Number	503-397-7214

APPENDIX A
USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

People with access to the information must sign and date this "Use and Disclosure of Confidential Information Form" (Appendix A) before accessing the information.

The Elections Office must retain a copy of the signed and dated form for each user as the Agreement remains in effect.

People with access to confidential information are responsible for understanding and following the laws, policies, procedures, and practices governing it, as provided in the Agreement. By signing below, the user certifies that he or she has reviewed and will abide by the terms of the Agreement.

Print Name	Debbie Klug
Signature	Debbie Klug
Date	2/27/2026
Email Address	Debbie.klug@columbiacountyor.gov
Phone Number	503-397-3796 ext 8442

APPENDIX B
DATA SECURITY REQUIREMENTS

Protection of Data
The Elections Office agrees to store information received under this Agreement (the data) within the United States on one or more of the following media, and to protect it as described below:

A. Passwords
1. Passwords must always be encrypted. When stored outside of the authentication mechanism, passwords must be in a secured environment that is separate from the data and protected in the same manner as the data. For example passwords stored on mobile devices or portable storage devices must be protected as described under section *E. Data storage on mobile devices or portable storage media*.

2. Complex Passwords are:

- At least 8 characters in length.
- Contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.
- Do not contain the user's name, user ID or any form of their full name.
- Do not consist of a single complete dictionary word, but can include a passphrase.
- Changed at least every 120 days.

B. Hard disk drives – Data stored on workstation hard disks:
1. The data must be encrypted as described under section *E. Data storage on mobile devices or portable storage media*. Encryption is not required when Potentially Identifiable Information is stored temporarily on local workstation hard disks. Temporary storage is thirty (30) days or less.

2. Access to the data is restricted to authorized users by requiring logon to the local workstation using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Accounts must lock after 5 unsuccessful access attempts and remain locked for at least 15 minutes, or require administrator reset.

C. Network server and storage area networks (SAN)
1. Access to the data is restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network.

2. Authentication must occur using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Accounts must lock after 5 unsuccessful access attempts, and remain locked for at least 15 minutes, or require administrator reset.

3. The data are located in a secured computer area, which is accessible only by authorized personnel with access controlled through use of a key, card key, or comparable mechanism.

4. If the servers or storage area networks are not located in a secured computer area **or** if the data is classified as Confidential or Restricted it must be encrypted as described under *E. Data storage on mobile devices or portable storage media*.

D. Optical discs (CDs or DVDs)

1. Optical discs containing the data must be encrypted as described under *E. Data storage on mobile devices or portable storage media*.

2. When not in use for the purpose of this Agreement, such discs must be locked in a drawer, cabinet or other physically secured container to which only authorized users have the key, combination or mechanism required to access the contents of the container.

E. Data storage on mobile devices or portable storage media

1. Examples of mobile devices are: smart phones, tablets, laptops, notebook or netbook computers, and personal media players.

2. Examples of portable storage media are: flash memory devices (e.g. USB flash drives), and portable hard disks.

3. The data must not be stored by the Information Recipient on mobile devices or portable storage media unless specifically authorized within the terms of this Agreement. If so authorized:

a) The devices/media must be encrypted with a key length of at least 128 bits, using industry standard mechanisms validated by the National Institute of Standards and Technologies (NIST).

- Encryption keys must be stored in a secured environment that is separate from the data and protected in the same manner as the data.

b) Access to the devices/media is controlled with a user ID and a Complex Password (of at least 6 characters), or a stronger authentication method such as biometrics.

c) The devices/media must be set to automatically wipe or be rendered unusable after no more than 10 failed access attempts.

d) The devices/media must be locked whenever they are left unattended and set to lock automatically after an inactivity activity period of 3 minutes or less.

e) The data must not be stored in the Cloud. This includes backups.

f) The devices/ media must be physically protected by:

- Storing them in a secured and locked environment when not in use;
- Using check-in/check-out procedures when they are shared; and
- Taking frequent inventories.

4. When passwords and/or encryption keys are stored on mobile devices or portable storage media they must be encrypted and protected as described in this section.

F. Backup Media

The data may be backed up as part of Information Recipient's normal backup process provided that the process includes secure storage and transport, and the data is encrypted as described under *E. Data storage on mobile devices or portable storage media.*

G. Paper documents

Paper records that contain data classified as Confidential or Restricted must be protected by storing the records in a secure area which is only accessible to authorized personnel. When not in use, such records is stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

H. Data Segregation

1. The data must be segregated or otherwise distinguishable from all other data. This is to ensure that when no longer needed by the Elections Office, all of the data can be identified for return or destruction. It also aids in determining whether the data has or may have been compromised in the event of a security breach.

2. When it is not feasible or practical to segregate the data from other data, then ***all*** commingled data is protected as described in this Exhibit.

I. Data Disposition

If data destruction is required by the Agreement, the data must be destroyed using the guidelines listed within OCIO Policy 141.10, para 8.3 (Media Handling and Disposal) and NIST 800-88 (Guidelines for Media Sanitization).

J. Notification of Compromise or Potential Compromise

The compromise or potential compromise of the data is reported to the Washington State Department of Health.