# WA-APCD Data Management Plan

Data applicants, pursuant to Washington Administrative Code ([WAC 182-70-220](https://apps.leg.wa.gov/wac/default.aspx?cite=182-70-220)), shall submit a Data Management Plan (hereinafter, “DMP”) to Health Care Authority, the Lead Organization for the Washington All-Payer Claims Database (“WA-APCD”). The DMP is a companion form that accompanies the Data Application. For approved data uses the DMP is incorporated, by exhibit, into the Data Use Agreement.

## Instructions

Any data recipient (hereinafter, the “Recipient”) requesting WA-APCD Data (“WA-APCD Data” or “Data”) must complete and execute this DMP. Any Recipient contractors or agents or third party (each an “Additional Organization”) that are to possess or have access to the Data also must be a signatory to this DMP.

The Recipient is encouraged to refer to the Data Use Agreement when completing this DMP. This DMP must be completed by the Chief Information Security Officer, Chief Privacy Officer, legal counsel or another officer with sufficient knowledge of the Recipient’s, or, as applicable, Additional Organization’s data privacy and security practices and who has the authority to bind the Recipient or Additional Organization.

NOTE: This DMP is confidential and is exempt from public disclosure in accordance with [RCW 42.56.420 (4)](http://app.leg.wa.gov/RCW/default.aspx?cite=42.56.420).

# Section 1. General Information and Certifications

1. **Enter the project title and recipient organization name as they appear on the WA-APCD Data Release Application.**

|  |  |
| --- | --- |
| Project title | Click here to enter text. |
| Recipient organization | Click here to enter text. |

1. **The Recipient and/or Additional Organization certify and agree as follows:**
* The Data will be encrypted at rest on storage media (backup tapes, local hard drives, network storage, et al.) meeting or exceeding FIPS 140-2 standards.
* The Data will be encrypted in transit consistent with the approved method(s) described in this DMP.
* Currently-patched anti-virus software or service is active on any server or endpoint containing the Data, and patches will be applied as soon as they are available from the software vendor and tested.
* If a Covered Entity or Business Associate under Health Insurance Portability and Accountability Act (HIPAA), the Recipient is in compliance with the privacy (45 CFR Part 160 and Subparts A and E of Part 164) and security (45 CFR Part 160 and Subparts A and C of Part 164) requirements of HIPAA; trains all staff who access protected health information (PHI) on the requirements of HIPAA; and has Business Associate Agreements with all non-employees who access PHI if required under HIPAA.
* Whether or not a Covered Entity or Business Associate under HIPAA, the Recipient has policies, procedures and controls, that are in compliance with the recommendations set forth in [NIST Special Publication 800-](http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=904990)66 , in place to address:
	+ The secure sharing, transmission and distribution of confidential information and the secure physical removal, transport and transmission of confidential information
	+ The secure physical possession and storage of confidential information
	+ The secure destruction of confidential information upon the completion of its use
	+ Confidentiality agreements with all individuals, including Additional Organizations, who will access the Data
* Each Recipient and, as applicable, Additional Organization will adopt and comply with Washington State Office of the [Chief Information Officer (OCIO) IT Security Standards 141.10](https://ocio.wa.gov/policy/securing-information-technology-assets-standards) . Remote access to Data by individuals outside the Recipient’s or Additional Organization’s secure network requires the use of Authentication Mechanisms listed below.

**OCIO IT Security Standards 141.10**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Description** | **APCD User Types** | **OCS Data Category Determination** | **Authentication Mechanism Required** |
| Patient Direct Identifiers | Research Org. (IRB Approved) | Category 4 | Multi-factor Authentication\* |
| Proprietary Financial Information | * Gov’t Agencies
* Research Org.
* Lead Org.
 | Category 3 | Multi-factor Authentication\* |
| Indirect Patient Identifiers | * Gov’t Agencies
* Research Org.
* Lead Org.
* Other Entities Per Approval
 | Category 3 | Multi-factor Authentication\* |
| Unique Identifiers | Any Entity Per Approval | Category 2 | Strong, hardened password |
| Other Data | Any Entity Per Approval | Category 2 | Strong, hardened password |

\*Requires use of strong hardened password plus something a user “has” such as hardware token, software token or digital certificate

# Section 2. Responsible Parties

A successful data management plan requires that the appropriate staffing resources are available and trained. In Questions 1-4 below, identify project participants within the Recipient, or, as applicable, the Additional Organization involved in the delineated roles and responsibilities in the management and retention of the WA-APCD Data. As needed, complete “Attachment A: Responsible Parties” to provide the required information for any additional responsible parties.

1. **The individual, and/or Affiliated Organization, responsible for receiving, storing and archiving the Data:**

|  |  |
| --- | --- |
| Name: | Click here to enter text. |
| Agency/Organization: | Click here to enter text. |
| Affiliation: | [ ] Recipient organization [ ] Additional organization |
| Title: | Click here to enter text. |
| Phone: | Click here to enter text. |
| Address: | Click here to enter text. |
| Email: | Click here to enter text. |
| Reports to (name and title): | Click here to enter text. |

1. **The individual(s) responsible, at a minimum, for oversight of use of the Data, including ensuring each authorized Data user: (i) has signed a confidentiality agreement, (ii) accesses and uses only the minimal Data necessary to achieve the approved purpose set forth in the Data Application, (iii) accesses the Data only on a secured server according to Recipient’s, or, as applicable, Additional Organization’s, policies:**

|  |  |
| --- | --- |
| Name: | Click here to enter text. |
| Agency/Organization: | Click here to enter text. |
| Affiliation: | [ ] Recipient organization [ ] Additional organization |
| Title: | Click here to enter text. |
| Phone: | Click here to enter text. |
| Address: | Click here to enter text. |
| Email: | Click here to enter text. |
| Reports to (name and title): | Click here to enter text. |

1. **The individual responsible for notifying the Lead Organization of any breach of the Data Use Agreement or this DMP including any suspected incidents where the security and privacy of the released Data may have been compromised:**

|  |  |
| --- | --- |
| Name: | Click here to enter text. |
| Agency/Organization: | Click here to enter text. |
| Affiliation: | [ ] Recipient organization [ ] Additional organization |
| Title: | Click here to enter text. |
| Phone: | Click here to enter text. |
| Address: | Click here to enter text. |
| Email: | Click here to enter text. |
| Reports to (name and title): | Click here to enter text. |

# Section 2. Responsible Parties

1. **The individual responsible for ensuring the Data are destroyed consistent with the terms of the Data Use Agreement upon termination of the Data Use Agreement, completing the Data Destruction Form and providing that Form to the Lead Organization:**

|  |  |
| --- | --- |
| Name: | Click here to enter text. |
| Agency/Organization: | Click here to enter text. |
| Affiliation: | [ ] Recipient organization [ ] Additional organization |
| Title: | Click here to enter text. |
| Phone: | Click here to enter text. |
| Address: | Click here to enter text. |
| Email: | Click here to enter text. |
| Reports to (name and title): | Click here to enter text. |

# Section 3. Physical Possession and Storage of the Data Files

Note: Storing the Data on a portable device such as a laptop or secure thumb drive is strongly discouraged.

1. **Provide the delivery address for the Data:**

|  |
| --- |
| Organization: Click here to enter text. |
| Street Address: Click here to enter text. |
| City: Click here to enter text. | State: Click here to enter text. | ZIP Code: Click here to enter text. |
| Office Telephone *(Include Area Code)*: Click here to enter text. |
| Secure File Transfer Protocol (SFTP) address if applicable: Click here to enter text. |

1. **Provide the full address, including building and floor, of each location where Data will be delivered and stored:**

|  |
| --- |
| Organization: Click here to enter text. |
| Street Address: Click here to enter text. |
| City: Click here to enter text. | State: Click here to enter text. | ZIP Code: Click here to enter text. |
| Office Telephone *(Include Area Code)*: Click here to enter text. |
| System address if applicable: |

1. **How would you like the WA-APCD Data transferred to your organization?**

☐ SFTP (recommended)

☐ External hard drive with encrypted data (only data de-identified in accordance with 45 CFR 164.514 will be provided using this method). Transmission using PGP encryption and exchange of public keys out of band.

# Section 3. Physical Possession and Storage of the Data Files

1. **Confirm that the Data shall be segregated from other institutional data to ensure that, at the conclusion of the Project, all Data will be destroyed consistent with requirements below and the Data Use Agreement.**

☐ Recipient has data destruction policies, procedures and controls that are in compliance with the recommendations set forth in NIST Special Publication 800-88 Guidelines for Media Sanitization.

 Describe Recipient’s data segregation and destruction processes.

|  |
| --- |
| Click here to enter text. |

Indicate Recipient’s storage method(s) for the WA-APCD Data (check all that apply and answer the corresponding question(s) below.):

☐ Network storage (question 5)

☐ Local hard drive of a computer (question 6)

☐ Cloud storage (question 7)

1. ☐ **Recipient affirms that it shall adhere to the following conditions for Data that is to be stored on a network drive and not on a local hard drive of a computer:**
* Access from within the Recipient’s secure network will be restricted to authorized Data users by requiring computer log-on with unique user accounts and passwords. Access by authorized data users originating outside the Recipient’s secure network will require the use of authentication mechanisms described in Section 2 of this DMP.
* Access will be restricted by limiting folder access to authorized Data users only.
* Any data included in the network backup will be encrypted.
* Storage complies with OCIO 141.10

☐ Not applicable: Data will not be stored on a network drive.

1. ☐ **Recipient affirms that it shall adhere to the following conditions for Data stored on the local hard drive of a computer (a**ny backups of the Data or analytic files will follow all of the requirements listed)**:**
* Access will be restricted to authorized Data users by requiring computer log-on with unique user accounts and passwords provided by the Recipient’s organization. Password complexity rules must be compliant with OCIO 141.10
* When not in use, the computer will be locked in a physically secured office, drawer, cabinet or other container to which access is restricted to authorized Data users.
* When not in use, data will be encrypted with a key length of at least 256 bits.
* Storage complies with OCIO 141.10

☐ Not applicable: Data will not be stored on a local drive of a computer.

# Section 3. Physical Possession and Storage of the Data Files

1. **Recipients are permitted to store or analyze WA-APCD Data using a cloud storage computing environment only if the Data to be stored or analyzed is de-identified in accordance with 45 CFR 164.514 prior to be Data being stored in a cloud computing environment. Skip this question (Section 3, #7) if data request does not include direct identifiers.**

☐ Recipient affirms that the proposed cloud storage computing environment: i) meets or exceeds NIST 800-53v4 security standards at the moderate control level, ii) is HIPAA compliant, and iii) is OCIO 141.10 compliant.

☐ Recipient has attached one or more of the following which are acceptable evidence for demonstrating NIST 800-53v4 compliance (circle all that apply)

* Certification audit against ISO 27001
* Assessment and audit against HIPAA standards
* SSAE 16 Overview
* Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization
* FedRAMP Certification

Other evidence supporting compliance with data security requirements will be considered by the WA-APCD on a case-by-case basis.

1. **For applicants utilizing off-site or cloud providers (other than the WA-APCD data enclave) please specify the name and physical street address of the other data center location(s).**

|  |  |
| --- | --- |
| Site Name | Site Address |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |

1. **Please describe the security procedures, data-storage security and back-up processes in place to ensure the WA-APCD Data will be sufficiently protected via the storage method(s) selected above. The text area below allows for carriage returns for multiple paragraphs.**

|  |
| --- |
| Click here to enter text. |

# Section 3. Physical Possession and Storage of the Data Files

1. **Please provide additional details related to the facilities, hardware and software that will secure the Data.** **The text area below allows for carriage returns for multiple paragraphs.**

|  |
| --- |
| Click here to enter text. |

1. **Please describe the additional physical, administrative, and technical safeguards in place to ensure the privacy and security of the Data. The text area below allows for carriage returns for multiple paragraphs.**

|  |
| --- |
| Click here to enter text. |

1. **Will the Data be housed in a cloud storage computing environment?**

[ ]  No

[ ]  Yes. **If you answered yes**, has this Cloud Service Provider passed a FedRAMP 3PAO assessment *for the specific cloud system which will host the Data?*

[ ]  No

[ ]  Yes. **If you answered yes**, what is the name of the provider *and* the FedRAMP level the specific cloud system hosting the Data is operating at? Click here to enter text.

# Section 4. Data Sharing, Transmission, and Distribution

## Data Encryption

1. **Will all WA-APCD Data at rest be encrypted on storage media (backup tapes, local hard drives, network storage, et al)** meeting or exceeding FIPS 140-2 standards.

☐ Yes

☐ No

If you are sharing information between sites, provide the following information regarding data transmission.

1. **Please identify the data transmission method(s) you plan to use.**

☐ Virtual private network (VPN)

☐ Secure FTP

☐ Other. Please specify and identify how this meets minimum data security requirements:

|  |
| --- |
| Click here to enter text. |

1. **By checking the following statement you are confirming compliance with the following data transfer encryption requirements:**

☐ WA-APCD Data transmission must be encrypted with a key length of at least 256 bits that meets or exceeds FIPS 140-2 standards.

1. **Will WA-APCD Data be transmitted over the Internet?**

☐ No.

☐ Yes. **If you answered yes,** which of the following are used when transmitting the Data over the internet?

☐ SSL (meets or exceeds TLS 1.0)

☐ Secure File Transfer Protocol (SFTP)

☐ Other (please describe): Click here to enter text.

# Section 4. Data Sharing, Transmission, and Distribution

## Information Security (sharing, transmitting, distributing and tracking Data files):

1. **How will authorized Data users access the WA-APCD Data?**

|  |
| --- |
| Click here to enter text. |

1. **How will access to the WA-APCD Data be restricted to only the individuals who require access?**

|  |
| --- |
| Click here to enter text. |

1. **Please provide information about the Recipient’s policies and procedures, or, as applicable, the Additional Organization’s, policies and procedures for sharing, transmitting, distributing and tracking data files.**

|  |
| --- |
| Click here to enter text. |

[ ]  I have attached Information Security policies and procedures.

# Section 4. Data Sharing, Transmission, and Distribution

1. **Has Recipient and/or the Additional Organization been subject to a state or federal regulatory action related to a data breach and has been found in violation and assessed a penalty, been a party to a criminal or civil action relating to a data breach and found guilty or liable for that breach, or had to take action to notify individuals due to a data breach for data maintained by Recipient and/or the Additional Organization or for which the Recipient and/or the Additional Organization was responsible for maintaining in a secure environment in the last five (5) years?**

☐ No

☐ Yes. **If you answered yes,** describe how the breach was resolved and what steps were taken to prevent a recurrence.

|  |
| --- |
| Click here to enter text. |

1. **Has Recipient and/or the Additional Organization violated a data use agreement, nondisclosure agreement or confidentiality agreement in the last three (3) years?**

☐ No

☐ Yes. Provide the facts surrounding the violation or data breach, the cause of the violation or data breach, and all steps taken to correct the violation or data breach and prevent a reoccurrence.

|  |
| --- |
| Click here to enter text. |

# Section 4. Data Sharing, Transmission, and Distribution

## Technical and Physical Safeguards:

1. **All the user accounts for users who log on to any machine (server or endpoint) that accesses the Data are uniquely assigned to individual users and in no circumstances are user accounts shared.**

☐ Yes

☐ No

1. **An audit log is maintained of all user log-ins to the system hosting the WA-APCD Data.**

☐ Yes

☐ No

1. **Minimum password length and character complexity (uppercase, lowercase, numeric, and special characters) in accordance with OCIO Standard 141.10, Section 6.2 (5) is required for passwords used on accounts to log-in on to the system accessing the WA-APCD Data. Please describe the password length and complexity used to access APCD data.**

|  |
| --- |
| Click here to enter text. |

1. **Describe any additional authentication technical security controls employed to defend the system against unauthorized logon (e.g. maximum failed login attempts, or lockout period).**

|  |
| --- |
| Click here to enter text. |

1. **A currently-patched version of a commercial off-the-shelf anti-virus or anti-malware product (e.g., McAfee, Symantec, Microsoft) will run on the server, or any computing device, that will host the WA-APCD Data.**

☐ Yes

# Section 4. Data Sharing, Transmission, and Distribution

1. **If the WA-APCD Data will be on a server or network accessible storage drive, then check all the security features present in the secure location containing WA-APCD Data:**

[ ]  Recorded video surveillance on a digital system

[ ]  Access log of all individuals entering the room and documentation of all actions taken while in the room.

[ ]  Secure server rack

[ ]  Access control limiting access only to authorized individuals

1. **What additional specific physical or technical safeguards (not mentioned in prior answers) will be used to *mitigate* the risk of unauthorized access to WA-APCD Data?**

|  |
| --- |
| Click here to enter text. |

1. **What policies and procedures are in place for physical removal and transport of Data files?**

|  |
| --- |
| Click here to enter text. |

# Section 4. Data Sharing, Transmission, and Distribution

1. **In the box below, enter (i) the date of the last information security risk assessment performed at the location where Data will be stored and used, (ii) the name of the assessor who conducted it; and (iii) briefly describe the outcome and any mitigation related to the outcome.**

|  |
| --- |
| Click here to enter text. |

1. **In the box below, enter (i) the date of the last IT audit performed, (ii) the name of the auditor who conducted it, and (iii) briefly describe the outcome and any mitigation related to the outcome.**

|  |
| --- |
| Click here to enter text. |

1. **Describe your administrative, technical, and physical safeguards in place for the auditing for all access to WA-APCD data.**

|  |
| --- |
| Click here to enter text. |

# Section 5. Internal Review

1. **In the box below, (i) describe your internal process for reviewing and approving this DMP within your organization and (ii) list the names and positions of the senior personnel who reviewed and/or approved this DMP.**

|  |
| --- |
| Click here to enter text. |

1. **Do you plan to initiate any periodic updates to this DMP during the Data Use Agreement period?**

☐ Yes

☐ No

# Section 6. Completion of Project Tasks and Data Destruction

The Recipient, or, as applicable, the Additional Organization attests that the WA-APCD Data and all copies of the WA-APCD Data used by the Recipient (or its employees) or, as applicable, the Additional Organization, will be destroyed within 10 business days upon Project Completion (as set forth in the Data Application) or termination of the Data Use Agreement, whichever is earlier. All Data destruction must conform to the recommendations set forth in NIST Special Publication 800-88 Guidelines for Media Sanitization and to the Data Use Agreement.

1. **Describe the process to complete the Certificate of Project Completion and Data Destruction form.**

|  |
| --- |
| Click here to enter text. |

# Section 6. Completion of Project Tasks and Data Destruction

1. **Describe your policies and procedures to:**
	* Dispose of WA-APCD Data and Data files upon completion of the Project;
	* Protect the WA-APCD Data and Data files when Recipient staff members of project teams (as well as collaborating Additional Organizations) terminate their participation in the Project (this may include staff exit interviews and immediate termination of Data access);
	* Process to inform the Lead Organization of project staffing changes, including when individual staff members' participation in projects is terminated, voluntarily or involuntarily, within twenty-one calendar days of the staffing change; and
	* Process to ensure that the WA-APCD Data and any derivatives or parts thereof are not used following the completion of the project

|  |
| --- |
| Click here to enter text. |

# Attestation

By submitting this DMP, the Recipient, and/or, as applicable, the Additional Organization, attests that it has evaluated all applicable state privacy and security laws and regulations as set forth in [RCW Chapter 43.371](https://apps.leg.wa.gov/RCW/default.aspx?cite=43.371), WAC [Chapter 182-70](https://apps.leg.wa.gov/wac/default.aspx?cite=182-70) and the Washington State Office of the [Chief Information Officer (OCIO) IT Security Standards 141.10](https://ocio.wa.gov/policy/securing-information-technology-assets-standards) and, as applicable, the privacy and security standards set forth in the federal Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA) *and* confirms that it is compliant with such use, privacy and security standards.

The Recipient or, as applicable, the Additional Organization, agrees and understands that it is solely responsible for any breaches or unauthorized access, disclosure or use of WA-APCD Data, including, but not limited to, any breach or unauthorized access, disclosure or use by its employees or Additional Organization. The Recipient or, as applicable, the Additional Organization, further agrees that every authorized Data user has received training on the proper handling of protected health information and/or personal data (including cyber security awareness training) within the last year or will have received this training by the time the Data is released.

By signature below, Recipient, and/or, as applicable, the Additional Organization, attest: (1) to the accuracy of the information provided herein; (2) that the Recipient, or, as applicable, the Additional Organization, agrees to hold and/or access WA-APCD Data at all times in compliance with all provisions of this DMP and the Data Use Agreement; and (3) that Recipient, or, as applicable, the Additional Organization, has authority to bind the Recipient, or, as applicable, the Additional Organization, undersigned as an authorized signatory of the Recipient, or, as applicable, the Additional Organization.

|  |  |
| --- | --- |
| **Signature of authorized signatory:** |  |
| **Printed name:** | Click here to enter text. |
| **Title:** | [ ] Recipient organization [ ] Additional organization |
| **Organization:** | Click here to enter text. |
| **Affiliation:** | Click here to enter text. |
| **Date:** | Click here to enter a date. |

|  |  |
| --- | --- |
| **Signature of authorized signatory:** |  |
| **Printed name:** | Click here to enter text. |
| **Title:** | [ ] Recipient organization [ ] Additional organization |
| **Organization:** | Click here to enter text. |
| **Affiliation:** | Click here to enter text. |
| **Date:** | Click here to enter a date. |

# Attachment A: Responsible Parties

Attachment A provides space to identify additional project participants within the Recipient, or, as applicable, the Additional Organization involved in the delineated roles and responsibilities in the management and retention of the WA-APCD Data.

1. **The individual, and/or Affiliated Organization, responsible for receiving, storing and archiving the Data:**

|  |  |
| --- | --- |
| Name: | Click here to enter text. |
| Agency/Organization: | Click here to enter text. |
| Affiliation: | [ ] Recipient organization [ ] Additional organization |
| Title: | Click here to enter text. |
| Phone: | Click here to enter text. |
| Address: | Click here to enter text. |
| Email: | Click here to enter text. |
| Reports to (name and title): | Click here to enter text. |

1. **The individual(s) responsible, at a minimum, for oversight of use of the Data, including ensuring each authorized Data user: (i) has signed a confidentiality agreement, (ii) accesses and uses only the minimal Data necessary to achieve the approved purpose set forth in the Data Application, (iii) accesses the Data only on a secured server according to Recipient’s, or, as applicable, Additional Organization’s, policies:**

|  |  |
| --- | --- |
| Name: | Click here to enter text. |
| Agency/Organization: | Click here to enter text. |
| Affiliation: | [ ] Recipient organization [ ] Additional organization |
| Title: | Click here to enter text. |
| Phone: | Click here to enter text. |
| Address: | Click here to enter text. |
| Email: | Click here to enter text. |
| Reports to (name and title): | Click here to enter text. |

1. **The individual responsible for notifying the Lead Organization of any breach of the Data Use Agreement or this DMP including any suspected incidents where the security and privacy of the released Data may have been compromised:**

|  |  |
| --- | --- |
| Name: | Click here to enter text. |
| Agency/Organization: | Click here to enter text. |
| Affiliation: | [ ] Recipient organization [ ] Additional organization |
| Title: | Click here to enter text. |
| Phone: | Click here to enter text. |
| Address: | Click here to enter text. |
| Email: | Click here to enter text. |
| Reports to (name and title): | Click here to enter text. |

1. **The individual responsible for ensuring the Data are destroyed consistent with the terms of the Data Use Agreement upon termination of the Data Use Agreement, completing the Data Destruction Form and providing that Form to the Lead Organization:**

|  |  |
| --- | --- |
| Name: | Click here to enter text. |
| Agency/Organization: | Click here to enter text. |
| Affiliation: | [ ] Recipient organization [ ] Additional organization |
| Title: | Click here to enter text. |
| Phone: | Click here to enter text. |
| Address: | Click here to enter text. |
| Email: | Click here to enter text. |
| Reports to (name and title): | Click here to enter text. |