Chapter 182-70 WAC
ALL PAYER HEALTH CARE CLAIMS DATABASE

Last Update: 8/26/21

WAC

DISPOSITION OF SECTIONS FORMERLY CODIFIED IN THIS CHAPTER

182-70-660 Final decision. [WSR 19-24-090, recodified as § 182-70-660, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-660, filed

7/5/18, effective 8/5/18.] Repealed by WSR 21-11-039, filed 5/12/21, effective 6/12/21. Statutory Authority: RCW 41.05.021, 41.05.160, 43.71C.110, and 2019 c 334.

ALL PAYER HEALTH CARE CLAIMS DATABASE

WAC 182-70-010 Purpose. (1) Chapter 43.371 RCW establishes the framework for the creation and administration of a statewide all-payer health care claims database.

(2) RCW 43.371.020 directs the health care authority to establish a statewide all-payer health care claims database to support transparent public reporting of health care information. The authority shall select a lead organization to coordinate and manage the database. The lead organization shall also contract with a data vendor to perform data collection, processing, aggregation, extracts, and analytics.

(3) RCW 43.371.070 mandates that the director of the health care authority adopt rules necessary to implement chapter 43.371 RCW. In addition, RCW 43.371.010 and 43.371.050 direct the adoption of specific rules by the director.

(4) The purpose of this chapter is to implement chapter 43.371 RCW, to facilitate the creation and administration of the Washington statewide all-payer health care claims database.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-010, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-010, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-010, filed 1/29/16, effective 2/29/16.]

WAC 182-70-020 Definitions required by chapter 43.371 RCW. The following definitions apply throughout this chapter unless the context clearly indicates another meaning.

"Allowed amount" means the maximum dollar amount contractually agreed to for an eligible health care service covered under the terms of an insurance policy, health benefits plan or state labor and industries program.

"Billed amount" means the dollar amount charged for a health care service rendered.

"Claim file" means a data set composed of health care service level remittance information for all nondenied adjudicated claims under the terms of an insurance policy, health benefits plan or state labor and industries program including, but not limited to, covered medical services files, pharmacy files and dental files.

"Covered medical services file" means a data set composed of service level remittance information for all nondenied adjudicated claims for Washington covered persons that are authorized under the terms of an insurance policy, health benefits plan or state labor and industries program including, but not limited to, member demographics, provider information, charge and payment information including facility fees, clinical diagnosis codes and procedure codes.

"Data file" means a data set composed of member or provider information including, but not limited to, member eligibility and enrollment data and provider data with necessary identifiers.

"Dental claims file" means a data set composed of service level remittance information for all nondenied adjudicated claims for dental

services for Washington covered persons including, but not limited to, member demographics, provider information, charge and payment information including facility fees, and current dental terminology codes as defined by the American Dental Association.

"Member eligibility and enrollment data file" means a data set containing data about Washington covered persons who receive health care coverage from a payer for one or more days of coverage during the reporting period including, but not limited to, subscriber and member identifiers, member demographics, plan type, benefit codes, and enrollment start and end dates.

"Paid amount" means the dollar amount paid for a health care service rendered under the terms of an insurance policy, health benefits plan or state labor and industries program for covered services, excluding member copayments, coinsurance, deductibles and other sources of third-party payment. This dollar amount includes incentive payments that are captured in the claims financial fields in the *WA-APCD Data Submission Guide;* such incentive payments include, but are not limited to, withholds, shared savings payments, case or episode payments, and pay-for-performance amounts. For capitated services the fee-for-service equivalent is to be reported as the paid amount.

"Pharmacy claims file" means a data set containing service level remittance information for all nondenied adjudicated claims for pharmacy services for Washington covered persons including, but not limited to, enrolled member demographics, provider information, charge and payment information including dispensing fees, and national drug codes.

"Provider data with necessary identifiers" means a data file containing information about health care providers that submitted claims for providing health care services, equipment or supplies, to subscribers or members and such other data as required by the data submission guide.

[WSR 19-24-090, recodified as § 182-70-020, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.050(6) and chapter 43.371 RCW. WSR 17-22-121, § 82-75-020, filed 10/31/17, effective 12/1/17. Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-020, filed 1/29/16, effective 2/29/16.]

WAC 182-70-030 Additional definitions authorized by chapter 43.371 RCW. The following additional definitions apply throughout this chapter unless the context clearly indicates another meaning.

"Authority" means the Washington state health care authority.

"Capitation payment" means a payment model where providers receive a payment on a per "covered person" basis, for specified calendar periods, for the coverage of specified health care services regardless of whether the patient obtains care. Capitation payments include, but are not limited to, global capitation arrangements that cover a comprehensive set of health care services, partial capitation arrangements for subsets of services, and care management payments.

"Claim" means a request or demand on a carrier, third-party administrator, or the state labor and industries program for payment of a benefit.

"Claimant" means a person who files a workers compensation claim with the Washington state department of labor and industries.

"Coinsurance" means the percentage or amount an enrolled member pays towards the cost of a covered service.

"Copayment" means the fixed dollar amount a member pays to a health care provider at the time a covered service is provided or the full cost of a service when that is less than the fixed dollar amount.

"Data management plan" or "DMP" means a formal document that outlines how a data requestor will handle the WA-APCD data to ensure privacy and security both during and after the project.

"Data policy committee" or "DPC" is the advisory committee required by RCW 43.371.020 (5)(h) to provide advice related to data policy development.

"Data release committee" or "DRC" is the advisory committee required by RCW 43.371.020 (5)(h) to establish a data release process and to provide advice regarding formal data release requests.

"Data submission guide" means the document that contains data submission requirements including, but not limited to, required fields, file layouts, file components, edit specifications, instructions and other technical specifications.

"Data use agreement" or "DUA" means the legally binding document signed by either the lead organization and the data requestor, or the authority and the data requestor, or the authority and a Washington state agency, that defines the terms and conditions under which access to and use of the WA-APCD data is authorized, how the data will be secured and protected, and how the data will be destroyed at the end of the agreement term.

"Days" means calendar days.

"Deductible" means the total dollar amount an enrolled member pays on an incurred claim toward the cost of specified covered services designated by the policy or plan over an established period of time before the carrier or third-party administrator makes any payments under an insurance policy or health benefit plan.

"Director" means the director of the health care authority.

"Fee-for-service equivalent" means the amount that would have been paid by the payer for a specified service if the service had not been capitated or paid under an alternative payment formula like treatment episodes, or the fee amount reflected in the payer's internal fee schedule(s) for services that are not paid on a fee-for-service basis.

"Fee-for-service payment" means a payment model where providers receive a negotiated or payer-specified rate for a specific health care service provided to a patient.

"Health benefits plan" or "health plan" has the same meaning as in RCW 48.43.005.

"Health care" means care, services, or supplies related to the prevention, cure or treatment of illness, injury or disease of an individual, which includes medical, pharmaceutical or dental care. Health care includes, but is not limited to:

(a) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(b) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

"Lead organization" means the entity selected by the health care authority to coordinate and manage the database as provided in chapter 43.371 RCW.

"Malicious intent" means the person acted willfully or intentionally to cause harm, without legal justification.

"Member" means a person covered by a health plan including an enrollee, subscriber, policyholder, beneficiary of a group plan, or individual covered by any other health plan.

"Person" means an individual; group of individuals however organized; public or private corporation, including profit and nonprofit corporations; a partnership; joint venture; public and private institution of higher education; a state, local, and federal agency; and a local or tribal government.

"PFI" means the proprietary financial information as defined in RCW 43.371.010(12).

"PHI" means protected health information as defined in the Health Insurance Portability and Accountability Act (HIPAA). Incorporating this definition from HIPAA, does not, in any manner, intend or incorporate any other HIPAA rule not otherwise applicable to the WA-APCD.

"Subscriber" means the insured individual who pays the premium or whose employment makes him or her eligible for coverage under an insurance policy or member of a health benefit plan.

"WA-APCD" means the statewide all payer health care claims database authorized in chapter 43.371 RCW.

"WA-APCD program director" means the individual designated by the authority as responsible for the oversight and management of the operations of the statewide all payer health care claims database authorized in chapter 43.371 RCW.

"Washington covered person" means any eligible member and all covered dependents where the covered person is a Washington state resident, or the state of Washington has primary jurisdiction, and whose laws, rules and regulations govern the members' and dependents' insurance policy or health benefit plan.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-030, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-030, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.010(3) and 43.371.070. WSR 19-05-054, § 82-75-030, filed 2/15/19, effective 3/18/19; WSR 18-19-056, § 82-75-030, filed 9/15/18, effective 10/16/18. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-030, filed 7/5/18, effective 8/5/18. Statutory Authority: RCW 43.371.050(6) and chapter 43.371 RCW. WSR 17-22-121, § 82-75-030, filed 10/31/17, effective 12/1/17. Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-030, filed 4/4/17, effective 5/5/17; WSR 16-22-062, § 82-75-030, filed 11/1/16, effective 12/2/16; WSR 16-04-068, § 82-75-030, filed 1/29/16, effective 2/29/16.]

WAC 182-70-040 Registration requirements. (1) **Washington covered persons threshold for data suppliers.** Any carrier, third-party administrator, public program, or other potential data supplier identified in RCW 43.371.030 with 1000 or more Washington covered persons, as defined in WAC 182-70-030, as of December 31st of the previous calendar year must submit data in accordance with this chapter.

(a) For the purposes of determining whether a potential data supplier is subject to the requirements of this chapter, potential data suppliers must aggregate the number of Washington covered persons for all companies at the group code level, as defined by the National Association of Insurance Commissioners.

(b) Potential data suppliers that offer any combination of medical, dental, or pharmaceutical benefits under separate or combined

plans must count all Washington covered persons, regardless of the comprehensiveness of the plan, toward the 1000 Washington covered persons threshold.

(2) **Initial registration.** Each data supplier required to submit health care data pursuant to chapter 43.371 RCW must register within thirty days of notification from the lead organization.

(3) **Annual registration.** Each data supplier required to submit health care data pursuant to chapter 43.371 RCW must register by December 31st of each year after the initial registration. If the data supplier initially registers September 1st or later, then the data supplier must file its annual registration by December 31st of the year following the year of the initial registration.

(4) Each data supplier newly required to submit health care data under chapter 43.371 RCW, either by a change in law or loss of qualified exemption, must register with the lead organization within thirty days of being required to submit data.

[Statutory Authority: RCW 41.05.021 and 41.05.160. WSR 21-18-057, § 182-70-040, filed 8/26/21, effective 9/26/21. WSR 19-24-090, recodified as § 182-70-040, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-040, filed 1/29/16, effective 2/29/16.]

WAC 182-70-050 Data submission schedule. (1) Data suppliers shall submit the required health care data in accordance with the schedule provided in this section.

(2) **Test file.**

(a) At least sixty calendar days prior to the data suppliers' first required submission, the lead organization will notify the data supplier in writing regarding the obligation to file. The lead organization will schedule time to work with the data supplier to establish a schedule for when the data supplier shall submit the initial test files.

(b) No more than ninety calendar days after notification of changes in requirements in the data submission guide, the data supplier shall submit initial test files. This deadline may be extended by the lead organization when it determines that additional time will be needed in order for the change to be implemented.

(3) **Submission file.** Data and claim files shall be submitted to the WA-APCD on a quarterly basis. On or before April 30th, July 31st, October 31st and January 31st of each year, data and claim files shall be submitted for all nondenied adjudicated claims paid in the preceding three months.

(4) **Resubmission file.** Failure to conform to the requirements of this chapter or the data submission guide shall result in the rejection of the applicable data and claim files. The lead organization shall notify the data supplier when data and claim files are rejected. All rejected files must be resubmitted in the appropriate, corrected format within fifteen business days of notification unless a written request for an extension is received by the lead organization before the expiration of this fifteen business day period.

(5) **Claims run-out file.** If health care coverage is terminated for a Washington covered person, the data supplier shall submit data for a six month period following the health care coverage termination date.

(6) **Replacement file.**

(a) A data supplier may replace a complete data file, claim file or both data and claim file submission. Requests must be made to the lead organization with a detailed explanation as to why the replacement is needed. The lead organization shall make a recommendation to the authority as to whether to approve or deny the request. The approval recommendation shall also state whether the approval is for the entire period requested or for a period less than requested.

(b) The authority shall approve or deny the request and provide written notification to the requestor within thirty calendar days of receipt of the request. The authority decision on the request for a replacement file will be provided in writing. If the authority does not approve the complete request for a replacement file, the written notification will include the reason for the denial or approval of the shorter period of time.

(c) Requests may not be made more than one year after the end of the month in which the file was submitted unless the data supplier can establish exceptional circumstances for the replacement. The lead organization may recommend approval and the authority may approve a request for more than one year for exceptional circumstances. The authority shall approve or deny the request using the process set forth in (b) of this subsection.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-050, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-050, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-050, filed 1/29/16, effective 2/29/16.]

WAC 182-70-060 Historical data submission. (1) The purpose of collecting historical data into the WA-APCD is to permit the systematic analysis of the health care delivery system including evaluation of the effectiveness of the Patient Protection and Affordable Care Act signed into law on March 23, 2010.

(2) The lead organization will provide written notification to the data suppliers when the WA-APCD is ready to accept the submission of historical data. Data suppliers shall submit the historical data within sixty days of notification. Requests for an extension of time to submit historical data shall be made in accordance with WAC 182-70-080(3).

(3) "Historical data" means covered medical services claim files, pharmacy claim files, dental claim files, member eligibility and enrollment data files, and provider data files with necessary identifiers for the period January 1, 2013, through December 31, 2016, or through the end of the quarter immediately prior to the first regular quarterly submission due in accordance with the data submission schedule.

(4) The authority may grant an exception to this section and approve the filing of historical data for a period less than the period specified in subsection (3) of this section. Requests for an exception under this subsection shall be made to the lead organization within fifteen calendar days of being notified in accordance with subsection (2) of this section. The lead organization shall make a recommendation to the authority as to whether to approve or deny the request. The authority may approve the request for good cause.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-060, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-060, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 17-05-024, § 82-75-060, filed 2/7/17, effective 3/10/17; WSR 16-04-068, § 82-75-060, filed 1/29/16, effective 2/29/16.]

WAC 182-70-070 Data submission guide. (1) Data files and claim files shall be submitted to the WA-APCD in accordance with the requirements set forth in this chapter and the data submission guide.

(2) The lead organization shall develop the data submission guide with input from stakeholders. The lead organization shall develop a process to allow for stakeholder review and comment on drafts of the data submission guide and all subsequent changes to the guide. The authority shall have final approval authority over the data submission guide and all subsequent changes.

(3) The lead organization shall notify data suppliers before changes to the data submission guide are final. Notification shall occur no less than one hundred twenty calendar days prior to the effective date of any change.

(4) Upon good cause shown, data suppliers may be granted an extension to comply with any changes to the data submission guide. Requests for extensions or exceptions shall be made in accordance with WAC 182-70-080.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-070, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-070, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-070, filed 1/29/16, effective 2/29/16.]

WAC 182-70-080 Waivers and extensions. (1) The authority may grant a waiver of reporting requirements or an extension of time to a reporting requirement deadline based on extenuating circumstances.

(2) **Waivers.**

(a) A data supplier may request a waiver from submission for a period of time due to extenuating circumstances affecting the data supplier's ability to comply with the reporting requirement for that period.

(b) The request shall be for no more than one reporting year and shall contain a detailed explanation as to the reason the data supplier is unable to meet the reporting requirements.

(c) A request for a waiver must be submitted to the lead organization at least sixty calendar days prior to the applicable reporting deadline. The lead organization shall make a recommendation to the authority as to whether to approve or deny the request. The approval recommendation shall also state whether the approval is for the entire period requested or for a period less than requested.

(d) The authority may approve a request for extenuating circumstances. Approval may be for a time period shorter than requested. The authority shall approve or deny the request and provide written notification to the requester within thirty calendar days of receipt of the request. The authority decision on the request for a waiver will be provided in writing. If the authority does not approve a request

for a waiver, the written notification will include the reason for the denial.

(3) **Extensions.**

(a) A data supplier may request an extension of time for submitting a quarterly report or the resubmission of a report due to extenuating circumstances affecting the data supplier's ability to submit the data by the deadline.

(b) The request shall be for no more than one reporting quarter and shall contain a detailed explanation as to the reason the data supplier is unable to meet the reporting requirements for that quarter.

(c) A request for an extension must be submitted to the lead organization at least thirty calendar days prior to the applicable reporting deadline unless the requestor is unable to meet this deadline due to circumstances beyond the data supplier's control. If unable to meet this deadline, the data supplier shall notify the lead organization in writing as soon as the data supplier determines that an extension is necessary.

(d) The lead organization shall make a recommendation to the authority as to whether to approve or deny the request. The approval recommendation shall also state whether the approval is for the entire period requested or for a period less than requested.

(e) The authority may approve a request for extenuating circumstances. The authority shall approve or deny the request and provide written notification to the requestor within fifteen calendar days from when the lead organization receives the request from the data supplier. The authority decision on the request for an extension will be provided in writing. If the authority does not approve a request for an extension, the written notification will include the reason for the denial.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-080, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-080, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-080, filed 1/29/16, effective 2/29/16.]

WAC 182-70-090 Penalties for failure to comply with reporting requirements. (1) The authority may assess fines for failure to comply with the requirements of this chapter including, but not limited to:

(a) General reporting requirements.

(b) Health care claim files and data files requirements.

(c) Health care claim files and data files submission requirements.

The authority will not assess fines when the data supplier is working in good faith with the lead organization to comply with the reporting requirements.

(2) Unless the authority has approved a waiver or extension, the authority may assess a fine for failure to comply with general reporting requirements including, but not limited to, the following occurrences:

(a) Failure to submit health care claim files or data files for a required line of business; and

(b) Submitting health information for an excluded line of business.

(3) Unless the authority has approved a waiver or extension, the authority may assess a fine for failure to comply with health care claim file or data file requirements including, but not limited to, the following occurrences:

(a) Submitting a health care claim or data file in an unapproved layout;

(b) Submitting a data element in an unapproved format;

(c) Submitting a data element with unapproved coding; and

(d) Failure to submit a required data element.

(4) Unless the authority has approved a waiver or extension, the authority may assess a fine for failure to comply with health care claim file or data file submission requirements including, but not limited to, the following occurrences:

(a) Failure to comply with WAC 182-70-050 (Data submission schedule);

(b) Rejection of a health care claim or data file by the data vendor that is not corrected by the data supplier; and

(c) Transmitting health care claim or data files using an unapproved process.

(5) Upon the failure to comply with a reporting requirement in this chapter, the authority shall first issue a warning notice to a data supplier. The warning notice shall set forth the nature of the failure to comply and offer to provide assistance to the data supplier to correct the failure.

(6) A data supplier that fails to comply with the same reporting requirement in this chapter for which it previously received a warning notice, may be assessed a penalty of two hundred fifty dollars per day, not to exceed a maximum of twenty-five thousand dollars per occurrence. Each failure to comply with a reporting requirement for a reporting period is considered a separate occurrence.

(7) For good cause shown, the authority may suspend in whole or in part any fine assessed in accordance with this section.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-090, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-090, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-090, filed 1/29/16, effective 2/29/16.]

WAC 182-70-100 Administrative review. (1) Data suppliers may request an administrative review of an authority decision to deny a request for an extension or waiver, or an assessment of a fine.

(2) A request for an administrative review may be initiated by a written petition filed with the authority within thirty calendar days after notice of the denial or assessment of a fine. The petition shall include the following information:

(a) Data supplier's name, address, telephone number, email address and contact person.

(b) Information about the subject of the appeal including remedy requested.

(c) A detailed explanation as to the issue or area of dispute, and why the dispute should be decided in the data supplier's favor.

(3) The petition and all materials submitted will be reviewed by the director or director's designee. The reviewing official may request additional information or a conference with the data supplier. A decision from the reviewing official shall be provided in writing to

the data supplier no later than thirty calendar days after receipt of the petition. A denial of the petition will include the reasons for the denial.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-100, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-100, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-100, filed 1/29/16, effective 2/29/16.]

WAC 182-70-110 Appeals. A data supplier may request an appeal of a denial of its administrative review conducted in accordance with WAC 182-70-100. See WAC 182-526-0205.

[Statutory Authority: RCW 41.05.021, 41.05.160, 43.71C.110, and 2019 c 334. WSR 21-11-039, § 182-70-110, filed 5/12/21, effective 6/12/21. Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-110, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-110, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-110, filed 1/29/16, effective 2/29/16.]

DATA REQUESTS AND RELEASE PROCEDURES

WAC 182-70-200 General data request and release procedures. (1) The lead organization must adopt clear policies and procedures for data requests and data release. At a minimum, the lead organization, in coordination with the data vendor, must develop procedures for making a request for data, how data requests will be reviewed, how decisions will be made on whether to grant or disapprove release of the requested data, and data release processes. The policies and procedures must be approved by the authority.

(2) The lead organization should help data requestors identify the best ways to describe and tailor the data request, understand the privacy and security requirements, and understand the limitations on use and data products derived from the data released.

(3) The lead organization must maintain a log of all requests and action taken on each request. The log must include at a minimum the following information: Name of requestor, data requested, purpose of the request, whether the request was approved or denied, if approved the date and data released, and if denied the date and reason for the denial. The lead organization shall post the log on the WA-APCD website that the lead organization is required to maintain.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-200, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-200, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-200, filed 11/1/16, effective 12/2/16.]

WAC 182-70-210 Procedures for data requests. (1) The lead organization must use an application process for data requests.

(2) In addition to the requirements in RCW 43.371.050(1), at a minimum, the application must require the following information:

(a) Detailed information about the project for which the data is being requested including, but not limited to:

(i) Purpose of the project and data being requested, and level of detail for the data requested.

(ii) Methodology for data analysis and timeline for the project.

(iii) If applicable, copy of an Institutional Review Board (IRB) protocol and approval or Exempt Determination and application for the IRB exemption for the project review. Researchers must use an IRB that has been registered with the United States Department of Health and Human Services Office of Human Research Protections. The IRB may however be located outside the state of Washington.

(iv) Staffing qualifications and resumes.

(v) Information on third-party organizations or individuals who may have access to the requested data as part of the project for which the data is requested. The information provided must include the same information required by the requestor, as applicable. Data cannot be shared with third parties except as approved in a data request.

(b) Information regarding whether the requestor has, within the three years prior to the data request date, violated a data use agreement, nondisclosure agreement or confidentiality agreement. Such information must include, but not be limited to, 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.

(c) Information regarding whether the requestor has, within the five years prior to the data request date, 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 the data requestor or for which the data requestor was responsible for maintaining in a secure environment.

(d) Submittal of the project's data management plan (DMP), which DMP must include the information required in WAC 182-70-220.

(e) Require all recipients of protected health information (PHI) to provide an attestation from an authorized individual that the recipient of the requested data has data privacy and security policies and procedures in place on the date of the request and will maintain these policies and procedures for the project period, these policies and procedures comply with Washington state laws and rules, and meet the standards and guidelines required by the Washington state office of chief information officer. Data recipients must also attest that recipients will provide copies of the data privacy and security policies and procedures upon request by the lead organization.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-210, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-210, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-210, filed 11/1/16, effective 12/2/16.]

WAC 182-70-220 Data management plan. (1)(a) The lead organization must require data requestors to submit data management plans with

the data request application. Data management plans must comply with the Washington state office of chief security officer standards.

(b) Additional organizations that are involved in using the data in the data requestors' projects must also provide the information required in the data management plan for their organizations.

(2) Data management plans must provide detailed information including, but not limited to, the following:

(a) Physical possession and storage of the data files, including details about the third-party vendor and personnel handling the data; the facilities, hardware and software that will secure the data; and the physical, administrative and technical safeguards in place to ensure the privacy and security of the released data.

(b) Data sharing, electronic transmission and distribution, including the data requestor's policies and procedures for sharing, transmitting, distributing and tracking data files; physical removal and transport of data files; staff restriction to data access; and use of technical safeguards for data access (e.g., protocols for passwords, log-on/log-off, session time out and encryption for data in motion and at rest).

(c) Data reporting and publication, including who will have the main responsibility for notifying the lead organization of any suspected incidents where the security and privacy of the released data may have been compromised; how DMPs are reviewed and approved by the data requestor; and whether the DMPs will be subjected to periodic updates during the DUA period for the released data.

(d) Completion of project tasks and data destruction, including the data requestor's process to complete the certificate of destruction form and the policies and procedures to:

(i) Dispose of WA-APCD data files upon completion of its project.

(ii) Protect the WA-APCD data files when staff members of project teams (as well as collaborating organizations) terminate their participation in projects. This may include staff exit interviews and immediate termination of data access.

(iii) 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.

(iv) Ensure that the WA-APCD data and any derivatives or parts thereof are not used following the completion of the project.

[WSR 19-24-090, recodified as § 182-70-220, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-220, filed 11/1/16, effective 12/2/16.]

WAC 182-70-230 Review of data requests. (1) The lead organization must establish a transparent process for the review of data requests, which includes a process for public review for specific requests. The process must include a timeline for processing requests, and notification procedures to keep the requestor updated on the progress of the review. The process must also include the ability for the public to comment on requests that include the release of protected health information or proprietary financial information or both. The authority shall have final approval over the process and criteria used for review of data requests and all subsequent changes.

(2) The lead organization must post on the WA-APCD website all requests that include the release of protected health information or

proprietary financial information, and the schedule for the receipt of public comment on the request. The time frame for public comment should not be less than fourteen calendar days. The lead organization must post the final decision for the request within seven days after the decision is made.

(3) The lead organization has the responsibility to convene the DRC when needed to review data requests and make a recommendation to the lead organization as to whether to approve or deny a data request. The lead organization must establish an annual meeting schedule for DRC and post the schedule on the website. The DRC must review requests for identifiable data and provide a recommendation regarding data release. The lead organization may request the DRC to review other data requests. The review must include a technical review of the data management plan by an expert on the DRC, staff from the office of chief information officer, or other technical expert. The DRC may recommend that the requestor provide additional information before a final decision can be rendered, approve the data release in whole or in part, or deny the release. For researchers who are required in RCW 43.371.050 (4)(a) to have IRB approval, the DRC may recommend provisional approval subject to the receipt of an IRB approval letter and protocol and submittal of a copy of the IRB letter to the lead organization.

(4) The lead organization may only deny a data request based on a reason set forth in WAC 182-70-280.

(5) The lead organization must notify the requestor of the final decision. The notification should include the process available for review or appeal of the decision.

(6) The lead organization must post all data requests and final decisions on the WA-APCD website maintained by the lead organization.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-230, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-230, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-230, filed 11/1/16, effective 12/2/16.]

WAC 182-70-240 Data release. (1) Upon approval of a request for data, the lead organization must provide notice to the requestor. The notice must include the following:

(a) The data use agreement (DUA). The DUA will include a confidentiality statement to which the requesting organization or individual must adhere.

(b) The confidentiality agreement that requestors and all other individuals who will have access to the released data, whether an employee of the requestor, subcontractor or other contractor or third-party vendor including data storage or other information technology vendor, who will have access to or responsibility for the data must sign. At a minimum, the confidentiality agreement developed for recipients must meet the requirements of RCW 43.371.050 (4)(a).

(c) Requestors must comply with the requirements for data release in WAC 182-70-500 through 182-70-520.

(2) A person with authority to bind the requesting organization must sign the DUA; or in the case of an individual requesting data, the individual must sign the DUA.

(3) All employees or other persons who will be allowed access to the data must sign a confidentiality agreement.

(4) No data may be released until the lead organization receives a signed copy of the DUA from the data requestor and signed copies of the confidentiality agreement.

(5) The lead organization must maintain a record of all signed agreements and retain the documents for at least six years after the termination of the agreements.

(6) Data fees, if applicable, must be paid in full to the lead organization. Itemized data fees assessed for each data request are subject to public disclosure and should be included in the approval that is posted on the WA-APCD website.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-240, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-240, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.050(6) and chapter 43.371 RCW. WSR 17-22-121, § 82-75-240, filed 10/31/17, effective 12/1/17. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-240, filed 11/1/16, effective 12/2/16.]

WAC 182-70-250 Data use agreement. (1) The lead organization must develop a standard data use agreement. The authority must approve the final form of the DUA, and all substantial changes to the form.

(2) At a minimum, the DUA shall include the following provisions:

(a) A start date and end date. The end date must be no longer than the length of the project for which the data is requested. The DUA may provide for the ability to extend the end date of the agreement upon good cause shown.

(b) The application for data should be incorporated into the DUA and attached as an exhibit to the agreement. There should be an affirmative provision that data provided for one project cannot be used for any other project or purpose.

(c) Data can be used only for the purposes described in the request. The data recipient agrees not to use, disclose, market, release, show, sell, rent, lease, loan or otherwise grant access to the data files specified except as expressly permitted by the DUA, confidentiality agreement if any and the approval letter.

(d) With respect to analysis and displays of data, the data recipient must agree to abide by Washington state law and rules, and standards and guidelines provided by the lead organization.

(e) A requirement for completion of an attestation by an officer or otherwise authorized individual of the data requestor that the data requestor will adhere to the WA-APCD's rules and lead organization policies regarding the publication or presentation to anyone who is not an authorized user of the data.

(f) A requirement that all requestor employees and all other individuals who access the data will sign a confidentiality agreement prior to data release. The confidentiality requirements should be set out in the DUA and include the consequences for failure to comply with the agreement.

(g) A requirement that any new employee who joins the organization or project after the data requestor has received the data and who will have access to the data must sign a confidentiality agreement prior and passed required privacy and security training prior to accessing the data.

(3) The authority or lead organization may audit compliance with data use agreements and confidentiality agreements. The requestor must comply and assist, if requested, in any audit of these agreements.

(4) Breach of a data use agreement or confidentiality agreement may result in immediate termination of the data use agreement. The data requestor must immediately destroy all WA-APCD data in its possession upon termination of the data use agreement. Termination of the data use agreement is in addition to any other penalty or regulatory action taken or that may be taken as a result of the breach.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-250, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-250, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-250, filed 11/1/16, effective 12/2/16.]

WAC 182-70-260 Confidentiality agreement. (1) The lead organization must develop a standard confidentiality agreement, as required, before data may be released. The authority must approve the final form for confidentiality agreement, and all substantial changes to the form.

(2) The confidentiality agreement must be signed by all requestor employees and other third parties who may have access to the data.

(3) In addition to other penalties or regulatory actions that may be taken, including denial of future data requests, breach of a confidentiality agreement may result in immediate termination of the agreement. If an individual breaches the confidentiality agreement, the lead organization must review the circumstances and determine if the requestor's agreement should be terminated or only the agreement with the individual who caused the breach should be terminated. When an agreement is terminated for breach of the confidentiality agreement, the data requestor or individual whose agreement is terminated must immediately destroy all WA-APCD data in his or her possession and provide an attestation of the destruction to the lead organization within seven business days. Attestation of destruction should be in the form as prescribed by the lead organization. Failure to destroy data or provide attestation of the destruction may result in other penalties or regulatory actions.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-260, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-260, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-260, filed 11/1/16, effective 12/2/16.]

WAC 182-70-270 Data procedures at the end of the project. (1) Upon the end of the project or the termination of the data use agreement, the data recipient shall destroy all WA-APCD data. The data recipient must provide to the lead organization an attestation that the data has been destroyed according to the required standards set forth in the DUA. The attestation shall account for all copies of the data being used by the requestor, its employees, subcontractors, and any other person provided access to the data. Attestation of destruction should be in the form as prescribed by the lead organization.

(2) The attestation of data destruction must be provided within ten business days from the end of the project or termination of the DUA or confidentiality agreement, whichever is sooner.

(3) Failure to destroy data or provide attestation of the destruction may result in other penalties or regulatory actions.

[WSR 19-24-090, recodified as § 182-70-270, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-270, filed 11/1/16, effective 12/2/16.]

WAC 182-70-280 Reasons to decline a request for data. The lead organization may decline a request for data for any of the following reasons:

(1) The requestor has violated a data use agreement, nondisclosure agreement or confidentiality agreement within three years of the date of request.

(2) Any person, other than the requestor, who will have access to the data has violated a data use agreement, nondisclosure agreement or confidentiality agreement within three years of the date of request.

(3) The requestor or any person other than the requestor, who will have access to the data, within the five years prior to the data request date, 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 the data requestor or for which the data requestor was responsible for maintaining in a secure environment.

(4) The proposed privacy and security protections in the data management plan on the date the data is requested are not sufficient to meet Washington state standards. The protections must be in place on the date the data is requested. For out-of-state requestors, meeting the standards in the state where the requestor or data recipient is located is not acceptable if those standards do not meet those required in Washington state.

(5) The information provided is incomplete or not sufficient to approve the data request.

(6) The proposed purpose for accessing the data is not allowable under WA-APCD statutes, rules or policies, or other state or federal statutes, rules, regulations or federal agency policy or standards for example the Department of Justice Statements of Antitrust Enforcement Policy in Health Care.

(7) The proposed use of the requested data is for an unacceptable commercial use or purpose. An unacceptable commercial use or purpose includes, but is not limited to:

(a) A requestor using data to identify patients using a particular product or drug to develop a marketing campaign to directly contact those patients; or

(b) A requestor using data to directly contact patients for fundraising purposes; or

(c) A requestor intends to contact an individual whose data is released; or

(d) Sells, gives, shares or intends to sell, give or share released data with another entity or individual not included in the original application for the data and for which approval was given.

[WSR 19-24-090, recodified as § 182-70-280, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-280, filed 11/1/16, effective 12/2/16.]

WAC 182-70-290 Process to review a declined data request. (1) A data requestor may request an administrative review of the lead organization's decision to deny a request for data.

(2) A request for an administrative review may be initiated by a written petition filed with the authority and also provided to the lead organization within thirty calendar days after notice of the denial. The petition shall include the following information:

(a) Data requestor's name, address, telephone number, email address and contact person.

(b) Information about the subject of the review including remedy requested.

(c) A detailed explanation as to the issue or area of dispute, and why the dispute should be decided in the data requestor's favor.

(3) The petition and all materials submitted will be reviewed by the director or director's designee. The reviewing official may request additional information or a conference with the data requestor. A decision from the reviewing official shall be provided in writing to the data requestor no later than thirty calendar days after receipt of the petition. A denial of the petition will include the reasons for the denial.

(4) The authority will post the petition and final decision on the authority website. The lead organization will provide a link to the petition and decision from its WA-APCD website.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-290, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-290, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-290, filed 11/1/16, effective 12/2/16.]

WAC 182-70-300 Process to appeal of final denial of data request. (1) A data requestor may appeal the denial of its administrative review conducted in accordance with WAC 182-70-290.

(2) Request for an appeal must be submitted in writing to the authority within fifteen calendar days after receipt of written notification of denial of its administrative review, with a copy provided to the lead organization.

(3) The lead organization must provide notice and a copy of the appeal request to affected data suppliers within five days of being served. Data suppliers may seek to intervene in an appeal by submitting a petition to intervene to the office of administrative hearings, and serving the petition to intervene on the authority, lead organization and requestor within five days of being notified of the appeal.

(4) Within ten business days of receipt of a written notice of appeal, the authority will transmit the request to the office of administrative hearings (OAH).

(a) **Scheduling.** OAH will assign an administrative law judge (ALJ) to handle the appeal. The ALJ will notify parties of the time when any additional documents or arguments must be submitted. If a party fails to comply with a scheduling letter or established timelines, the ALJ

may decline to consider arguments or documents submitted after the scheduled timelines. A status conference in complex cases may be scheduled to provide for the orderly resolution of the case and to narrow issues and arguments for hearing.

(b) **Hearings.** Hearings may be by telephone or in-person. The ALJ may decide the case without a hearing if legal or factual issues are not in dispute, the appellant does not request a hearing, or the appellant fails to appear at a scheduled hearing or otherwise fails to respond to inquiries. The ALJ will notify the appellant by mail whether a hearing will be held, whether the hearing will be in-person or by telephone, the location of any in-person hearing, and the date and time for any hearing in the case. The date and time for a hearing may be continued at the ALJ's discretion. Other authority employees may attend a hearing, and the ALJ will notify the appellant when other authority employees are attending. The appellant may appear in person or may be represented by an attorney.

(c) **Decisions.** The decision of the ALJ shall be considered a final decision. A petition for review of the final decision may be filed in the superior court. If no appeal is filed within the time period set by RCW 34.05.542, the decision is conclusive and binding on all parties. The appeal must be filed within thirty days from service of the final decision.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-300, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-75-300, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-300, filed 11/1/16, effective 12/2/16.]

PRIVACY AND SECURITY PROCEDURES

WAC 182-70-400 Privacy and security. (1) RCW 43.371.070 (1)(d) authorizes the director of the health care authority to adopt rules providing procedures for ensuring that all data received from data suppliers are securely collected and stored in compliance with applicable state and federal law.

(2) RCW 43.371.070 (1)(e) authorizes the director of the health care authority to adopt rules providing procedures for ensuring compliance with state and federal privacy laws.

(3) WAC 182-70-410 through 182-70-470 provide the procedures required in subsections (1) and (2) of this section.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-400, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-400, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-400, filed 4/4/17, effective 5/5/17.]

WAC 182-70-410 Requirements for data vendor. (1) The data vendor must enter into an agreement with the lead organization that contains the following requirements:

(a) A provision that the data vendor is responsible for ensuring compliance of all aspects of WA-APCD operations with all applicable

federal and state laws, and the state's security standards established by the office of the chief information officer;

(b) Provisions that the data vendor is required to keep logs and documentation on activities conducted pursuant to the security plan consistent with the state records retention requirements, which the authority can request to verify that the security protocols are being followed;

(c) A provision that requires a detailed security process, which should include, but is not limited to, details regarding security risk assessments and corrective actions plans when deficiencies are discovered;

(d) Provisions that require secure file transfer for all receipt and transmission of health care claims data; and

(e) Provisions for encryption of data both in motion and at rest using latest industry standard methods and tools for encryption, consistent with the standards of the office of the chief information officer.

(2) The data vendor must enter into a legally binding data use and confidentiality agreement with the lead organization. The agreement must include provisions that restrict the access and use of data in the WA-APCD to that necessary for the operation and administration of the database as authorized by chapter 43.371 RCW.

(3)(a) The data vendor must annually engage the services of an independent third-party security auditor to conduct a security audit to verify that the infrastructure, environment and operations of the WA-APCD are in compliance with federal and state laws, Washington state information technology security standards, and the contract with the lead organization. The data vendor must prepare a plan to correct any deficiency found in the annual security audit.

(b) The data vendor must submit its latest HITRUST common security framework (CSF) report and the latest statement on standards for attestation engagements (SSAE) No. 16 service organization control 2 (SOC 2) Type II audit report covering the data vendor's third-party data center, to the authority within thirty calendar days of receiving the final report. The data vendor must develop and implement an appropriate corrective action plan, including remediation timelines, when necessary, and provide the corrective action plan to the authority or the office of the state chief information security officer upon request.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-410, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-410, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-410, filed 4/4/17, effective 5/5/17.]

WAC 182-70-420 Data submission. (1) All data suppliers must submit data to the WA-APCD using a secure transfer protocol and transmission approach approved by the office of the state chief information security officer.

(2) All data suppliers must encrypt data using the latest industry standard methods and tools for encryption consistent with the data vendor's requirements for data encryption as required in WAC 182-70-410.

(3) The data vendor must provide a unique set of login credentials for each individual acting on behalf of or at the direction of an active data supplier.

(4) The data vendor must ensure that the data supplier can only use strong passwords consistent with the state standards when securely submitting data or accessing the secure site.

(5) The data vendor must automatically reject and properly dispose of any files from data suppliers that are not properly encrypted.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-420, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-420, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-420, filed 4/4/17, effective 5/5/17.]

WAC 182-70-430 WA-APCD infrastructure. (1) The data vendor must limit access to the secure site. Personnel allowed access must be based on the principle of least privilege and have an articulable need to know or access the site.

(2) The data vendor must conduct annual penetration testing and have specific requirements around the timing of penetration and security testing of infrastructure used to host the WA-APCD by the outside firm. The results of penetration and security testing must be documented and the data vendor must provide the summary results, along with a corrective action plan and remediation timelines, to the authority and the office of the state chief information security officer within thirty calendar days of receipt of the results.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-430, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-430, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-430, filed 4/4/17, effective 5/5/17.]

WAC 182-70-440 Accountability. (1) The data vendor must submit an annual report to the lead organization, the authority, and the office of the state chief information security office that includes the following information:

(a) Summary results of its independent security assessment; and

(b) Summary of its penetration testing and vulnerability assessment results.

(2) The data vendor, upon reasonable notice, must allow access and inspections by staff of the office of the state chief information security officer to ensure compliance with state standards.

(3) The data vendor, upon reasonable notice, must allow on-site inspections by the authority to ensure compliance with laws, rules and contract terms and conditions.

(4) The data vendor must have data retention and destruction policies that are no less stringent than that required by federal standards, including the most current version of NIST *Special Publication 800-88, Guidelines for Media Sanitization*.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-440, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-440, filed 12/3/19, effective

1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-440, filed 4/4/17, effective 5/5/17.]

WAC 182-70-450 Data vendor and lead organization compliance with privacy and security requirements. (1) To ensure compliance with privacy and security requirements, the data vendor must immediately report to the authority and the office of the state chief information security officer any data breach of the WA-APCD or knowledge that a data recipient is not complying with confidentiality requirements in accordance with health care authority-approved data breach notification procedures. The data vendor may not unilaterally disclose any information related to a breach of the WA-APCD without written permission from the authority and the state chief information security officer.

(2) Upon receiving approval from the authority and the state chief information security officer, the data vendor must notify the data supplier if the data it supplied has been the subject of a data breach for which the reporting requirements in subsection (1) of this section apply. The data vendor is responsible for complying with the applicable notification provisions in state and federal law.

(3) To ensure compliance with privacy and security requirements, the lead organization must:

(a) Conduct follow-up with data recipients of PHI or PFI on a schedule developed by the lead organization;

(b) Request data recipients share any manuscripts, reports, or products with lead organization and the authority;

(c)(i) Require data recipients to complete a project completion form, attesting that the project has terminated and data have been destroyed in accordance with the data use agreement;

(ii) Require the data recipient to provide the written verification that the data has been destroyed in a manner no less stringent than is required in WAC 182-70-440(4).

(d) Track all requests and research projects and follow up with the data recipient when the research or project is expected to be completed; and

(e) Follow up and require written verification that data is destroyed.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-450, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-450, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-450, filed 4/4/17, effective 5/5/17.]

WAC 182-70-460 Additional requirements. (1) The data vendor will ensure access to the WA-APCD data is strictly controlled and limited to authorized staff with appropriate training, clearance, background checks, and confidentiality agreements.

(2) All data vendor employees who are provided access to data submitted to the WA-APCD must attend security and privacy training before actual access to data is allowed. The training will cover the relevant privacy and security requirements in state and federal law.

[WSR 19-24-090, recodified as § 182-70-460, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-460, filed 4/4/17, effective 5/5/17.]

WAC 182-70-470 State oversight of compliance with privacy and security requirements. In order to ensure compliance with privacy and security requirements and procedures, the authority or the office of chief information officer or both may request from the lead organization any or all of the following:

(1) Audit logs pertaining to accessing the WA-APCD data;

(2) Completion of a security design review as required by Washington state IT security standards;

(3) Documentation of compliance with OCIO security policy (OCIO policy 141.10 Securing information technology assets standards);

(4) All data use agreements.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-470, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-470, filed 12/3/19, effective 1/1/20. Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-470, filed 4/4/17, effective 5/5/17.]

FORMAT FOR THE CALCULATION AND DISPLAY OF DATA

WAC 182-70-500 Additional definitions related to the format for the calculation and display of data. The following additional definitions apply throughout this chapter unless the context clearly indicates another meaning. These definitions are related to the rules regarding the format for the calculation and display of cost data.

(1) "Aggregate cost data" means data collected from individual-level records that are maintained in a form that does not permit the identification of individual records.

(2) "Arithmetic mean" means the sum of a set of values, divided by the number of values in the set.

(3) "Average" means the arithmetic mean.

(4) "Cell size suppression" means a method used to report data that restricts or suppresses disclosure of subsets of data to protect the identity and privacy of data subjects and to avoid the risk of identification of individuals or providers in small population groups.

(5) "Median" means the middle value of a list of values where the values have been sorted in size order. If the list has an even number of values, the median is the arithmetic mean of the two middle values.

(6) "Outlier" means an observation that is well outside of the expected range of values in a study or experiment, and which is often discarded from the data set.

(7) "Proportion" means a comparative relation between things or magnitudes as to size, quantity, number, or ratio.

(8) "Range" is the largest value in the set of numbers minus the smallest value in the set. Often, a range is expressed to denote a particular span, e.g., 25th to 75th percentile range. Note that as a statistical term, the range is a single number, not a range of numbers.

[WSR 19-24-090, recodified as § 182-70-500, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.050(6) and chapter 43.371 RCW. WSR 17-22-121, § 82-75-500, filed 10/31/17, effective 12/1/17.]

WAC 182-70-510 Data formatting rules apply to proprietary financial information. (1) The format rules apply to all proposed uses of proprietary financial information submitted to the WA-APCD. The format rules apply to three categories of users for which proprietary financial information may be disclosed in accordance with chapter 43.375 RCW:

(a) Lead organization;

(b) Federal agencies, Washington state agencies, and units of Washington local government; and

(c) Researchers with IRB approval.

(2) The lead organization shall assess a data requestor's proposed methods submitted in compliance with RCW 43.371.050 (1)(c) and WAC 182-70-210(2), which require the data requestor to submit a description of the proposed methodology for data analysis. The lead organization's assessment shall include evaluating the data requestor's methodology as it pertains to the calculation and presentation of cost information that rely upon proprietary financial information.

(3) To evaluate data requestor methodology, the lead organization shall adopt criteria to prevent the disclosure or determination of proprietary financial information to any third party.

(4) The data release advisory committee shall advise the lead organization on the criteria to be adopted.

(5) Nothing in this rule shall contravene the authorized uses of proprietary financial information as provided in RCW 43.371.050.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-510, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-510, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.050(6) and chapter 43.371 RCW. WSR 17-22-121, § 82-75-510, filed 10/31/17, effective 12/1/17.]

WAC 182-70-520 Elements to safeguard the use of proprietary financial information. All reports, analytics or other information drawn from the WA-APCD that an approved WA-APCD data user as defined in WAC 182-70-510(1) shares with any third party shall comply with the following restrictions.

(1) Allowed amount data may be made available for public use.

(2) Allowed amount data shall be provider or payer deidentified.

(3) Provider-specific allowed amount data shall be suppressed if that payer accounts for more than fifty percent of that provider's patient market share that payer deidentified data could readily be payer reidentified.

(4) Absolute or relative allowed cost information shall be communicated in ways that mitigate the potential to mislead data users including, but not limited to:

(a) Median cost mitigates the impact of outlier cases;

(b) Cost variation statistics (ranges, confidence intervals) illustrate the typical distribution of costs around a point estimate;

(c) Categorization, stratification or risk-adjustment techniques make like-comparisons of patient populations;

(d) Minimum case volume rules and/or reporting of volume alerts users to the universe or sample underlying the cost result; and

(e) Cell size suppression rules are followed whereby cells containing cost data based on a number of patients or providers that is below a minimum threshold count is suppressed.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-520, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-520, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.050(6) and chapter 43.371 RCW. WSR 17-22-121, § 82-75-520, filed 10/31/17, effective 12/1/17.]

FEE SCHEDULES

WAC 182-70-550 Requirement for fee schedules and processes. (1) RCW 43.371.020 (5)(g) requires the lead organization to develop a plan for the financial sustainability of the database, and charge fees for reports and data files to fund the database.

(2) The authority must approve any fee established by the lead organization.

(3) RCW 43.371.070 requires the authority to establish by rule, procedures for the lead organization to establish these statutorily required fees.

(4) The process to develop, review and approve fee schedules will be open and transparent, and allow for stakeholder feedback.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-550, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-550, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(f). WSR 18-10-074, § 82-75-550, filed 5/1/18, effective 6/1/18.]

WAC 182-70-560 Process to establish fee schedules. (1) The lead organization must develop a draft fee schedule consistent with the requirements in RCW 43.371.020 (5)(g). The lead organization must maintain documentation that supports the development of and final decisions regarding the fee schedule.

(2) The lead organization must present the draft fee schedule and supporting documentation to the data policy committee for review and feedback. The lead organization must provide any other available data requested by the DPC that supports the development and draft fee schedule presented.

(3) The DPC must review the draft fee schedule, supporting documentation, and adopt recommendations, including the basis for each recommendation, as to whether the fee schedule should be approved by the authority. The DPC must provide the recommendations to the lead organization for its consideration.

(4) The lead organization must review the DPC recommendations and make any changes to the draft fee schedule based on the recommendations. The lead organization must document which recommendations it implemented into the fee schedule. For those recommendations that the lead organization did not act upon, the lead organization must document the reasons why each recommendation was not accepted.

(5) The lead organization must provide the authority the draft fee schedule, as modified, supporting documentation, the DPC recommendations, and the reasoning for why the lead organization did not make changes for any recommendation not accepted. The lead organization must also provide any other available data requested by the authority that supports the development and draft fee schedule provided to the authority.

(6) The authority shall post on the agency website the draft fee schedule, and solicit public comment for thirty days. The authority may also convene a stakeholder meeting to provide an opportunity for interested parties another avenue to give feedback on the draft fee schedule. If the authority decides to hold a stakeholder meeting, the meeting may be in person, by telephone or other electronic means, as determined by the authority.

After the comment period, the authority will review all the stakeholder feedback, recommendations of the DPC, and any data received from the lead organization and make a final determination regarding the fee schedule. The authority shall provide the final determination to the lead organization, publish the final determination on the agency website, and send notification through the authority listserv or other electronic means.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-560, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-560, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(f). WSR 18-10-074, § 82-75-560, filed 5/1/18, effective 6/1/18.]

WAC 182-70-570 Process to modify fee schedules. (1) Fee schedules shall be reissued no less frequently than on an annual basis. The reissuance of the fee schedule can include maintaining the fee schedule without modification, modifying the fee schedule, or a combination of these two actions.

(2) The lead organization shall review fee schedules at least once every year. Annual period shall be from the date upon which the fee schedule is adopted. The review shall include whether any fee should be changed, removed from the schedule, or new fees added. The lead organization must maintain documentation that supports the recommended changes from the review of the fee schedule.

(3) The lead organization must present the changes, supporting documentation, and proposed modifications to the fee schedule to the data policy committee for review and feedback. The lead organization must provide any other available data requested by the DPC that supports the proposed modifications to the fee schedule.

(4) The DPC must review the changes, supporting documentation, and proposed modifications to the fee schedule and adopt recommendations, including the basis for each recommendation, as to whether the changes should be accepted and the modified fee schedule approved by the authority. The DPC must provide the recommendations to the lead organization for its consideration.

(5) The lead organization must review the DPC recommendations and make any changes to the recommendations and proposed modifications to the fee schedule based on the recommendations. The lead organization must document which recommendations it implemented into the fee schedule. For those recommendations that the lead organization did not act

upon, the lead organization must document the reasons why each recommendation was not accepted.

(6) The lead organization must provide the authority the proposed modifications to the fee schedule, as modified, with supporting documentation, the DPC recommendations, and the reasoning for why the lead organization did not make changes for any recommendation not accepted. The lead organization must provide any other available data requested by the authority that supports the changes and proposed modified fee schedule provided to the authority.

(7) The authority shall post on the agency website the recommendations and proposed modifications to the fee schedule, and solicit public comment for thirty days. The authority may also convene a stakeholder meeting to provide an opportunity for interested parties another avenue to give feedback on the draft fee schedule. If the authority decides to hold a stakeholder meeting, the meeting may be in person, by telephone or other electronic means, as determined by the authority.

(8) After the comment period, the authority will review all the stakeholder feedback, recommendations of the DPC, and any data received from the lead organization and make a final determination regarding the fee schedule. The authority shall provide the final determination to the lead organization, publish the final determination on the agency website, and send notification through the authority listserv or other electronic means.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-570, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-570, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(f). WSR 18-10-074, § 82-75-570, filed 5/1/18, effective 6/1/18.]

PENALTIES FOR INAPPROPRIATE DISCLOSURES OR USES

WAC 182-70-600 Causes for penalties. (1) The authority may impose penalties for the inappropriate disclosure or use of direct patient identifiers, indirect patient identifiers, and proprietary financial information received from, provided to, or contained in the WA-APCD.

(2) Any penalty imposed pursuant to this subchapter and in accordance with RCW 43.371.050 shall be in addition to and does not prevent the assessment of penalties authorized by state or federal law, contract, or court order.

(3) The following definitions apply to WAC 182-70-600 through 182-70-665.

(a) "Inappropriate disclosures" or "uses" are those that are inconsistent or in violation of the requirements in RCW 43.371.050. In addition, inappropriate disclosure or uses also include defamatory or malicious use and disclosure or use and disclosure with the intent to cause harm.

(b) "Protected information" is direct patient identifiers, indirect patient identifiers and proprietary financial information.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-600, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-600, filed 12/3/19, effective

1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-600, filed 7/5/18, effective 8/5/18.]

WAC 182-70-605 Alleging a violation. (1) Any person, as defined in WAC 182-70-030, may bring to the attention of the lead organization or the authority information concerning the inappropriate disclosure or use of protected information as set forth in RCW 43.371.050 and WAC 182-70-600.

(2) The authority must conduct an investigation unless it determines that the complaint is without merit or is frivolous, regardless of how the authority has received the information that led to that belief, including information derived from any audit conducted by or at the direction of the authority.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-605, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-605, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-605, filed 7/5/18, effective 8/5/18.]

WAC 182-70-610 Complaints. (1) Any complaint filed pursuant to WAC 182-70-605 must be in writing and include the following information, if known:

(a) The name and contact information of the complainant;

(b) The specific facts supporting the violation alleged, including the dates, and locations for all events upon which the complaint is made;

(c) The facts upon which the complaint is based; and

(d) The name of the individual(s) and organization the complainant believes has committed an inappropriate disclosure or use of protected information and should be subject to penalties.

(2) If sufficient information is provided as required in subsection (1)(b) through (d) of this section, the authority will accept the complaint without the complainant's name and contact information. In cases when the name and contact information is not provided, the complainant waives any future contact or notification from the authority regarding the complaint.

(3) The complainant must provide additional information if requested by the lead organization or the authority.

(4) Complaints alleging the lead organization made inappropriate disclosure or use of protected information must be filed directly with the authority. The complaint must contain the information required in subsection (1) of this section. If a complaint of this nature is filed with the lead organization, the lead organization must forward to the authority within one business day of receipt, without further review or action.

(5) Regardless of whether the complaint was filed with the authority or the lead organization, except as provided by subsection (4) of this section, the lead organization will review the complaint and compile any information it may have related to the complaint. The lead may review the complaint as to whether the facts as presented support the finding of an inappropriate disclosure or use of protected information. The lead organization must forward the complaint, and all supporting documents to the authority, including the result of any initial review the lead may have undertaken.

(6) The authority must review the information provided by the lead organization pursuant to subsection (5) of this section.

(a) If the authority determines that the facts as presented, if true, support the finding of an inappropriate disclosure or use of protected information, the authority will conduct an investigation to substantiate the allegations.

(b) If the authority determines that the facts as presented, if true, do not support the finding of an inappropriate disclosure or use of protected information, the authority will close the complaint without further action. If closed without further action, the notice will include the basis for that determination.

(c) The authority may conduct the investigation, or contract with a third party, other than the lead organization or a subcontractor to the lead organization, to conduct the investigation.

(7) The authority will notify the complainant in writing and state whether the complaint will be investigated or closed without action.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-610, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-610, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-610, filed 7/5/18, effective 8/5/18.]

WAC 182-70-615 Investigation. (1) If the authority accepts a complaint and conducts an investigation, the authority will notify the person(s) that is the subject of the complaint in writing.

(2) The notice will include the following information:

(a) The factual allegations supporting each alleged inappropriate disclosure or use of protected information violation in terms sufficient to put the persons on notice of the specific reasons for the investigation;

(b) The statutory and administrative code provisions addressing the allegations, if applicable;

(c) A request that the person provide a written response to the allegations including any documents that support the response, and notice that failure to respond will result in the authority making a decision without the person's input; and

(d) A directive to cease using or destroy the data received from the WA-APCD until the investigation has been completed and the person is notified that he/she may again use the data provided. The person shall complete an attestation that the person has complied with this directive. A violation of this directive shall be grounds for finding a separate violation of the inappropriate disclosure or use of protected information.

(3) The lead organization and the data vendor shall cooperate with the investigator and timely respond to requests for information or documents during the course of an investigation.

(4) At the conclusion of the investigation, the investigator will issue a report to the WA-APCD program director that includes the following information:

(a) Facts found by the investigator;

(b) Whether the facts support finding inappropriate disclosures or uses of protected information; and

(c) A recommendation to dismiss the complaint with no further action or to issue an order with a penalty, which recommendation may in-

clude a penalty amount and any other actions that the authority should take as a result of the violation(s).

(5) A finding that the person inappropriately disclosed or used protected information is a violation for purposes of this section. In the case of a continuing inappropriate disclosure or use of protected information, each day of the inappropriate disclosure or use is a separate violation.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-615, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-615, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-615, filed 7/5/18, effective 8/5/18.]

WAC 182-70-620 Notice of violation and recommended penalty. (1) If, based on the investigation, the WA-APCD program director determines that the facts support finding an inappropriate disclosure or use of protected information and imposition of a penalty as set forth in the investigation report, the WA-APCD program director shall notify the alleged violator. The WA-APCD program director shall cause service of the notice of violation and recommended penalty on each alleged violator. The notice shall include the following information:

(a) Date when the recommended penalty and other actions imposed will take effect, if not appealed;

(b) Each inappropriate disclosure or use of protected information found and the facts supporting each inappropriate disclosure or use of protected information;

(c) The recommended penalty, other monetary amounts to be assessed, including the cost of the investigation, and any other action authorized by WAC 182-70-625 and 182-70-630;

(d) If the person will be prohibited from receiving data from the WA-APCD in the future, the period of the recommended prohibition;

(e) Notice that each alleged violator may request a hearing in accordance with WAC 182-70-645 to dispute the finding of a violation, the recommended penalty, or both. The notice shall state that if no hearing is requested within thirty days of the date of issuance of the notice, the authority shall issue a final, unappealable order.

(2) In the event the alleged violator or violators do not timely request a hearing, the WA-APCD program director will provide the report and recommendation to the director, who shall issue a final order, which will include the date upon which the order becomes effective.

(3) The WA-APCD program director shall provide a copy of the investigation report and the notice prepared pursuant to subsection (1) of this section to all data suppliers with protected information identified in the report as having been inappropriately disclosed or used. This notice is separate and in addition to any other notice required by law.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-620, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-620, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-620, filed 7/5/18, effective 8/5/18.]

WAC 182-70-625 Monetary penalties that may be imposed upon finding a violation of inappropriate disclosures or uses. (1) If a person has been found to have made inappropriate disclosures or uses of direct patient identifiers, indirect patient identifiers, and proprietary financial information received from the WA-APCD, the director may impose one or more of the following monetary penalties:

(a) A civil penalty determined pursuant to the criteria and requirements in this chapter;

(b) Cost, including reasonable investigative costs, that do not exceed the amount of any civil penalty;

(c) The cost of any audit performed that uncovered the violation, or was conducted as a result of investigating an alleged violation; and

(d) Up to three times the amount of financial gain received by the alleged violator or financial loss of any person whose protected information was inappropriately disclosed or used.

(2) The director shall include with the decision regarding the monetary penalty assessment, the director's reasoning for the specific penalty, or lack thereof, that is being assessed.

[WSR 19-24-090, recodified as § 182-70-625, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-625, filed 7/5/18, effective 8/5/18.]

WAC 182-70-630 Nonmonetary penalties that may be imposed upon finding a violation of inappropriate disclosures or uses. In addition to the monetary penalties set forth in WAC 182-70-625, if a person has been found to have made inappropriate disclosures or uses of direct patient identifiers, indirect patient identifiers, and proprietary financial information received from the WA-APCD, the director may order the following nonmonetary penalties:

(1)(a) Direct WA-APCD program director to review the contract between the person and lead organization to determine whether the finding is a breach of that contract, and take appropriate action including requiring all WA-APCD data provided to be destroyed, termination of the contract, and seeking damages if the contract has been breached; or

(b) In lieu of (a) of this subsection, direct the lead organization to review whether the finding is also a breach of any contract between the person and the lead organization, and take appropriate action including requiring all WA-APCD data provided to be destroyed, termination of the contract, and seeking damages if the contract has been breached, unless the lead organization is the violator, in which case (a) of this subsection shall apply.

(2) Demand the destruction of all WA-APCD data provided, whether stand alone or combined with other data, all data products, and derivatives produced from WA-APCD data, and in the person's custody or contract, including proof of the destruction in the form and manner as prescribed by the authority;

(3) Bar the person from receiving any data from the WA-APCD for a designated period of time; and

(4) Notify the funding entity of the violation, when the violation involves research funded by another entity, and any other regulatory agency that has oversight over the person or the data that the person requested.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-630, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-630, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-630, filed 7/5/18, effective 8/5/18.]

WAC 182-70-635 Penalty ranges based on culpability. (1) In determining the appropriate sanction, including the amount of any civil penalty, the director will consider the level of culpability associated with the violation. The levels of culpability, in the order of less severe to severe, are as follows:

(a) Did not know. The person did not know and by exercising reasonable diligence, would not have known the violation had occurred.

(b) Reasonable cause. The person knew, or by exercising diligence should have known, that the violation had taken place, but the person did not act with willful negligence.

(c) Willful neglect - Corrected. The violation was due to the person's conscious, intentional failure or reckless indifference, and the violation was corrected within thirty days from the date the person knew or with reasonable diligence should have known of the inappropriate disclosure or use.

(d) Willful neglect - Uncorrected. The violation was due to the person's conscious, intentional failure or reckless indifference, and the violation was not corrected within thirty days from the date the person knew or with reasonable diligence should have known of the inappropriate disclosure or use.

(2) The penalty ranges for each level of culpability and the yearly cap for violations of a similar nature are as follows:

Culpability Category	Penalty Range per Violation	Yearly Cap for Similar Violations
Did not know	$5,000 - $100,000	$2,500,000
Reasonable cause	$10,000 - $250,000	$2,500,000
Willful neglect - Corrected	$50,000 - $500,000	$5,000,000
Willful neglect - Not corrected	$100,000 - $1,500,000	$10,000,000

(3) Violations that involve malicious intent, as that term is defined in WAC 182-70-030, are not subject to the yearly caps set forth in subsection (2) of this section.

(4) The director may assess a penalty outside the penalty ranges set forth in subsection (2) of this section if the person has previously committed the same violation in the same culpability category.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-635, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-635, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-635, filed 7/5/18, effective 8/5/18.]

WAC 182-70-640 Other factors that may be considered in determining the penalty for a violation of this chapter. In addition to the culpability category set forth in WAC 182-70-635, to determine the penalty amount, the director may consider the following factors:

(1) The nature and extent of the violation including, but not limited to, the number of persons affected, the duration of the violation, and whether the violation was done with malicious intent.

(2) The nature and extent of the harm resulting from the violation including, but not limited to:

(a) Whether the violation resulted in physical harm;

(b) Whether the violation resulted in financial harm;

(c) Whether the violation resulted in harm to a person's reputation;

(d) Whether the violation hindered an individual's ability to obtain health care;

(e) Whether the violation resulted in any other actual or potential harm.

(3) The history of compliance with the statutory, regulatory, and contractual provisions related to prior data release from the WA-APCD including, but not limited to:

(a) Whether the current violation is the same or similar to previous noncompliance;

(b) Whether and to what extent the person has attempted to correct previous noncompliance;

(c) How the person has responded to the complaint, investigation and any assistance provided to correct and mitigate any effect from the violation;

(d) How the person has responded to prior complaints for the same or similar violations including, but not limited to, changes in process or procedures for securing the confidentiality of the protected information, changes in recruitment, retention, or training requirements for employees or contractor with access to protected information.

(4) Any other factor relevant to the violation or the impact of the violation including, but not limited to:

(a) The frequency of incidents and/or duration of the wrongdoing;

(b) Whether there is a pattern or prior history of wrongdoing;

(c) Whether the person has accepted responsibility for the wrongdoing and recognizes the seriousness of violation;

(d) Whether the person paid or agreed to pay any criminal, civil, and administrative liabilities for the improper activity, including any investigative or administrative costs incurred by the government, and has made or agreed to make full restitution;

(e) Whether the person has cooperated fully during the investigation and any administrative action. In determining the extent of cooperation, the director may consider when the cooperation began and whether the person disclosed all known pertinent information;

(f) The kind of positions held by the individuals involved in the wrongdoing;

(g) Whether the person fully investigated the circumstances surrounding the violation and, if so, made the result of the investigation available to the reviewing official, and took appropriate corrective action or remedial measures;

(h) Whether effective standards of conduct and internal control systems were in place at the time the violation occurred;

(i) Whether appropriate disciplinary action was taken against the individuals responsible for the activity that constitutes the violation.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-640, filed 3/25/20, effective 4/25/20. WSR

19-24-090, recodified as § 182-70-640, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-640, filed 7/5/18, effective 8/5/18.]

WAC 182-70-645 Process to appeal determination of a violation and assessed penalties. (1) Each person to whom a notice of a violation and recommended penalty is issued may request a hearing to be conducted in accordance with WAC 182-70-655.

(2) The request for a hearing must be submitted to the director in writing within thirty days after receipt of written notification of the notice provided pursuant to WAC 182-70-620. The person requesting a hearing must also provide a copy of the request to the WA-APCD program director.

(3) The request for hearing must be in writing and specify:

(a) The name of the person requesting the hearing and the person's or representative's contact information;

(b) The items, facts, or conclusions in the notice of violation being contested; and

(c) The basis for contesting the penalty, if applicable, including any mitigating factors upon which the person relies and the outcome the requestor is seeking.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-645, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-645, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-645, filed 7/5/18, effective 8/5/18.]

WAC 182-70-650 Informal dispute resolution prior to a hearing. (1) The following procedures are available for informal dispute resolution prior to a hearing that may make more elaborate proceedings under the Administrative Procedure Act unnecessary.

(2) Settlements. Any appeal of a notice of violation and recommended penalty before the director or director's designee, for which a hearing has not yet been held, may be resolved by settlement. The respondent shall communicate his or her request to the WA-APCD program director, setting forth all pertinent facts and the desired remedy. Settlement negotiations shall be informal and without prejudice to rights of a participant in the negotiations.

(3) Stipulations. The WA-APCD program director and respondent may agree to terms of any stipulation of facts, violations, and/or penalty. If a stipulation is reached, the WA-APCD program director shall prepare the stipulation for presentation to the director.

(a) Any proposed stipulation shall be in writing and signed by each party to the stipulation or his or her representative. The WA-APCD program director shall sign for the authority. Any stipulation shall be provided no later than three business days preceding the hearing.

(b) The director has the option of accepting, rejecting, or modifying the proposed stipulation or asking for additional facts to be presented. If the director accepts the stipulation or modifies the stipulation with the agreement of the parties, the director shall enter an order in conformity with the terms of the stipulation. If the director rejects the stipulation or one or both of the parties does

not agree to the director's proposed modifications to the stipulation, then the hearing shall be scheduled and held.

(4) Informal dispute resolution negotiations shall be informal and without prejudice to the rights of the participants.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-650, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-650, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-650, filed 7/5/18, effective 8/5/18.]

WAC 182-70-655 Hearing and final order. For penalties imposed under WAC 182-70-600, the WA-APCD program director or the director's designee conducts a hearing and prepares a final order in accordance with WAC 182-526-0206.

[Statutory Authority: RCW 41.05.021, 41.05.160, 43.71C.110, and 2019 c 334. WSR 21-11-039, § 182-70-655, filed 5/12/21, effective 6/12/21. Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-655, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-655, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-655, filed 7/5/18, effective 8/5/18.]

WAC 182-70-665 Posting of information related to inappropriate disclosure or use of protected information. (1) Except as provided in subsection (2) of this section, the authority will maintain a website to provide public access to information related to the inappropriate disclosure or use of protected information. For each complaint for which an investigation is conducted, the authority will post the complaint, the information that the lead organization provided to the authority pursuant to WAC 182-70-610(5), investigation report and final disposition of the complaint. In addition, if the complaint finds a violation, the authority will post the notice of violation and the final hearing order, if a hearing is requested.

(2) If any of the records specified for posting in subsection (1) of this section contains confidential or protected information, that information is privileged and not subject to disclosure under the Public Records Act, chapter 42.56 RCW, and will be redacted from any documents posted on the authority website.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-665, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-665, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070 (1)(h). WSR 18-15-002, § 82-75-665, filed 7/5/18, effective 8/5/18.]

AUDITS

WAC 182-70-700 Purpose of audits. There are two primary areas for which audits may be performed to ensure compliance with laws and rules related to the WA-APCD.

(1) Audits may be performed to determine if data suppliers are in compliance with the requirements for the submission of data to the WA-APCD including, but not limited to:

(a) Compliance with the data submission guide including, but not limited to, accuracy of financial fields;

(b) Data integrity, as opposed to data quality checks that the data vendor performs using thresholds and variances;

(c) Finding data that is missing or being withheld from submission into the WA-APCD; and

(d) Documenting the process for determining the number of Washington covered persons for each line of business in order to ensure that data suppliers are not artificially creating lines of business with small numbers of covered lives in order to meet the minimum threshold for exclusion to report.

(2) Audits can be performed to determine whether requestors who receive data from the WA-APCD are in compliance with the data release requirements or agreements, whether provided datasets or licenses to the data enclave including, but not limited to:

(a) For physical datasets, compliance with data use agreements, confidentiality agreements, compliance with collecting, storing, analyzing, and destroying the data; and

(b) For data enclave licenses, compliance with data use agreements, confidentiality agreements, compliance with analyzing, storing, destroying, and user license access to the data.

(3) For purposes of this section, the following definitions apply:

(a) "Data quality checks" means the extent to which data is missing or the data conforms with the data format requirements; and

(b) "Data integrity checks" means the completeness and validity of the submitted data, whether the submitted values are consistent with the instructions and intent of the data submission guide.

[WSR 19-24-090, recodified as § 182-70-700, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070. WSR 18-22-095, § 82-75-700, filed 11/5/18, effective 12/6/18.]

WAC 182-70-705 When an audit may be commenced. (1) The authority may initiate a random audit to ensure compliance with data release requirements. A data requestor may not be subject to a random audit more frequently than once every three years.

(2) The authority may initiate an audit of a data supplier or data requestor upon notice that one of the following events has occurred:

(a) Reports from the data vendor that there is a material change, without justification or a reasonable basis for the change provided by the data supplier, in the number of claims submitted from a data supplier. Before submitting a report under this subsection, the data vendor should have worked with the data supplier to cure any inadvertent data submission issues.

(b) Reports from the data vendor that certain types of claims are missing for a data supplier.

(c) Notice that the data requestor or data user is publishing data in reports that are not compliant with data use agreements. Violations of the data use agreements are subject to penalties in accordance with the process set forth in this chapter.

(d) Notice that the data requestor or data user is publishing PFI or PHI not in compliance with state or federal requirements.

(e) Other occurrence that could indicate that the data supplier or data requestor is not in compliance with the requirements in law or rule regarding the WA-APCD.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-705, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-705, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070. WSR 18-22-095, § 82-75-705, filed 11/5/18, effective 12/6/18.]

WAC 182-70-710 Audit process. (1) Once the authority determines an audit will be conducted, either as a random audit or based on a triggering event set forth in WAC 182-70-705(2), the authority shall provide written notice to the subject of the audit at least thirty days before the start of the audit. The notice must include the name of the company or individuals who will be conducting the audit and the subject of the audit, including the time period for which the audit covers, which time period must be no longer than the prior three years. If the audit is the result of a triggering event, the notice will include information regarding the triggering event. The notice will also include information regarding the audit entrance conference that has been scheduled to take place within fourteen days before the audit will begin. The notice will include the location, date and time and contact person for the entrance conference and such other information as required. The authority will work with the subject of the audit to ensure sufficient time is provided between providing the written notice, the date of the entrance conference, and the start of the audit.

(2) The subject of the audit is required to cooperate with the auditor, providing the information as requested. If there is a dispute during the audit, the issue should be brought to the attention of the WA-APCD program director, who will resolve the dispute. Both the auditor and the subject of the audit will be provided an opportunity to present its issues regarding the dispute, either in writing or in person. The WA-APCD program director may engage a mediator to help resolve the dispute.

(3) The auditor will be required to prepare an audit report. A draft of the audit report shall be provided to the subject of the audit for review and comments. The subject of the audit should be provided no less than thirty days to provide comment to the draft report.

(4) After receiving and reviewing any comments, and revising the draft audit report as deemed necessary, the auditor shall schedule an exit conference with the subject of the audit to review the audit and final audit report. The subject of the audit shall be provided an opportunity to submit comments or responses to the findings in the audit. The auditor shall provide a deadline, not less than thirty days after the exit conference for submission of any response to the audit.

(5) The auditor shall issue a final audit report no later than thirty days after the deadline for submission of any response. The report shall be provided to the authority and the subject of the audit. The final report shall include any response provided by the subject of the audit. The authority shall publish the final report on the agency website.

(6) The auditor shall be required to sign a confidentiality/nondisclosure agreement if the auditor will have access to any confidential or proprietary information.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-710, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-710, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070. WSR 18-22-095, § 82-75-710, filed 11/5/18, effective 12/6/18.]

WAC 182-70-715 Audit guide. (1) The authority shall develop the audit guide with input from the data vendor, lead organization, and stakeholders. The audit guide shall include, but is not limited to, the following topics:

(a) The audit standards that will be used for all audits to ensure compliance with generally accepted auditing practices;

(b) The process that will be used to select an auditor, including the auditor qualifications, process to identify and address conflicts of interest;

(c) Specific contract terms that should be included in any contract with an auditor including retention and destruction process for working papers.

(2) The authority shall develop a process to allow for stakeholder review and comment on drafts of the audit guide and all subsequent changes to the guide. Prior to final adoption, the DPC shall be given an opportunity to review and provide comments on the draft audit guide to the authority. The authority shall have final approval authority over the adoption of the audit guide and all subsequent changes.

(3) The authority shall conduct an annual review of the audit guide. The authority will post notice that the review is being conducted and provide a time period for stakeholder to submit comments and changes to the audit guide. The authority will follow the process developed pursuant to subsection (2) of this section for review and comment on draft changes to the guide.

(4) The authority shall notify data suppliers before changes to the audit guide are final. Notification shall occur no less than one hundred twenty calendar days prior to the effective date of any change.

(5) The version of the audit guide that is in effect must be posted on the authority website. Notice should be given through the authority listserv when a new audit guide is posted.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-715, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-715, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070. WSR 18-22-095, § 82-75-715, filed 11/5/18, effective 12/6/18.]

WAC 182-70-720 Audit findings of a violation. (1) If the audit finds that any person has violated laws, rules or data use agreements, the WA-APCD program director shall require an investigation be conducted in accordance with WAC 182-70-615. If the investigation determines that a violation or violations have occurred, the authority will take appropriate action as set forth in this chapter.

(2) In addition to any other penalties authorized by law or rule, the audited party may be required to pay the cost of the audit if, after an investigation conducted pursuant to this chapter, a violation is found. The subject of the audit may contest the requirement to pay the cost of the audit or the amount requested using the appeal process set forth in this chapter for the appeal of penalties.

[Statutory Authority: RCW 41.05.021, 41.05.160 and 43.371.020. WSR 20-08-059, § 182-70-720, filed 3/25/20, effective 4/25/20. WSR 19-24-090, recodified as § 182-70-720, filed 12/3/19, effective 1/1/20. Statutory Authority: RCW 43.371.070. WSR 18-22-095, § 82-75-720, filed 11/5/18, effective 12/6/18.]