Chapter 82-75 WAC
ALL PAYER HEALTH CARE CLAIMS DATABASE

WAC 82-75-010 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 office of financial management to establish a statewide all-payer health care claims database to support transparent public reporting of health care information. The office 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 office of financial management 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: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-010, filed 1/29/16, effective 2/29/16.]

WAC 82-75-020 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 cap-

tured 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.

[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 82-75-030 Additional definitions authorized by chapter 43.371 RCW. The following additional definitions apply throughout this chapter unless the context clearly indicates another meaning.

"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.

"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 release committee" or "DRC" is the 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 the lead organization and the data requestor 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.

"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 office of financial management.

"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 office of financial management to coordinate and manage the database as provided in chapter 43.371 RCW.

"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.

"Office" means the Washington state office of financial management.

"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.

"Washington covered person" means any eligible member and all covered dependents where 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 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 82-75-040 Registration requirements. (1) **Initial registration.** Each data supplier required to submit health care data pursuant to chapter 43.371 RCW shall regis-

ter within thirty days of notification from the lead organization.

(2) **Annual registration.** Each data supplier required to submit health care data pursuant to chapter 43.371 RCW shall 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 shall file its annual registration by December 31st of the year following the year of the initial registration.

(3) 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, shall register with the lead organization within thirty days of being required to submit data.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-040, filed 1/29/16, effective 2/29/16.]

WAC 82-75-050 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 office 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 office shall approve or deny the request and provide written notification to the requestor within thirty calendar days of receipt of the request. The office decision on the request for a replacement file will be provided in writing. If the office 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 office may approve a request for more than one year for exceptional circumstances. The office shall approve or deny the request using the process set forth in (b) of this subsection.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-050, filed 1/29/16, effective 2/29/16.]

WAC 82-75-060 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 82-75-080(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 office 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 office as to whether to approve or deny the request. The office may approve the request for good cause.

[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 82-75-070 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 office 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 82-75-080.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-070, filed 1/29/16, effective 2/29/16.]

WAC 82-75-080 Waivers and extensions. (1) The office 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 office 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 office may approve a request for extenuating circumstances. Approval may be for a time period shorter than requested. The office shall approve or deny the request and provide written notification to the requester within thirty calendar days of receipt of the request. The office decision on the request for a waiver will be provided in writing. If the office 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 office 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 office may approve a request for extenuating circumstances. The office 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 office decision on the request for an extension will be provided in writing. If the office does not approve a request for an extension, the written notification will include the reason for the denial.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-080, filed 1/29/16, effective 2/29/16.]

WAC 82-75-090 Penalties for failure to comply with reporting requirements. (1) The office 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 office 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 office has approved a waiver or extension, the office 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 office has approved a waiver or extension, the office 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 office has approved a waiver or extension, the office 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 82-75-050 (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 office 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 office may suspend in whole or in part any fine assessed in accordance with this section.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-090, filed 1/29/16, effective 2/29/16.]

WAC 82-75-100 Administrative review. (1) Data suppliers may request an administrative review of an office 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 office 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: Chapter 43.371 RCW. WSR 16-04-068, § 82-75-100, filed 1/29/16, effective 2/29/16.]

WAC 82-75-110 Appeals. (1) A data supplier may request an appeal of a denial of its administrative review conducted in accordance with WAC 82-75-100.

(2) Request for an appeal must be submitted in writing to the office within fifteen calendar days after receipt of written notification of denial of its administrative review.

(3) Within ten business days of receipt of a written notice of appeal, the office 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 office employees may attend a hearing, and the ALJ will notify the appellant when other office 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. Either party or both may file a petition for review of the final decision to superior court. If neither party files an appeal 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: 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 82-75-200 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 office.

(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 web site that the lead organization is required to maintain.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-200, filed 11/1/16, effective 12/2/16.]

WAC 82-75-210 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 82-75-220.

(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: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-210, filed 11/1/16, effective 12/2/16.]

WAC 82-75-220 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.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-220, filed 11/1/16, effective 12/2/16.]

WAC 82-75-230 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 office 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 web site 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 web site. 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 deci-

sion 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 82-75-280.

(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 web site maintained by the lead organization.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-230, filed 11/1/16, effective 12/2/16.]

WAC 82-75-240 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 82-75-500 through 82-75-520.

(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 web site.

[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 82-75-250 Data use agreement. (1) The lead organization must develop a standard data use agreement. The office 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 office 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: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-250, filed 11/1/16, effective 12/2/16.]

WAC 82-75-260 Confidentiality agreement. (1) The lead organization must develop a standard confidentiality agreement, as required, before data may be released. The office 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: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-260, filed 11/1/16, effective 12/2/16.]

WAC 82-75-270 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.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-270, filed 11/1/16, effective 12/2/16.]

WAC 82-75-280 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 fund-raising 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.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-280, filed 11/1/16, effective 12/2/16.]

WAC 82-75-290 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 office 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 office will post the petition and final decision on the office web site. The lead organization will provide a link to the petition and decision from its WA-APCD web site.

[Statutory Authority: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-290, filed 11/1/16, effective 12/2/16.]

WAC 82-75-300 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 82-75-290.

(2) Request for an appeal must be submitted in writing to the office 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 office, 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 office 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 office employees may attend a hearing, and the ALJ will notify the appellant when other office 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: Chapter 43.371 RCW. WSR 16-22-062, § 82-75-300, filed 11/1/16, effective 12/2/16.]

PRIVACY AND SECURITY PROCEDURES

WAC 82-75-400 Privacy and security. (1) RCW 43.371.070 (1)(d) authorizes the director of the office of financial management 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 office of financial management to adopt rules providing procedures for ensuring compliance with state and federal privacy laws.

(3) WAC 82-75-410 through 82-75-470 provide the procedures required in subsections (1) and (2) of this section.

[Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-400, filed 4/4/17, effective 5/5/17.]

WAC 82-75-410 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 office 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 office 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 office or the office of the state chief information security officer upon request.

[Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-410, filed 4/4/17, effective 5/5/17.]

WAC 82-75-420 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 82-75-410.

(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: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-420, filed 4/4/17, effective 5/5/17.]

WAC 82-75-430 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 office and the office of the state chief information security officer within thirty calendar days of receipt of the results.

[Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-430, filed 4/4/17, effective 5/5/17.]

WAC 82-75-440 Accountability. (1) The data vendor must submit an annual report to the lead organization, the office, and the office of the state chief information security officer 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 office 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: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-440, filed 4/4/17, effective 5/5/17.]

WAC 82-75-450 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 office 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 OFM-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 office and the state chief information security officer.

(2) Upon receiving approval from the office 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 office;

(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 82-75-440(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: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-450, filed 4/4/17, effective 5/5/17.]

WAC 82-75-460 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.

[Statutory Authority: Chapter 43.371 RCW. WSR 17-08-079, § 82-75-460, filed 4/4/17, effective 5/5/17.]

WAC 82-75-470 State oversight of compliance with privacy and security requirements. In order to ensure compliance with privacy and security requirements and procedures, the office 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: 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 82-75-500 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.

[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 82-75-510 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 82-75-210(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 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 82-75-520 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 82-75-510(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 43.371.050(6) and chapter 43.371 RCW. WSR 17-22-121, § 82-75-520, filed 10/31/17, effective 12/1/17.]