

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.

"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.

"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 data base 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.

"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 data base 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.

DATA REQUESTS AND RELEASE PROCEDURES

NEW SECTION

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.

NEW SECTION

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.

NEW SECTION

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.

NEW SECTION

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 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 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.

NEW SECTION

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).

(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.

NEW SECTION

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.

NEW SECTION

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.

NEW SECTION

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.

NEW SECTION

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 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.

NEW SECTION

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, e-mail 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.

NEW SECTION

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.