

NOTE: OFM received comments on the draft rule provisions, suggestions for additional provisions in some of the rules, and edits to the rule language. OFM added stakeholder comments on the rule provisions at the end of rule section to which the comments applied. OFM added the suggestions for additional provisions to the rule and identified them as stakeholder suggestions. OFM added edits to the rule language in track changes. Thank you for your input

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, and data release processes. The policies and procedures must be approved by the office.

(2) The lead organization ~~should~~ help data requesters 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 requester, 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.

Stakeholder suggested this provision be added:

4) The lead organization must maintain a website to allow for stakeholders to review data requests and an adequate timeframe to provide comments.

NEW SECTION

WAC 82-75-210 Procedures for Data Requests

(1) The lead organization must use an application process for data 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 request.

(ii) Research methodology and timeline for the project.

(iii) Copy of an Institutional Research Board (IRB) approval 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 any third-party organizations that may have access to the requested data. This information must include the same information required by the requester, as applicable.

Stakeholder comment: 82-75-210 (1) (a) (v) states the applicant must provide information on any "third-party organizations that may have access to the requested data." We suggest this be changed to say "third party organizations or individuals . . ."

Stakeholder suggested the following provision be added to 1(a):

(vi) Information to specify the level of detail of data to be released. I.e. provider specific, carrier-specific or aggregated data.

(b) Information regarding whether the requester has, within the 3 years prior to the data request date, violated a Data Use Agreement (DUA) or Confidentiality Agreement. Such information ~~should~~ must include, but not limited to, the facts surrounding the DUA violation or data breach, the cause of the

DUA violation or data breach, and all steps taken to correct the DUA violation or data breach and prevent a reoccurrence.

Stakeholder comment on (b): In addition to considering whether the requestor has violated a confidentiality agreement (CA) or non-disclosure agreement (NDA) in the past three years, language should be added to consider whether the requestor has been subject to regulatory action (either state or federal) related to a breach, paid a penalty, or been a party to a criminal or civil proceeding stemming from a breach.

Stakeholder comment: 82-75-210 (1)(b) requires that applicant provide information regarding whether the requestor has, within the 3 years prior to the data request, violated a data use agreement or confidentiality agreement. We suggest this be expanded to also include whether the applicant has experienced a data breach as defined in HIPAA or a state privacy law.

(c) Submittal of the project's Data Management Plan (DMP), which DMP ~~should~~ must include the information required in WAC 82-75-220.

Stakeholder Comment: Please define Data Management Plan.

(d) Require all recipients of protected health information (PHI) to provide copies of their data privacy and security policies and procedures.

Stakeholder comment on (1)(d): Personal health information (PHI) recipients should be required to sign something akin to a business associate agreement (BAA) here, that includes commitments to particular safeguards, indemnification language, etc.

Additional safeguards should be put in place to protect data suppliers in the event a requestor misuses discloses our data.

Stakeholder comment on 82-75-210(1)(d), we would like to be clear on the ability for the Lead Org to deny based on insufficient privacy and security protections. Will this authority be based on the then-current privacy and security policies/procedures submitted by the possible recipient? Or will the authority be based on the proposed privacy and security policies/procedures included in the DMP? Furthermore, what will the procedure be when an out-of-state requestor meets that state's requirements, but which are insufficient to meet WA state requirements?

NEW SECTION

WAC 82-75-220 Data Management Plan

(1) (a) The lead organization must require data requesters to submit data management plans with the data request application.

(b) Additional organizations that are involved in using the data in the data requesters' 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 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.

Stakeholder comment on (2)(a): The lead organization should sign an attestation indicating that it has required contractual agreements in place with any downstream third party vendors including cloud providers.

(b) Data sharing, electronic transmission and distribution, including the data requester'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 requester; and whether the DMPs will be subjected to periodic updates during the DUA period for the released data.

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

(i) Dispose of Washington All Payer Claims Database (WA-APCD) data files upon completion of its research.

(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 research projects is terminated, voluntarily or involuntarily.

(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 public review of data requests. The process must include a timeline for processing requests, and notification procedures to keep the requester updated on the progress of the review. The office shall have final approval over the process and

criteria used for review of data requests and all subsequent changes.

Stakeholder suggests adding 2 new sections:

(2) The lead organization must post all data requests on the website with identifying the request review period to allow stakeholders to review data requests and an adequate timeframe to provide comments.

(3) The lead organization must respond in writing to the comments if the data is released when written concerns are communicated.

~~(2-4)~~ 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 DRC must review the request and provide a recommendation regarding data release. 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 requester 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 submittal of a copy of the IRB letter to the lead organization.

Stakeholder comment: On review we would recommend clarifying the role of the Data Review Committee (DRC). The rules appear to read that it is OFM's intent that the DRC be convened to review each and every data request. That has the potential to be time consuming for members, administratively burdensome and has the potential to lead to unwarranted delays in reviews and decisions.

We would recommend that the DRC be utilized to determine the policy and procedures for staff to review requests and to provide periodic oversight and review of the release process assuring that all policies and procedures are followed and that decision making is sound.

(35) The lead organization may only deny a data request based on a reason set forth in WAC 82-75-280.

Stakeholder comment on (5): Data submitters should have a mechanism to submit comments during the data request process. In addition, a data request should be posted for several weeks before the lead organization or data request committee (DRC) makes a final decision on a data request.

(45) The lead organization must notify the requester of the final decision. The notification ~~should~~ shall include the process available for review or appeal of the decision.

(65) The lead organization must post all data requests prior to review and then post final decisions on the WA-APCD website 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 requester. 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 researchers and all other individuals, whether an employee of the requester or a third party contractor, who will have access to the data must sign. At a minimum, the confidentiality agreement developed for researchers must meet the requirements of RCW 43.371.050(4)(a).

Stakeholder comment on (1)(b): In addition to all of the actors mentioned, third party data storage or other IT vendors should be required to sign a confidentiality agreement.

(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 ~~that~~ 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 requester 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.

NEW SECTION

WAC 82-75-250 Data Use Agreement

(1) The lead organization must develop a standard data use agreement (DUA). 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 or otherwise by law.

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

(e) A requirement for completion of a ~~A~~ attestation by an officer of the data requester's corporation that the data requester will adhere to the WA-APCD's cell suppression policy regarding the publication or presentation to anyone who is not an authorized user of the data

(f) A requirement that all requester employees and all other individuals who access the data will sign a confidentiality agreement prior to data release. The confidentiality requirements ~~should~~ must be set out in the DUA as an appendix.

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

Stakeholder comment for (2) (f) and (g): Greater internal protocols are needed with the lead organization. In some situations, a lead organization may be a competitor to a data supplier, and will have data that may be used to bolster their position in that market. Therefore, merely requiring a signature on a document is insufficient, data suppliers must know how the data is being stored, how access to the data is being controlled, and how that access is documented and monitored.

(3) Breach of a data use agreement may result in immediate termination of the agreement. The data requester will be required to immediately destroy all WA-APCD data in its possession.

Stakeholder comment: The entity that destroyed data should certify that the data was properly destroyed.

Stakeholder comment: We suggest that the rules indicate that the data use agreement include a right by the lead organization to audit the recipients of the data to ensure that the recipients comply with the data use agreement and all applicable laws.

Stakeholder comment: Under 82-75-250, should there be a requirement that individuals/employees who will access data undergo or verify participation in privacy/security training?

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 requester employees and other third parties who may have access to the data.

(3) 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 requester'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 requester or individual whose agreement is terminated must immediately destroy all WA-APCD data in his or her possession and provide proof of the destruction to the lead organization within 7 business days.

Stakeholder Comment: Under 82-75-260(3), seven days seems excessive for destruction after violation - perhaps five business days (calendar week) would work better.

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 requester, its employees, subcontractors, and any other person provided access to the data.

(2) The proof of data destruction must be provided within 10 business days from the end of the project or termination of the DUA, whichever is sooner.

Stakeholder comment: The lead organization should consider how it will ensure the data requestor is protecting the data not stored or used on premises, e.g., cloud, unencrypted laptops, mobile devices, etc.

Stakeholder comment: Under 82-75-270, clarification that "all" and "all copies" includes electronic and other means, including extracts, sample print outs, etc.

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 requester has violated a data use agreement or confidentiality agreement within three years of the date of request.
- (2) Any person, other than the requester, who will have access to the data has violated a data use agreement or confidentiality agreement within three years of the date of request.
- (3) The proposed privacy and security protections in the data management plan are not sufficient to meet state standards.

Stakeholder Comment on 82-75-280(3): We would like to be clear on the ability for the Lead Org to deny based on insufficient privacy and security protections. Will this authority be based on the then-current privacy and security policies/procedures submitted by the possible recipient? Or will the authority be based on the proposed privacy and security policies/procedures included in the DMP? Furthermore, what will the procedure be when an out-of-state requestor meets that state's requirements, but which are insufficient to meet WA state requirements?

- (4) The information provided is incomplete or not sufficient to approve the data request.
- (5) The proposed purpose for accessing the data is not allowable under WA-APCD policies or state or federal statutes, or rules ~~or regulations, including Federal Trade Commission (FTC) and Department of Justice (DOJ) Statements of Antitrust Enforcement Policy in Health Care-Statement 6 which requires that appropriate safeguards and protections should be in place in order to ensure that the exchange or release of confidential and proprietary information does not facilitate collusion or anti-competitive behaviors, thereby reducing competition and increasing prices and availability of health care services.~~
- (6) 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 requester using data to identify patients using a particular product or drug to develop a marketing campaign to directly contact those patients; or
 - b. A requester using data ~~Data will be used~~ to directly contact patients for fundraising purposes.

Stakeholder comment: A data request should be declined if the requestor has been subject to regulatory action (either state or federal) related to a breach, paid a penalty, or been a party to a criminal or civil proceeding stemming from a breach

NEW SECTION

WAC 82-75-290 Process for Review of a -Declined Data Request

(1) A data requester 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 within thirty calendar days after notice of the denial. The petition shall include the following information:

(a) Data requester'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 requester'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 requester. A decision from the reviewing official shall be provided in writing to the data requester no later than thirty calendar days after receipt of the petition. A denial of the petition will include the reasons for the denial.

Stakeholder suggested the following provisions be added to this section:

(4) The petition for review must be submitted to the office, and served on both the lead organization.

(5) The office must post a record of all proceedings under this section on its website, for a period of not less than three years from the inception of the request for review.

Formatted: Indent: First line: 0", Line spacing: Multiple 1.15 li

NEW SECTION

WAC 82-75-300 Process to Appeal of Final Denial of Data Request

(1) A data requester may request an appeal of a 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.

(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~~ The data requester may file a petition for review of the final decision to superior court. ~~If the data requester does not file 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.

Stakeholder comment: Data suppliers should have standing in proceedings or disputes involving data requests. For example, if a data supplier had a poor experience with a particular entity, there should be some mechanism whereby the supplier's objection to the entity's request will be heard and considered

Stakeholder comment: A state agency cannot file a petition for judicial review.

AMENDATORY SECTION

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 requester 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 requester 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 and includes "health insurance policy". -

"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.

"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' health insurance policy or health benefit plan.

Commented [MS(1): Stakeholder suggests using "subscriber" instead of member. Use of the work "member" was decided in the Phase I rulemaking when the term "Washington covered person" was defined.

Commented [MS(2): Stakeholder suggests using subscriber's instead of members'. See comment above.

Stakeholder comment: Health Insurance Portability and Accountability Act (HIPAA) should be capitalized

DRAFT