

CONCISE EXPLANATORY STATEMENT

SUBJECT: Concise Explanatory Statement as required by RCW 34.05.325
WAC: Chapter 82-75 WAC, All-Payer Health Care Claims Database, Privacy and Security Procedures

Pursuant to RCW 34.05.325(6)(a):

(6)(a) Before it files an adopted rule with the code reviser, an agency shall prepare a concise explanatory statement of the rule:

- (i) Identifying the agency's reasons for adopting the rule;
- (ii) Describing differences between the text of the proposed rule as published in the register and the text of the rule as adopted, other than editing changes, stating the reasons for differences; and
- (iii) Summarizing all comments received regarding the proposed rule, and responding to the comments by category or subject matter, indicating how the final rule reflects agency consideration of the comments, or why it fails to do so.

In accordance with this requirement, the Office of Financial Management (OFM) prepared this concise explanatory statement for the rules related to privacy and security of the Washington all-payer health care claims database (WA-APCD). The rules are intended to provide the procedures for ensuring that privacy and security standards are met. These standards may be set by federal or state law, or by the Washington State Office of Chief Information Officer. In all events, it is necessary to ensure that the privacy of the data is maintained and that the security standards are understood and met to safeguard the public's data.

Reasons for adopting the rule.

Chapter 43.371 RCW directs the Office of Financial Management (OFM) to establish a statewide all-payer health care claims database to support transparent public reporting of health care information. To accomplish this requirement, OFM is further directed to select a lead organization to coordinate and manage the database. RCW 43.371.070(d) and (e) provide that the OFM director shall adopt rules necessary to implement this chapter including:

(d) Procedures for ensuring that all data received from data suppliers are securely collected and stored in compliance with state and federal law;

(e) Procedures for ensuring compliance with state and federal privacy laws (privacy rules).

Differences between the text of the proposed rule as published and the text of the rule as adopted.

Based on the comments received, a number of changes were made to the text of the proposed rules that were published. The adopted rules reflect these changes, which are more in the way of clarification than substantive changes. Since the adopted rules are not substantially different from the proposed rules, further comment is not needed.

The changes are as follows:

- WAC 82-75-410(1)(b) was changed to add that the provision in the data vendor contract that requires the vendor to keep logs and documentation on activities conducted pursuant to the security plan must be consistent with the state records retention requirements.
- WAC 82-75-410(1)(c) was changed to add that the detailed security process should include but not be limited to details regarding security risk assessments and corrective actions plans when deficiencies are discovered.
- WAC 82-75-420(3) was changed to clarify that the unique set of login credentials for each active data supplier is a unique set of login credentials for each individual acting on behalf of or at the direction of the data supplier, and not one login credential for the data supplier as an entity.
- WAC 82-75-450(3)(d) was changed from “requester” to “the data recipient” as that term is the correct one.
- WAC 82-75-470 was changed to clarify that both the office of the chief information officer and OFM may request the information listed. It was also clarified that this request is to be made to the lead organization.

Summary of comments, OFM response and reflection in the final rule.

OFM worked with stakeholders, including the Office of the Chief Information Officer Privacy Office and IT Security Office, a Privacy and Security Workgroup made up of members of both state agencies and the private sector, and the selected Lead Organization and Data Vendor. In addition, OFM staff did extensive research on both federal and state laws, and how other states have provided for the privacy and security of data in the states’ APCDs. Also, OFM received substantial input from stakeholders prior to drafting these rules, as well as comments on two versions of the rules developed. The comments requested and received were incorporated into the final version of the rules that were the subject of this hearing.

Once published, OFM received written comments from Premera Blue Cross and Cambia Health Solutions. Finally, OFM held a hearing on March 7, 2017 where the following organizations provided verbal comment

on the published rules; Cambia Health Solutions, Department of Social and Health Services and Office of Cyber Security within Washington Technology Solutions. Exhibit 1 is a summary of all the comments received and OFM's response.