

**Exhibit 1**  
**Privacy and Security Rules**  
**Summary of Stakeholder comments and OFM response to comments**

Stakeholder comments	OFM response to comments
<b>Department of Social and Health Services</b>	
WAC 82-75-450(3)(d). This provision requires the lead organization to track all requests with the “:requester.” This should be changed to require the lead organization to track all requests with “the data recipient.”	OFM agrees that the reference to “requester” is incorrect. The final rule has been changed to read “Track all requests and research projects and follow up with the data recipient when the research or project is expected to be completed; and.
<b>Office of Cyber Security, Washington Technology Solutions</b>	
WAC 82-75-470. The first sentence states that the office may request the information listed in this section. It is not clear from which organization the request is to be made. OFM should include language as to whether the request is to be made to the lead organization, data vendor, OFM, etc.	OFM agrees that it should be clear from whom the request is to be made. The request is to be made to the lead organization, which language has been added to the rule. In addition, the Office of the Chief Information Officer (OCIO) should also be able to request the information listed in the rule. The OCIO has been added to the sentence in this rule, authorizing it to request this information in addition to OFM.
<b>Cambia Health Solutions (CHS) (written and verbal comments)</b>	
1. WAC 82-75-410(1)(b). This section states that the data vendor contract should include a provision requiring it to keep logs and documentation on activities conducted pursuant to the security plan. The section does not state how long those records should be kept. CHS requests the section add language regarding the length of time the records must be kept.	1. The rule does not need specific language regarding the amount of time the records must be kept. State law dictates the length of time contract related records must be kept. Generally, this information must be maintained for 6 years after the termination of the contract. To make this section clearer, language will be added that the data vendor must keep this material “consistent with the state records retention requirements.”

<p>2. WAC 82-75-410(1)(c). This section provides for a detailed security process but lacks the details as to what that would include. The section should include security risk assessment requirement.</p> <p>3. WAC 82-75-420(3). This section can be improved by requiring the data vendor to provide a unique set of login credentials for each user, instead of one login credential for the data supplier.</p> <p>4. WAC 82-75-430(2). The data vendor must perform an annual penetration test. Data suppliers should receive an executive summary of the results.</p> <p>5. WAC 82-75-440(4). Data suppliers should receive an executive summary of the accountability report results. The report details results related to security assessments.</p> <p>6. WAC 82-75-450(3). The data vendor must have a breach response plan and should contact the data supplier if a breach of the supplier's information occurs.</p>	<p>2. OFM agrees that some additional detail regarding what should be included in the security process would be helpful. Language is added to require the detailed security process to include but not be limited to security risk assessments and corrective actions plans when deficiencies are discovered.</p> <p>3. CHS is misreading the section. It does require a unique set of login credentials for each user from the data supplier. To ensure clarity, this section is revised to make clear that each individual acting on behalf of or at the direction of a data supplier will have her/his own unique login credentials.</p> <p>4. In consultation with the OCIO, OFM disagrees with this request. It would be inconsistent with security protocols to release any information regarding the results of penetration tests and could place the APCD at risk.</p> <p>5. In consultation with the OCIO, OFM disagrees with this request. It would be inconsistent with security protocols to release any information regarding the results in the accountability report and could place the APCD at risk.</p> <p>6. This comment was previously provided and the proposed rules amended to incorporate these suggestions. CHS did not realize that the change had already been made.</p>
<p><b>Premera Blue Cross</b></p>	
<p>Premera's previously comments have been addressed. Premera does not have any additional comments or changes.</p>	<p>No response needed.</p>