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.]