

WAC 308-10A-201 Recipient compliance requirements. (1) Audits -

For a recipient receiving protected personal information:

(a) A recipient receiving recurring lists of protected personal information must undergo data security and permissible use audits as outlined in the data sharing agreement.

(b) A recipient receiving a one-time list containing protected personal information must demonstrate security controls are in place to protect the information and may be required to undergo audits as outlined in the data sharing agreement.

(c) A recipient receiving individual records of protected personal information is subject to audits.

(d) The department may conduct random audits of any recipient it deems necessary.

(e) The department will determine the frequency of all audits.

(f) The cost of all audits, including actual costs incurred by the department to coordinate, schedule, conduct, draft, receive, review, and report the audit up to the point when the department issues the final audit review or report, is the responsibility of the recipient.

(g) The department may suspend or terminate a recipient's access to data if the recipient fails to provide or allow an acceptable audit by the due date established by the department.

(h) The department will only accept third-party audits that meet department audit standards and are performed by auditors that meet independent third-party auditor qualifications.

(2) Subrecipient lists - A recipient must provide the department with a list of:

(a) All subrecipients and secondary subrecipients that received protected personal information originating from the recipient in the time frame requested; and

(b) All customers.

[Statutory Authority: RCW 46.01.110. WSR 23-19-010, § 308-10A-201, filed 9/7/23, effective 10/8/23.]