

Vaccine Loss Policy

Introduction

Proper vaccine storage, handling, and accountability are vital components to the success of the Washington State Department of Health's Adult and Childhood Vaccine Programs (AVP and CVP). This policy outlines processes and repercussions when vaccine is lost.

Scope

This policy applies to all Washington providers that receive publicly supplied adult and childhood vaccines.

Definitions

- **Provider:** An individual, partnership, private organization, or public organization enrolled in AVP or CVP.
- **Incident/Vaccine Loss:** Expired, spoiled, wasted, or lost/unaccounted for vaccine.
- **Negligence:** Failure to take reasonable action to prevent vaccine loss.

Expectations of Providers

- Providers agree to maintain proper storage and handling practices to avoid vaccine loss.
- Providers agree to manually review vaccine storage unit temperatures during clinic hours based on program requirements.
- Providers agree to follow the [Vaccine Temperature Excursion Guide](#) for any inappropriate storage conditions or temperature readings outside the recommended ranges as outlined in the manufacturers' package insert.
- Providers agree to report all vaccine loss using the online return function in the Washington State Immunization Information System (IIS).
- Providers agree to retain the monthly paper [Vaccine Loss Log](#) for three years and submit to WAAdultVaccines@doh.wa.gov or WACHildhoodVaccines@doh.wa.gov, depending on the loss scenarios listed below (Flu and COVID loss due to expiration only are exempt).

Note: If the vaccine loss was due to expiration of short-dated transferred vaccines from another provider, the receiving provider reporting the loss is exempt from the repercussions on the following page.

Vaccine Loss and Repercussions

In accordance with the Provider Agreement and Vaccine Management Plan, providers acknowledge and agree that the program may require the provider to complete additional training and/or purchase or update equipment to help reduce the risk for future vaccine loss. The program will work in partnership with the provider to determine if the loss was due to negligence. See the scenarios and repercussion key below.

Vaccine Loss Scenarios

- Provider's first incident within 365 days that's greater than \$2,500 but less than \$10,000 (A,B,C).
- Provider experiences any additional negligent incidents that are greater than \$2,500 within 365 days of their most recent negligent incident (A,B,C,D,E).
- Provider experiences any negligent incident greater than \$10,000 (A,B,C,D,E).
- Provider continues to have negligent incidents (A,B,C,D,E,F).
- Provider fails to comply with the Vaccine Loss policy (A,G,H).

Repercussion Key

- A. The program may turn off provider vaccine ordering permissions until issue is resolved.
- B. The program will provide an email and resources to educate the provider regarding their incident.
- C. The program will require the provider to submit their Vaccine Loss Log outlining the incident and actions they plan to take to prevent future vaccine loss.
- D. The program will require providers to complete additional training regarding vaccine storage and handling procedures.
- E. The program may require the provider to purchase or update equipment to help reduce the risk for future incidents (i.e. digital data loggers, remote monitoring data loggers, or pharmaceutical grade storage units).
- F. The program may perform an unannounced site visit to ensure the provider is following best practices.
- G. DOH may put the provider on probation.
- H. DOH may disenroll provider if conditions of probation are not met.

Reasons of negligence include but are not limited to the following:

- Failure to open vaccine shipments from McKesson, Merck, or Pfizer immediately, resulting in damaged and non-viable vaccine.
- Failure to rotate vaccine stock, resulting in preventable expired vaccine.
- Failure to alert the program three months prior to vaccine expiration to determine vaccine transfer options.
- Not requesting prior approval from the program to transfer vaccine and/or transferring vaccine inappropriately, thereby potentially impairing vaccine viability.
- Failure to follow an emergency response plan.
- Using publicly supplied childhood vaccine for adult populations or using publicly supplied adult vaccine for unapproved populations.
- Freezing vaccine intended to be refrigerated and/or refrigerating vaccine intended to be frozen.
- Failure to maintain proper refrigeration and/or freezer temperatures.
 - ▶ Refrigerator or freezer left unplugged.
 - ▶ Electrical breaker switched off by provider staff, contractors, or any other individual.
 - ▶ Refrigerator or freezer door left open or ajar by staff, contractors, or any other individual.
 - ▶ Any power outage in which the provider fails to act according to their vaccine storage back up plan.
 - ▶ Not having correct/certified thermometers and/or incorrect placement in each vaccine refrigerator and freezer compartment.
 - ▶ Failure to read and record refrigerator and freezer temperatures, and/or failure to take immediate corrective action when temperatures are determined to be out of range.
- Vaccine left out of the storage unit.
- Failure to notify the program when provider office hours change or the provider address changes, resulting in vaccine not being delivered and consequently becoming non-viable.
- Discarding non-expired vaccine prior to stated expiration date.
- Routinely pre-drawing (pre-filling) syringes that go unused resulting in non-viable vaccine. Pre-drawing vaccines for later use, even if kept within temperature requirements so the vaccine stays viable, is not acceptable. Routinely pre-drawing syringes is not a best practice and is against state and federal vaccine requirements. Pre-drawing is acceptable if done following CDC guidelines for mass immunization clinics.
- Failure to use continuous temperature monitoring devices (data loggers) and required back-up thermometers to monitor vaccines during routine onsite storage of vaccine, during transport of vaccine, and during mass vaccination clinics.
- Any other preventable incidents made by provider.