RCW 70.58A.060 Vital records system security requirements—Fraud detection—Data validation. (1) A person may not prepare or issue any vital record that purports to be an original, certification of, or copy of a vital record except as authorized in this chapter.

(2) All certifications of vital records must include security features to deter alteration, counterfeiting, or simulation without ready detection.

(3) All informational copies must indicate that they cannot be used for legal purposes on their face.

(4) The state registrar may:

(a) Authorize users of the vital records system to access specific components of the vital records system based on their official duties;

(b) Require users authorized under this section to acknowledge having read and understood security procedures and penalties;

(c) Revoke user access of the vital records system when the user violates security procedures or when the user no longer needs access to conduct official duties;

(d) Ensure that state birth records are marked as deceased upon receipt of death records; and

(e) Periodically test and audit the vital records system for purposes of detecting fraud. If fraud is suspected, the state registrar may provide copies of the evidence to appropriate authorities for further investigation consistent with the provisions of RCW 70.58A.580. The state registrar may retain the results of such tests and audits, which are not subject to inspection or copying except upon order of a court of competent jurisdiction.

(5) The state registrar may, at the state registrar's discretion, validate data provided in reports filed for registration through site visits or with independent sources outside the vital records system at a frequency specified by the state registrar to maximize the integrity of the data collected. [2019 c 148 s 7.]