RCW 40.26.020 Biometric identifiers—Notice and consent—Agencies—Use, storage, retention—Review—Definitions—Exceptions. (1) Unless authorized by law, an agency may not collect, capture, purchase, or otherwise obtain a biometric identifier without first providing notice and obtaining the individual's consent, as follows:

(a) The notice provided must clearly specify the purpose and use of the biometric identifier; and

(b) The consent obtained must be specific to the terms of the notice, and must be recorded and maintained by the agency for the duration of the retention of the biometric identifier.

(2) Any biometric identifier obtained by an agency:

(a) May not be sold;

(b) May only be used consistent with the terms of the notice and consent obtained under subsection (1) of this section, or as authorized by law; and

(c) May be shared, including with other state agencies or local governments, only:

(i) As needed to execute the purposes of the collection, consistent with the notice and consent obtained under subsection (1) of this section, or as authorized by law; or

(ii) If such sharing is specified within the original consent.

(3) An agency that collects, purchases, or otherwise obtains biometric identifiers must:

(a) Establish security policies that ensure the integrity and appropriate confidentiality of the biometric identifiers;

(b) Address biometric identifiers in the agency's privacy policies;

(c) Only retain biometric identifiers necessary to fulfill the original purpose and use, as specified in the notice and consent obtained under subsection (1) of this section, or as authorized by law;

(d) Set record retention schedules tailored to the original purpose of the collection of biometric identifiers;

(e) Otherwise minimize the review and retention of the biometric identifiers, consistent with state record retention requirements; and

(f) Design a biometric policy to ensure that the agency is minimizing the collection of biometric identifiers to the fewest number necessary to accomplish the agency mission.

(4) The use and storage of biometric identifiers obtained by an agency must comply with all other applicable state and federal laws and regulations, including the health insurance portability and accountability act (HIPAA), the family educational rights and privacy act (FERPA), regulations regarding data breach notifications and individual privacy protections, and any policies or standards published by the office of the chief information officer.

(5) Biometric identifiers may not be disclosed under the public records act, chapter 42.56 RCW.

(6) Agency policies, regulations, guidance, and retention schedules regarding biometric identifiers must be reviewed annually to incorporate any new technology, as appropriate, and respond to citizen complaints.

(7) The definitions in this subsection apply throughout this section unless the context requires otherwise.

(a) "Agency" means every state office, department, division, bureau, board, commission, or other state agency.

(b) "Biometric identifier" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's retina or iris scan, fingerprint, voiceprint, DNA, or scan of hand or face geometry, except when such information is derived from:

(i) Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color;

(ii) Donated organ tissues or parts, or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency;

(iii) Information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996; or

(iv) X-ray, roentgen process, computed tomography, magnetic resonance imaging (MRI), positron emission tomography (PET) scan, mammography, or other image or film of the human anatomy used to diagnose, develop a prognosis for, or treat an illness or other medical condition or to further validate scientific testing or screening.

(8) Subsection (1) of this section does not apply to general authority Washington law enforcement agencies, as defined under RCW 10.93.020.

(9)(a) For purposes of the restrictions and obligations in subsection (1) of this section, "biometric identifier" does not include fingerprints or DNA for the following:

(i) Limited authority Washington law enforcement agencies, as defined under RCW 10.93.020;

(ii) Agencies authorized by statute to confine a person involuntarily, or to petition for such confinement; and

(iii) The attorney general's office when obtaining or using biometric identifiers is necessary for law enforcement, legal advice, or legal representation.

(b) When an agency listed under (a) of this subsection has a need to collect, capture, purchase, or otherwise obtain a biometric identifier other than a fingerprint or DNA to fulfill a purpose authorized by law, for either an individual circumstance or a categorical circumstance, the requirements of subsection (1) of this section are waived upon such agency providing prompt written notice to the state's chief privacy officer and to the appropriate committees of the legislature, stating the type of biometric identifier at issue and the general circumstances requiring the waiver. [2017 2nd sp.s. c 1 § 1; 2017 c 306 § 2.]

Effective date—2017 2nd sp.s. c 1: "This act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and takes effect on the date that Substitute House Bill No. 1717 takes effect [July 23, 2017]." [2017 2nd sp.s. c 1 § 2.]