RCW 42.56.590 Personal information—Notice of security breaches.

(1) Any agency that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

(2) Any agency that maintains or possesses data that may include personal information that the agency does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section and except under subsection (5) of this section and RCW 42.56.592, notice may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or

(c) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) Email notice when the agency has an email address for the subject persons;

(ii) Conspicuous posting of the notice on the agency's website page, if the agency maintains one; and

(iii) Notification to major statewide media.

(5) An agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(6) Any agency that is required to issue notification pursuant to this section shall meet all of the following requirements:

(a) The notification must be written in plain language; and

(b) The notification must include, at a minimum, the following information:

(i) The name and contact information of the reporting agency subject to this section;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and

(iv) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

(7) Any agency that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall notify the attorney general of the breach no more than thirty days after the breach was discovered.

(a) The notice to the attorney general must include the following information:

(i) The number of Washington residents affected by the breach, or an estimate if the exact number is not known;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach;

(iv) A summary of steps taken to contain the breach; and

(v) A single sample copy of the security breach notification, excluding any personally identifiable information.

(b) The notice to the attorney general must be updated if any of the information identified in (a) of this subsection is unknown at the time notice is due.

(8) Notification to affected individuals must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered, unless the delay is at the request of law enforcement as provided in subsection (3) of this section, or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. An agency may delay notification to the consumer for up to an additional fourteen days to allow for notification to be translated into the primary language of the affected consumers.

(9) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

(10)(a) For purposes of this section, "personal information" means:

(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements:

(A) Social security number or the last four digits of the social security number;

(B) Driver's license number or Washington identification card number;

(C) Account number, credit or debit card number, or any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account;

(D) Full date of birth;

(E) Private key that is unique to an individual and that is used to authenticate or sign an electronic record;

(F) Student, military, or passport identification number;

(G) Health insurance policy number or health insurance identification number;

(H) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or

(I) Biometric data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;

(ii) User name or email address in combination with a password or security questions and answers that would permit access to an online account; and

(iii) Any of the data elements or any combination of the data elements described in (a)(i) of this subsection without the consumer's first name or first initial and last name if:

(A) Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and

(B) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

(b) Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(11) For purposes of this section, "secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person. [2020 c 65 s 1; 2019 c 241 s 5; 2015 c 64 s 3; 2007 c 197 s 9; 2005 c 368 s 1. Formerly RCW 42.17.31922.]

Effective date—2019 c 241: See note following RCW 19.255.010.

Intent—2015 c 64: See note following RCW 19.255.010.

Similar provision: RCW 19.255.010.