Washington Personal Information Protection

Washington regulates the protection of personal information as follows:

What is Considered Personal Information

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social security number;
- Driver's license number or Washington identification card number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

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

Requirements for Employers

- Any entity that conducts business in Washington and that **owns or licenses** data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any Washington resident whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person and the personal information was not secured.
    - Note: 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.
- Any person or business that maintains data that includes personal information **that the person or business does not own** must 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.
- Any business that is required to issue notification under the law must meet **all of the following requirements**:
    - The notification must be written in plain language; and
    - The notification must include (at a minimum) the following information:
        - The name and contact information of the reporting person or business subject to the law;
        - A list of the types of personal information that were—or are reasonably believed to have been—the subject of a breach; and
        - The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.
- Any business that is required to issue a notification to **more than 500** Washington residents as a result of a single breach must, by the time notice is provided to affected consumers, **electronically submit** a single sample copy of that security breach notification—excluding any personally identifiable information—to the state attorney general. The business must also **provide the attorney general** with the number of Washington consumers affected by the breach (or an estimate if the exact number is not known).
- Notification to affected consumers and to the attorney general must be made in the most expedient time possible and without unreasonable delay, no more than **45 calendar days** after the breach was discovered

(unless at the request of law enforcement or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system).

Note: Special rules apply to HIPAA covered entities and certain financial institutions.

Participation in EAPs

On March 4, 2022, the state of Washington adopted senate bill (SB) 5564. SB 5564 seeks to encourage employee participation in employee assistance programs (EAPs) by strengthening privacy and anti-retaliation protections for program participants. The new law becomes effective on June 9, 2022.

An EAP is a program offered by employers to assist employees with work and life concerns. EAPs may provide support to employees for depression, stress, addictions, anger, parenting, relationships, and grief and loss. EAPs may also provide support regarding legal and financial concerns.

The new law prohibits employers from obtaining individually identifiable information regarding their employees' participation in an EAP. Individually identifiable information gathered in the process of conducting an EAP must be kept confidential.

In addition, employee participation or nonparticipation in an EAP must not be a factor in a decision affecting the employee's job security, promotional opportunities, corrective or disciplinary action or other employment rights.

Exceptions

EAP participation protections extended by this law do not apply to:

- Disclosures permitted or required by law (RCW 41.04.730, 18.225.105, 70.02.050 or 71.05.120);
- Disclosures to an employer regarding an employee's attendance if the employee was required to attend as a condition of continued employment; or
- Disclosures that are made to prevent or lessen a perceived threat to the health or safety of an individual or the public.

For More Information

- Washington Breach Notification Law
- 2015 Amendments to the Law
- State Attorney General