State Law Changes to Data Breach Notification Requirements

By Christal Harrison-Delgado (charrisondelgado@omwlaw.com)

In 2020, the Washington State Legislature implemented modifications to certain data breach notification requirements, which require private and public entities to provide notification of data breaches involving Personal Information, including Protected Health Information ("PHI"). These changes affect Chapters 19.255 and 42.56 of the RCWs regarding private and public entities, respectively. These modifications would impact private and public entities who: (1) own or license data which includes Personal Information, and/or (2) maintain or possess data that may include Personal Information that the entity does not own or license.

These changes became effective on March 1, 2020 under HB 1071. One of the most notable modifications expressed in the statutes is the expansion upon the definition of "Personal Information." The following elements are now included within the definition of "Personal Information" if combined with either (1) an individual's first name or (2) an individual's first initial and last name:

- Full Date of Birth;
- Private key that is unique to an individual which is used to authenticate or sign an electronic record;
- Student, military, or passport identification number;
- Health insurance policy number or health insurance identification number;
- Any information about a consumer's medical history (or mental or physical condition), or any information about a health care professional's medical diagnosis or treatment of the consumer;
- 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; or
- Username or email address in combination with a password or security question(s) and answer(s) that would permit access to an online account.[1]

Effective June 11, 2020, under SB 6187, RCW 42.56.590 now includes the last four digits of a person's Social Security Number within the definition of "Personal Information". However, this addition concerns public entities only.

Additionally, any of the foregoing data elements (or any combination of the foregoing data elements) are now included within the definition of "Personal Information" without (1) an individual's first name or (2) an individual's first initial and last name if:

- Encryption, redaction, or other methods have not rendered the data element (or combination of data elements) unusable; and
- The data element (or combination of data elements) would enable a person to commit identity theft against a consumer.

[1] The former definition of "Personal Information" included the following elements if combined with either (1) an individual's first name or (2) an individual's first initial and last name: 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, or any other numbers or information that can be used to access a person's financial account.

Another noteworthy modification to the breach notification requirements is the timeframe within which public and private entities (as the case may be) must notify both the individuals affected by the breach and the Attorney General. The modification shortens the time frame, from the original 45 days, to 30 days. Additionally, all notices must now include (1) the date of the breach and (2) the date of the entity's discovery of the breach.

Further, all notices provided to the Attorney General must now include more information, including:

- A list of the types of Personal Information that were (or are reasonably believed to have been) the subject of the breach;
- A summary of measures taken to contain the breach; and
- A copy of the security breach notification after having redacted any personally identifiable information.

If any of the above information is unknown by the time the notice is due to the Attorney General, the notice must be updated once the information is available.

Modifications to the breach notification requirements now allow private entities to email individuals the breach notification, but only if the breach involves Personal Information including a username or password. If the breach did not include a username or password, then private entities may not utilize email notification as the primary breach notification method. This change allows for a more timely notice to affected individuals so they may change their login information more quickly than they would if other notification methods were used.

However, if the breach involves login credentials of an email account furnished by the private entity, the notice cannot be sent to that email address and must be sent using written, electronic, or substitute notice. However delivered, the notice must also inform the person whose Personal Information has been breached to promptly change his or her password and security question(s) and answer(s), as applicable, or to take other appropriate steps to protect the online account with the notifying entity as well as all other online accounts for which the person uses the same user name/email address and password or security question(s) and/or answer(s).

It is important to note that none of these changes affect the exceptions for Covered Entities under the Health Insurance Portability and Accountability Act (HIPAA). Under RCW 19.255.030 and RCW 42.56.592, Covered Entities (not including Business Associates) will be deemed to have complied with state law requirements if they comply with the requirements under the Health Information Technology for Economic and Clinical Health (HITECH) Act regarding breaches involving PHI.

For more information regarding this guidance, please contact Christal Harrison-Delgado at charrisondelgado@omwlaw.com.