Washington "My Health, My Data" Act Summary

On April 27, 2023, Governor Jay Inslee (D) signed HB 1155, the "My Health, My Data Act" into law. For most covered entities the Act takes effect on March 31, 2024, however, small businesses will have until June 30, 2024. While the Act is branded as a health data privacy bill, it is likely to affect businesses in all industries due to its vague definitions and overly broad scope of covered data and entities. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **My Health, My Data Act** applies to any legal entity that: (a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data. The Act does not apply to government agencies, tribal nations, or contracted services providers when processing consumer health data on behalf of the government agency.
Covered Data	***"Personal Information"***: information that identifies or is reasonably capable of being associated or linked, directly or indirectly, with a particular consumer, including data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier. Does NOT include deidentified data or publicly available information. ***"Consumer Health Data"***: personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status. "Physical or mental health status" includes, but is not limited to: (a) individual health conditions, treatment, diseases, or diagnosis; (b) social, psychological, behavioral, and medical interventions; (c) health-related surgeries or procedures; (d) use or purchase of prescribed medication: (e) bodily functions, vital signs, symptoms, or certain measurements; (f) diagnoses or diagnostic testing, treatment, or medication; (g) gender-affirming care information; (h) reproductive or sexual health information; (i) biometric data; (j) genetic data; (k) precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies; (l) data that identifies a consumer seeking health care services; or (m) any information that a regulated entity or a small business, or their respective processor, processes to associate or identity a consumer with certain data that is derived or extrapolated from non-health information (i.e., proxy, derivative, inferred, or emergent data, including algorithms or machine learning). Employee and business to business data is not considered within the scope. ***"Genetic Data"***: any data, regardless of its format, that concerns a consumer's generic characteristics. ***"Reproductive or Sexual Health Information"***: personal information relating to seeking or obtaining past, present, or future reproductive or sexual health services, including: (a) precise location information that could reasonably indicate a consumer's attempt to acquire or receive reproductive or sexual health services; (b) efforts to research or obtain reproductive or sexual health services; (c) any reproductive or sexual health information that is derived, extrapolated, or inferred, including from non-health information.
Key Definitions	***"Biometric Data":*** data that is generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data. Biometric data includes, but is not limited to: (a) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; or (b) Keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information." The Act adopts a broader definition than the one used by the state's existing biometric privacy law, RCW 19.375.010. ***"Consent"***: a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in,

	voluntary, and unambiguous agreement, which may include written consent provided by electronic means. The Act also creates a new consent regime, requiring separate consent for sharing data and collecting or processing data beyond what is in the notice; and standalone written "authorization" for the sale of consumer health data. ***"Collect":*** means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner. ***"Deceptive Design":*** a user interface designed or manipulated with the effect of subverting or impairing user autonomy, decision making, or choice. ***"Deidentified Data"***: data that cannot reasonably be used to infer information about, or otherwise linked to, an identified or identifiable consumer, or a device linked to such a consumer, if the regulated entity or the small business that possesses such data (a) take reasonable measures to ensure that such data cannot be associated with a consumer; (b) publicly commits to process such data only in a deidentified fashion and not attempt to reidentify such data; and (c) contractually obligates any recipients of such data to satisfy the specified criteria. ***"Process" or "Processing":*** means any operation or set of operations performed on consumer health data. ***"Sell" or "sale":*** the exchange of consumer health data for monetary or other valuable consideration.
Consumer Rights	• **Access**: A consumer has the right to confirm whether a regulated entity or a small business is collecting, sharing, or selling consumer health data concerning the consumer and to access such data, including a list of all third parties and affiliates with whom the regulated entity or the small business has shared or sold the consumer health data and an active email email address or other online mechanism that the consumer may use to contact these third parties. • **Affirmative Consent:** A regulated entity shall not sell or offer to sell consumer health data concerning a consumer without first obtaining valid authorization from the consumer. The sale of consumer health data must be consistent with the valid authorization signed by the consumer. • **Deletion**: A consumer has the right to have consumer health data concerning the consumer deleted and may exercise that right by informing the regulated entity or the small business of the consumer's request for deletion. • **Revocation:** A consumer has the right to withdraw consent from the regulated entity or small business collection and sharing of consumer health data concerning the consumer.
Business Obligations	• **Responding to Consumer Requests**: A regulated entity or small business must establish a secure and reliable means for consumers to exercise their rights set forth in the Act and describe such means in its consumer health data privacy policy. The method must take into account the ways in which consumers normally interact with the regulated entity or small business, the need for secure and reliable communication, and the ability to authenticate the identity of the consumer making the request. A regulated entity may not require a consumer to create a new account to exercise consumer rights. A regulated entity is not required to comply with a request if it is unable to authenticate a consumer request using commercially reasonable efforts and may request that a consumer provide additional information to authenticate the consumer request. A regulated entity and a small business must comply with a consumer request without undue delay, but in all cases within 45 days of receipt of the request. A regulated entity and a small business must promptly take steps to authenticate a consumer request, but this does not extend the duty to comply with the consumer request within 45 days of receipt of the request. The response period may be

	extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, slo long as the regulated entity or small business informs the consumer of the extension within the initial 45-day response period, together with the reason for the extension. A regulated entity and small business must establish a process for a consumer to appeal the regulated entity or small business's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process must be conspicuously available and similar to the process for submitting consumer requests. Within 45 days of receipt of an appeal, a regulated entity or small business must inform the consumer in writing of any action taken or not taken in response to the appeal, along with an explanation of the reasons for the decisions. If the appeal is denied, the regulated entity or small business must provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint. A regulated entity or small business must respond to a consumer request free of charge up to twice annually. If requests from a consumer are manifestly unfounded, excessive or repetitive, the regulated entity or small business may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The regulated entity and small business bear the burden of demonstrating that a consumer request is manifestly unfounded, excessive, or repetitive in nature. • **Data Minimization**: A regulated entity may not collect, use, or share additional categories of consumer health data not disclosed in the consumer health data privacy policy without first disclosing the additional categories and obtaining the consumer's affirmative consent prior to the collection, use, or sharing of such consumer health data. • **Avoid Secondary Use:** A regulated entity or small business may not collect, use, or share consumer health data for additional purposes not disclosed in the consumer health data privacy policy without first disclosing the additional purposes and obtaining the consumer's affirmative consent. • **Data Security**: A regulated entity and small business must establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy a reasonable standard of care within the regulated entity or the small business's industry to protect the confidentiality, integrity and accessibility of consumer health data appropriate to the volume and nature of the consumer health data at issue. • **No Unlawful Discrimination:** A regulated entity or small business may not unlawfully discriminate against a consumer for exercising any rights included in the Act. • **Transparency**: A regulated entity and a small business shall maintain a consumer health data privacy policy that clearly and conspicuously discloses: (a) the categories of consumer health data collected and the purpose for which the data is collected, including how the data will be used; (b) the categories of sources from which the consumer health data is collected; (c) the categories of consumer health data that is shared; (d) a list of the categories of third parties and specific affiliates with whom the regulated entity or the small business shares the consumer health data; and (e) how a consumer can exercise the rights provided in the Act. A regulated entity and a small business must prominently publish a link to its consumer health data privacy policy on its homepage.
Controller / Processor Distinction	A processor may process consumer health data pursuant only to a binding contract between the processor and regulated entity or the small business that sets forth the processing instructions and limit the actions the processor may take with respect to the consumer health data it processes on behalf of the regulated entity or small business. A processor may process consumer health data only in a manner that is consistent with the binding instructions set forth in the contract with the regulated entity or small business. A processor shall assist the regulated entity or small business by appropriate technical and organizational measures, insofar as this is possible in fulfilling the regulated entity and

	the small business obligations under the Act. If a processor fails to a adhere to the regulated entity or small business instructions or processes consumer health data this is outside the scope of the processor's contract with the regulated entity or the small business, the processor is considered a regulated entity or small business with regard to such data and is subject to all the requirements with regard to such data.
Exceptions and Exemptions	• The Act does not restrict a regulated entity, small business, or processor's ability to collect, use , or disclose consumer health data to: (a) prevent, detect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under state or federal law; (b) preserve the integrity or security of systems; or (c) investigate, report, or prosecute those responsible for any such action this is illegal under state or federal law. • Data exempt from Act includes: information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, FERPA, the Gramm-Leach-Bliley Act.
Enforcement	• The Act provides for both **attorney general enforcement and a private right of action** under the Washington Consumer Protection Act. • The Act provides that a joint committee must review enforcement actions brought by the attorney general and consumers to enforce violations of the Act. The report, at minimum, must include: (a) the number of enforcement actions reported by the attorney general, a consumer, a regulated entity, or a small business that resulted in a settlement, including the average settlement amount; (b) the number of complaints reported, including the categories of complaints and the number of complaints for each category; (c) the number of enforcement actions brought by the attorney general and consumers, including the categories of violations and number of violations per category; (d) the number of civil actions where a judge determined the position of the nonprevailing party was frivolous; (e) the types of resources, including associated costs, expended by the attorney general, a consumer, a regulated entity, or a small business for enforcement actions; and (f) recommendations for potential changes to enforcement of the Act. • **Right to Cure**: The Act does not include a right to cure.