**1155-S.E AMS SHOR S3026.1 - NOT FOR FLOOR USE**

**ESHB 1155** - S AMD TO S AMD (S-2826.4/23) **303**

By Senator Short

**NOT ADOPTED 04/05/2023**

Beginning on page 9, line 1, strike all of sections 4 through 9 and insert the following:

"NEW SECTION. **Sec.**  (1) 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 section 6 of this act.

(2) A regulated entity and a small business shall prominently publish a link to its consumer health data privacy policy on its home page.

(3) A regulated entity or a small business 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.

(4) A regulated entity or a 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 prior to the collection, use, or sharing of such consumer health data.

(5) It is a violation of this chapter for a regulated entity or a small business to contract with a processor to process consumer health data in a manner that is inconsistent with the regulated entity's or the small business's consumer health data privacy policy.

NEW SECTION. **Sec.**  (1) A regulated entity or a small business may not collect any consumer health data except:

(a) With consent from the consumer for such collection for a specified purpose; or

(b) To the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business.

(2) A regulated entity or a small business may not share any consumer health data except:

(a) With consent from the consumer for such sharing that is separate and distinct from the consent obtained to collect consumer health data; or

(b) To the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business.

(3) Consent required under this section must be obtained prior to the collection or sharing, as applicable, of any consumer health data, and the request for consent must clearly and conspicuously disclose: (a) The categories of consumer health data collected or shared; (b) the purpose of the collection or sharing of the consumer health data, including the specific ways in which it will be used; (c) the categories of entities with whom the consumer health data is shared; and (d) how the consumer can withdraw consent from future collection or sharing of the consumer's health data.

(4) A regulated entity or a small business may not unlawfully discriminate against a consumer for exercising any rights included in this chapter.

NEW SECTION. **Sec.**  (1) 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 address or other online mechanism that the consumer may use to contact these third parties.

(2) A consumer has the right to withdraw consent from the regulated entity's or the small business's collection and sharing of consumer health data concerning the consumer.

(3) 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.

(a) A regulated entity or a small business that receives a consumer's request to delete any consumer health data concerning the consumer shall:

(i) Delete the consumer health data from its records, including from all parts of the regulated entity's or the small business's network, including archived or backup systems pursuant to (c) of this subsection; and

(ii) Notify all affiliates, processors, contractors, and other third parties with whom the regulated entity or the small business has shared consumer health data of the deletion request.

(b) All affiliates, processors, contractors, and other third parties that receive notice of a consumer's deletion request shall honor the consumer's deletion request and delete the consumer health data from its records, subject to the same requirements of this chapter.

(c) If consumer health data that a consumer requests to be deleted is stored on archived or backup systems, then the request for deletion may be delayed to enable restoration of the archived or backup systems and such delay may not exceed six months from authenticating the deletion request.

(4) A consumer may exercise the rights set forth in this chapter by submitting a request, at any time, to a regulated entity or a small business. Such a request may be made by a secure and reliable means established by the regulated entity or the small business and described 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 the small business, the need for secure and reliable communication of such requests, and the ability of the regulated entity or the small business to authenticate the identity of the consumer making the request. A regulated entity or a small business may not require a consumer to create a new account in order to exercise consumer rights pursuant to this chapter but may require a consumer to use an existing account.

(5) If a regulated entity or a small business is unable to authenticate the request using commercially reasonable efforts, the regulated entity or the small business is not required to comply with a request to initiate an action under this section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(6) Information provided in response to a consumer request must be provided by a regulated entity and a small business free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the regulated entity or the 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 the small business bear the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

(7) A regulated entity and a small business shall comply with the consumer's requests under subsections (1) through (3) of this section without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described in this section. A regulated entity and a small business must promptly take steps to authenticate a consumer request but this does not extend the regulated entity's and the small business's duty to comply with the consumer's request within 45 days of receipt of the consumer's 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, so long as the regulated entity or the small business informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

(8) A regulated entity and a small business shall establish a process for a consumer to appeal the regulated entity's or the 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 requests to initiate action pursuant to this section. Within 45 days of receipt of an appeal, a regulated entity or a small business shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the regulated entity or the small business shall also 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.

NEW SECTION. **Sec.**  A regulated entity and a small business shall:

(1) Restrict access to consumer health data by the employees, processors, and contractors of such regulated entity or small business to only those employees, processors, and contractors for which access is necessary to further the purposes for which the consumer provided consent or where necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business; and

(2) Establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable standard of care within the regulated entity's 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.

NEW SECTION. **Sec.**  (1)(a) A processor may process consumer health data only pursuant to a binding contract between the processor and the regulated entity or the small business that sets forth the processing instructions and limits the actions the processor may take with respect to the consumer health data it processes on behalf of the regulated entity or the small business.

(b) 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 the small business.

(2) A processor shall assist the regulated entity or the small business by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the regulated entity's and the small business's obligations under this chapter.

(3) If a processor fails to adhere to the regulated entity's or the small business's instructions or processes consumer health data in a manner that 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 a small business with regard to such data and is subject to all the requirements of this chapter with regard to such data.

NEW SECTION. **Sec.**  (1) It is unlawful for any person to 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. This authorization must be separate and distinct from the consent obtained to collect or share consumer health data, as required under section 5 of this act.

(2) A valid authorization to sell consumer health data is a document consistent with this section and must be written in plain language. The valid authorization to sell consumer health data must contain the following:

(a) The specific consumer health data concerning the consumer that the person intends to sell;

(b) The name and contact information of the person collecting and selling the consumer health data;

(c) The name and contact information of the person purchasing the consumer health data from the seller identified in (b) of this subsection;

(d) A description of the purpose for the sale, including how the consumer health data will be gathered and how it will be used by the purchaser identified in (c) of this subsection when sold;

(e) A statement that the provision of goods or services may not be conditioned on the consumer signing the valid authorization;

(f) A statement that the consumer has a right to revoke the valid authorization at any time and a description on how to submit a revocation of the valid authorization;

(g) A statement that the consumer health data sold pursuant to the valid authorization may be subject to redisclosure by the purchaser and may no longer be protected by this section;

(h) An expiration date for the valid authorization that expires one year from when the consumer signs the valid authorization; and

(i) The signature of the consumer and date.

(3) An authorization is not valid if the document has any of the following defects:

(a) The expiration date has passed;

(b) The authorization does not contain all the information required under this section;

(c) The authorization has been revoked by the consumer;

(d) The authorization has been combined with other documents to create a compound authorization; or

(e) The provision of goods or services is conditioned on the consumer signing the authorization.

(4) A copy of the signed valid authorization must be provided to the consumer.

(5) The seller and purchaser of consumer health data must retain a copy of all valid authorizations for sale of consumer health data for six years from the date of its signature or the date when it was last in effect, whichever is later."

On page 19, after line 4, insert the following:

"NEW SECTION. **Sec.**  Sections 4 through 9 of this act take effect July 31, 2025."

EFFECT: Aligns the effective dates for when regulated entities and small businesses must comply with this act to July 31, 2025.