MISSISSIPPI LEGISLATURE REGULAR SESSION 2024

By: Representative Porter To: Judiciary A

HOUSE BILL NO. 1268

AN ACT TO BE KNOWN AS THE "MISSISSIPPI PROTECT HEALTH DATA PRIVACY ACT"; TO DEFINE CERTAIN TERMS; TO REQUIRE REGULATED ENTITIES TO DISCLOSE AND MAINTAIN A HEALTH DATA PRIVACY POLICY THAT DISCLOSES SPECIFIED INFORMATION; TO PRESCRIBE REQUIREMENTS FOR HEALTH DATA PRIVACY POLICIES; TO PROHIBIT REGULATED ENTITIES FROM COLLECTING, SHARING AND STORING HEALTH DATA EXCEPT IN SPECIFIED CIRCUMSTANCES; TO PROHIBIT PERSONS FROM SELLING HEALTH DATA CONCERNING A CONSUMER WITHOUT FIRST OBTAINING AUTHORIZATION FROM THE CONSUMER; TO SPECIFY CERTAIN INFORMATION THAT MUST BE CONTAINED IN A VALID AUTHORIZATION TO SELL CONSUMER HEALTH DATA; TO REQUIRE A COPY OF THE AUTHORIZATION TO BE PROVIDED TO THE CONSUMER; TO REQUIRE SELLERS AND PURCHASERS OF HEALTH DATA TO RETAIN COPIES OF ALL SUCH AUTHORIZATIONS FOR A SPECIFIED TIME; TO PRESCRIBE REQUIREMENTS FOR COLLECTING, SHARING AND STORING HEALTH DATA; TO AUTHORIZE CONSUMERS TO WITHDRAW CONSENT FROM THE COLLECTION, SHARING, SALE OR STORAGE OF THE CONSUMER'S HEALTH DATA; TO PROHIBIT REGULATED ENTITIES FROM ENGAGING IN DISCRIMINATORY PRACTICES AGAINST CONSUMERS SOLELY BECAUSE THEY HAVE NOT CONSENTED TO THE COLLECTION, SHARING, SALE OR STORAGE OF THEIR HEALTH DATA; TO AUTHORIZE CONSUMERS TO CONFIRM WHETHER A REGULATED ENTITY IS COLLECTING, SELLING, SHARING OR STORING ANY OF THE CONSUMER'S HEALTH DATA; TO AUTHORIZE CONSUMERS TO HAVE THE THEIR HEALTH DATA THAT IS COLLECTED BY A REGULATED ENTITY DELETED; TO PROHIBIT THE USE OF GEOFENCING REGARDING CONSUMER HEALTH DATA; TO AUTHORIZE PERSONS AGGRIEVED BY A VIOLATION OF THIS ACT TO FILE AN ACTION AGAINST AN OFFENDING PARTY IN CIRCUIT COURT; TO AUTHORIZE THE ATTORNEY GENERAL TO ENFORCE VIOLATIONS OF THE ACT; AND FOR RELATED PURPOSES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MISSISSIPPI:

SECTION 1. This act shall be known and may be cited as the "Mississippi Protect Health Data Privacy Act."

SECTION 2. As used in this act, the following words and phrases have the meanings ascribed in this section unless the context clearly requires otherwise:

(a) "Collect" means to buy, rent, lease, access, retain, receive or acquire health data in any manner.

(b) "Consent" means a clear affirmative act by a consumer that unambiguously communicates the consumer's express, freely given, informed, opt-in, voluntary, specific and unambiguous written agreement, including written consent provided by electronic means, to the collection, sale, sharing or storage of health data. Consent may not be implied, and consent cannot be obtained by:

(i) Acceptance of a general or broad terms of use agreement or a similar document that contains descriptions of personal data processing along with other, unrelated information;

(ii) Hovering over, muting, pausing or closing a given piece of digital content; or

(iii) Agreement obtained through the use of deceptive designs.

(c) "Consumer" means a person who is a resident of this state, however identified, including by any unique identifier. A person located in this state when the person's health data is collected by a regulated entity creates a presumption that the person is a resident of this state for purposes of enforcing this

act. "Consumer" does not include an individual acting in a commercial or employment context.

(d) "Deceptive design" means any user interface or element of a user interface which has the substantial effect of subverting, impairing or impeding an individual's autonomy, decision-making or choice.

(e) "Deidentified data" means data that cannot be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to that individual. A regulated entity that possesses deidentified data shall:

(i) Take reasonable measures to ensure that the data cannot be associated with an individual;

(ii) Publicly commit to process the data only in a deidentified fashion and not attempt to reidentify the data; and

(iii) Contractually obligate a recipient of the data to satisfy the criteria set forth in items (i) and (ii).

(f) "Geofence" means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless Internet data or any other form of spatial or location detection to establish a virtual boundary around a specific physical location or to locate a consumer within a virtual boundary. For purposes of this act, a "geofence" is a virtual boundary that is no more than one thousand

seven hundred fifty (1,750) feet around a specific physical location that provides health services.

(g) "Health data" means information regarding, relating to, derived or extrapolated from the past, present or future physical or mental health of a consumer, including, but not limited to, any information relating to:

(i) Individual health conditions, treatment, status, diseases or diagnoses;

(ii) Health related surgeries or procedures;

(iii) Use or purchase of medication;

(iv) Social, psychological, behavioral and medical interventions;

(v) Bodily functions, vital signs, measurements or symptoms;

(vi) Diagnoses or diagnostic testing, treatment or medication;

(vii) Efforts to research or obtain health services or supplies;

(viii) Health services or products that support or relate to lawful health care;

(ix) Precise location information that could reasonably be used to determine a consumer's attempt to acquire or receive health services or supplies; and

(x) Any information described in subparagraphs (i) through (ix) which is derived or extrapolated from nonhealth

information, including by use of algorithms or machine learning, if such information is used or processed in connection with the advertising, marketing or provision of health services.

"Health data" does not include: personal information collected with the consumer's consent which is used to engage in public or peer-reviewed scientific, historical or statistical research in the public interest, which research adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board, human subjects research ethics review board or a similar independent oversight entity that determines that the regulated entity has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or deidentified data.

(h) "Health services" means any service, medical care or information related to a consumer's health data provided to a consumer.

(i) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, the Health Information Technology for Economic and Clinical Health Act, and any subsequent amendments thereto and any regulations promulgated thereunder, including the Privacy Rule, as specified in 45 CFR 164.500-534, the Security Rule, as specified in 45 CFR 164.302-318, and the Breach Notification Rule, as specified in 45 CFR 164.400-414.

(j) "Homepage" means the introductory page of a website where personal information is collected. In the case of an online service, such as a mobile application, "homepage" means the application's platform page or download page, such as from the application configuration, "About" page, "Information" page or settings page, and any other location that allows consumers to review the notice.

(k) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or is linked, directly or indirectly, with a particular consumer or household. "Personal information" does not include publicly available information or deidentified data.

(l) "Precise location information" means information that identifies the location of an individual within a radius of one thousand seven hundred fifty (1,750) feet. "Precise location information" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(m) "Processor" means an individual or legal entity that processes health data on behalf of a regulated entity pursuant to a written agreement or contract.

(n) "Processing" means arranging, storing, organizing, structuring, retrieving, transmitting or otherwise making available data.

(o) "Publicly available" means information that is lawfully made available from federal, state or local government records.

(p) "Regulated entity" means any individual, partnership, corporation, limited liability company, association or other group, however organized, that:

(i) Conducts business in this state or produces products or services that are available to consumers in this state; and

(ii) For any purpose, handles, collects, shares, sells, stores or otherwise deals with health data.

"Regulated entity" does not include governmental agencies, tribal nations, a clerk, judge or justice of the court, or contracted service providers when processing consumer health data on behalf of the governmental agency. "Regulated entity" also does not include any entity that is a covered entity or a business associate, as defined in Section 160.103 of Title 45 of the Code of Federal Regulations, subject to and in compliance with HIPAA to the extent the entity is acting as a covered entity or business associate under the Privacy and Security rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations. "Regulated entity" also does not include an entity that is subject to and in compliance with restrictions on disclosure of records under Section 543 of the Public Health Service Act, 42 U.S.C.

290dd-2, to the extent the entity is acting in a capacity subject to those restrictions.

(q) "Sell" or "sale" means when a regulated entity, directly or indirectly, receives any form of remuneration or other valuable consideration from the use of health data or from the recipient of the health data in exchange for the health data. "Sell" does not include:

(i) The sharing of health data to a recipient where the regulated entity maintains control and ownership of the health data;

(ii) The sharing of health data to comply with applicable laws or regulations;

(iii) The use of the health data by an entity exclusively at the direction of the regulated entity and consistent with the purpose for which it was collected and disclosed; and

(iv) The transfer of health data to a third party as an asset as part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the regulated entity's assets which complies with the requirements and obligations of this act.

(r) "Share" means to release, disclose, disseminate, divulge, loan, make available, provide access to, license or otherwise communicate orally, in writing or by electronic or other means, health data by a regulated entity to a third party except

where the regulated entity maintains exclusive control and ownership of the health data. "Share" does not include:

(i) The disclosure of health data to a processor that collects or processes the personal data on behalf of the regulated entity, when the regulated entity maintains control and ownership of the data and the processor maintains or uses the health data only for the regulated entity's distinct purposes pursuant to a contract;

(ii) The disclosure of health data to a third party with whom the consumer has a direct relationship for purposes of, and only to the extent necessary for, providing a product or service requested by the consumer when the regulated entity maintains control and ownership of the data and the third party maintains or uses the health data only for the regulated entity's distinct purposes; or

(iii) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the regulated entity's assets and complies with the requirements and obligations in this act.

(s) "Strictly necessary" means essential or required to be done.

(t) "Third party" means an entity other than a consumer, regulated entity, service provider or affiliate of the regulated entity.

SECTION 3. (1) This act applies to consumers seeking, researching or obtaining health services within this state or information about health services available in this state and regulated entities.

(2) This act does not affect an individual's right to voluntarily share the individual's own health care information with another person or entity.

SECTION 4. (1) A regulated entity shall disclose and maintain a health data privacy policy that, in plain language, clearly and conspicuously discloses:

(a) The specific types of health data collected and the purpose for which the data is collected and used;

(b) The categories of sources from which the health data is collected;

(c) The specific types of health data that are shared, sold and stored;

(d) The categories of third parties with whom the regulated entity collects, shares, sells and stores health data, and the process to withdraw consent from having health data collected, shared, sold and stored;

(e) A list of the specific third parties to which the regulated entity shares health data, and an active electronic mail

address or other online mechanism that the consumer may use to contact these third parties free of charge;

(f) How a consumer may exercise the rights provided in this act, including, but not limited to, identifying two (2) or more designated methods for a consumer to contact the regulated entity in connection with the exercise of any rights provided in this act;

(g) The length of time the regulated entity intends to retain each category of health data, or if that is not possible, the criteria used to determine that period; however, a regulated entity may not retain health data for each disclosed purpose for which the health data was collected for longer than is reasonably necessary to fulfill that disclosed purpose; and

(h) Whether the regulated entity collects health data when the consumer is not interacting directly with the regulated entity or its services.

(2) A regulated entity shall publish prominently or provide a link to its health data privacy policy on its website homepage or in another manner that is clear and conspicuous to consumers. The health data privacy policy must be distinguishable from other matters. A regulated entity providing health services in a physical location also shall post its health data privacy policy in a conspicuous place that is readily available for viewing by consumers.

(3) A regulated entity may not collect, share, sell or store additional categories of health data not disclosed in the health data privacy policy without first disclosing the additional categories of health data and obtaining the consumer's consent before the collection, sharing, selling or storing of the health data.

(4) A regulated entity may not collect, share, sell or store health data for additional purposes not disclosed in the health data privacy policy without first disclosing the additional purposes and obtaining the consumer's consent before the collection, sharing, selling or storing of the health data.

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

SECTION 5. A regulated entity may not collect, share or store health data, except:

(a) With the consent of the consumer to whom the information relates for a specified purpose; or

(b) As is strictly necessary to provide a product or service that the consumer to whom the health data relates specifically has requested from the regulated entity.

SECTION 6. (1) It is unlawful for a person to sell or offer to sell 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.

(2) A valid authorization to sell consumer health data is an agreement 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 any person or entity collecting and selling the health data;

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

(d) A description of the purpose for the sale, including how the health data will be gathered and how it will be used by the purchaser identified in paragraph (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 of how a consumer may revoke 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 (1) 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 health data must retain a copy of all valid authorizations for sale of health data for six (6) years after the date of its signature or the date when it was last in effect, whichever is later.

SECTION 7. (1) A regulated entity may not seek consent to collect, share or store health data without first disclosing its health data privacy policy as required under Section 4.

(2) Consent required under this section must be obtained before the collection, sharing or storing, as applicable, of any health data, and the request for consent must disclose clearly and conspicuously, separate and apart from its health data privacy policy:

(a) The categories of health data collected, sold, shared or stored;

(b) The purpose of the collection, sharing or storage of the health data, including the specific ways in which it will be used; and

(c) How the consumer can withdraw consent from future collection, sharing or storage of the person's health data.

(3) Consent required under this section must be obtained before the use of any health data for any additional purpose that was not specified before obtaining a consumer's consent for the use of the health data.

SECTION 8. A consumer has the right to withdraw consent from the collection, sharing, sale or storage of the consumer's health data, consistent with the requirements of Section 7.

SECTION 9. (1) It is unlawful for a regulated entity to engage in discriminatory practices against a consumer solely because the consumer has not provided consent to the collection,

sharing, sale or storage of the consumer's health data pursuant to this act or has exercised any other rights provided under this act or guaranteed by law. Discriminatory practices include, but are not limited to:

(a) Denying or limiting goods or services to the consumer;

(b) Imposing additional requirements or restrictions on the individual which would not be necessary if the consumer provided consent;

(c) Providing materially different treatment to consumers who provide consent as compared to consumers who do not provide consent;

(d) Providing or suggesting that the consumer will receive a lower level or quality of goods or services;

(e) Suggesting that the consumer will receive a different price or rate for goods or services; or

(f) Charging different prices or rates for goods or services, including using discounts or other benefits or imposing penalties.

(2) It is not a discriminatory practice under this section to use health data as is strictly necessary to provide a product or service that the consumer to whom the health data relates has specifically requested from a regulated entity.

SECTION 10. A consumer has the right to confirm whether a regulated entity is collecting, selling, sharing or storing any of

the consumer's health data and to confirm that a regulated entity has deleted the consumer's health data following a deletion request pursuant to Section 11. A regulated entity that receives a consumer request to confirm must respond within forty-five (45) calendar days after receiving the request to confirm from the consumer. The regulated entity, without reasonable delay, promptly shall take all steps necessary to verify the consumer's request, but this does not extend the regulated entity's duty to respond within forty-five (45) days of receipt of the consumer's request. The time period to provide the required confirmation may be extended once by an additional forty-five (45) calendar days when reasonably necessary, if the consumer is provided notice of the extension within the first forty-five (45) days.

SECTION 11. (1) A consumer has the right to have the consumer's health data that is collected by a regulated entity deleted by informing the regulated entity of the consumer's request for deletion, except as provided in subsection (7).

(2) Except as otherwise specified in subsection (6), a regulated entity that receives a consumer request to delete any of the consumer's health data, without unreasonable delay, and no more than forty-five (45) calendar days from receiving the deletion request, must:

(a) Delete the consumer's health data from its records, including from all parts of the regulated entity's network; and

(b) Notify all service providers, contractors and third parties with whom the regulated entity has shared the consumer's health data of the deletion request.

(3) If a regulated entity stores any health data on archived or backup systems, it may delay compliance with the consumer's request to delete with respect to the health data stored on the archived or backup system until the archived or backup system relating to that data is restored to an active system or is next accessed or used.

(4) A processor, service provider, contractor or other third party that receives notice of a consumer's deletion request from a regulated entity shall honor the consumer's deletion request and delete the health data from the regulated entity's records, including from all parts of its network or backup systems.

(5) A consumer or a consumer's authorized agent may exercise the rights set forth in this act by submitting a request, at any time, to a regulated entity. The request may be made by:

(a) Contacting the regulated entity through the manner included in its health data privacy policy;

(b) By designating an authorized agent who may exercise the rights on behalf of the consumer;

(c) In the case of collecting health data of a minor, the minor seeking health services may exercise their rights under this act, or the parent or legal guardian of the minor may exercise the rights of this act on the minor's behalf; or

(d) In the case of collecting health data concerning a consumer subject to guardianship, conservatorship or other legal protective arrangement, the guardian or the conservator of the consumer may exercise the rights of this act on the consumer's behalf.

(6) The time period to delete any of the consumer's health data may be extended once by an additional thirty (30) calendar days when reasonably necessary, if the consumer is provided notice of the extension within the first thirty (30) days.

(7) Neither a regulated entity nor a processor is required to comply with a consumer's request to delete the consumer's health data if it is necessary for the regulated entity or the processor to maintain the consumer's health data to:

(a) Complete the transaction for which the health data was collected, provide a good or service requested by the consumer, or otherwise fulfill the requirements of an agreement between the regulated entity and the consumer;

(b) Detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity, if the use of health data for those purposes is limited in time pursuant to a valid record retention schedule;

(c) Engage in public or peer-reviewed scientific, historical or statistical research in the public interest which adheres to all other applicable ethics and privacy laws, if the entities' deletion of the information is likely to render

impossible or seriously impair the achievement of such research, and if the consumer has provided consent to such use of the person's health data;

(d) Comply with any applicable legal obligation, such as data retention requirements set forth in Section 6 of the federal Hospital Licensing Act, 45 CFR 164.316, and 45 CFR 164.530;

(e) Comply with an applicable legal obligation if the regulated entity has been notified, in writing by an attorney, that there is litigation pending in court involving the consumer's health data as possible evidence and that the consumer is the attorney's client or is the person who has instituted the litigation against the client, in which case the regulated entity must retain the record of that consumer until notified in writing by the plaintiff's attorney, with the approval of the defendant's attorney of record, that the case in court involving the record has been concluded or for a period of twelve (12) years after the date that the record was produced, whichever occurs first in time; or

(f) Otherwise use the consumer's health data, internally, in a lawful manner that is compatible with the context in which the consumer provided their health data.

SECTION 12. (1) A regulated entity that receives a consumer request to confirm or delete may take reasonable measures to authenticate the consumer's identity to a reasonably high degree

of certainty. A reasonably high degree of certainty may include matching at least three (3) pieces of personal information provided by the consumer with personal information maintained by the regulated entity that it has determined is reliable for the purpose of authenticating the consumer, together with a signed declaration under penalty of perjury that the consumer making the request is the consumer whose health data is the subject of the request. If a regulated entity uses this method for authentication, the regulated entity must make all forms necessary for authentication of a consumer's identity available to consumers. The entity shall maintain all signed declarations as part of its recordkeeping obligations.

(2) A regulated entity is not required to comply with a consumer request to confirm or delete if the regulated entity, using commercially reasonable efforts, is unable to authenticate the identity of the consumer making the request. If a regulated entity is unable to authenticate the consumer's identity, the regulated entity must inform the consumer that it was unable to authenticate the consumer's identity and advise the consumer of other methods, if available, of authenticating their identity.

(3) If a regulated entity denies an authenticated consumer request to delete that consumer's health data, in whole or in part, because of a conflict with federal or state law, the regulated entity must inform the requesting consumer and explain the basis for the denial unless prohibited from doing so by law.

(4) Any information provided by a consumer to a regulated entity for the purpose of authenticating the consumer's identity may not be used for any purpose other than authenticating the consumer's identity and must be destroyed immediately following the authentication process.

SECTION 13. (1) A regulated entity shall restrict access to health data by the employees, processors, service providers and contractors of the regulated entity to only those employees, processors, services providers and contractors for which access is necessary to provide a product or service that the consumer to whom the health data relates has requested from the regulated entity.

(2) A regulated entity shall establish, implement and maintain administrative, technical and physical data security practices that at least satisfy a reasonable standard of care within the regulated entity's industry to protect the confidentiality, integrity and accessibility of health data appropriate to the volume and nature of the personal data at issue.

SECTION 14. (1) It is unlawful for a person to implement a geofence that enables the sending of a notification, message, alert or other piece of information to a consumer which enters the perimeter around any entity that provides health services.

(2) It is unlawful for a person to implement a geofence around any entity that provides in-person health care services

where the geofence is used to identify, track or collect data from a consumer that enters the virtual perimeter.

SECTION 15. A person aggrieved by a violation of this act has a right of action in circuit court. A prevailing party may recover for each violation:

(a) Against an offending party that negligently violates a provision of this act, liquidated damages of One Thousand Dollars ($1,000.00) or actual damages, whichever is greater;

(b) Against an offending party that intentionally or recklessly violates a provision of this act, liquidated damages of Five Thousand Dollars ($5,000.00) or actual damages, whichever is greater;

(c) Reasonable attorney's fees and costs, including expert witness fees and other litigation expenses; and

(d) Other relief, including an injunction, as the state may deem appropriate.

SECTION 16. The Attorney General may enforce a violation of this act as an unlawful practice. All rights and remedies are available to the Attorney General for enforcement of a violation of this act.

SECTION 17. (1) Nothing in this act may be construed to prohibit the lawful and authorized disclosure of health data by regulated entities to local health departments or state

governmental agencies or among local health departments and state governmental agencies as may be required by state and federal law.

(2) If any provision of this act, or the application of that provision to any person or circumstance, is held invalid, the remainder of this act and the application of that provision to other persons not similarly situated or to other circumstances is not affected by the invalidation.

(3) This act does not apply to personal information collected, processed, sold or disclosed subject to the federal Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations.

SECTION 18. This act shall take effect and be in force from and after July 1, 2024.