HOUSE JUDICIARY COMMITTEE SUBSTITUTE FOR
HOUSE BILL 430

57TH LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2025

AN ACT

RELATING TO PRIVACY; ENACTING THE HEALTH DATA PRIVACY ACT; PROVIDING DEFINITIONS; PROVIDING DUTIES FOR REGULATED ENTITIES; PROVIDING FOR ENFORCEMENT AND PENALTIES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

SECTION 1. [NEW MATERIAL] SHORT TITLE.--This act may be cited as the "Health Data Privacy Act".

SECTION 2. [NEW MATERIAL] DEFINITIONS.--As used in the Health Data Privacy Act:

A. "de-identified data" means data that does not identify and cannot be used to infer information about, or otherwise be linked to, an identified or identifiable individual or a device linked to the individual, if the regulated entity that possesses such data:

(1) takes reasonable physical, administrative

underscored material = new
[bracketed material] = delete

and technical measures to ensure that the data cannot be associated with an individual or used to identify the individual or be associated with a device that identifies, is linked to or can reasonably be linked to an individual;

(2) publicly commits to process the data only in a de-identified fashion and not to attempt to re-identify the data; and

(3) contractually obligates any recipient of the de-identified data to comply with Paragraphs (1) and (2) of this subsection;

B. "health care provider" means a person, a corporation, a facility, an organization or an institution that is licensed, certified or organized in this state to provide health care services, and the health care services provided comprise seventy percent of the total services or products provided;

C. "health information exchange" means an entity that provides services to enable the electronic and secure sharing of health care information or a record locator service as defined in the Electronic Medical Records Act;

D. "process" or "processing" means conduct or an operation performed or a set of operations performed on regulated health information, including the collection, use, access, sharing, sale, monetization, brokerage, analysis, retention, creation, generation, derivation, recording,

underscored material = new
[bracketed material] = delete

organization, structuring, modification, storage, disclosure, transmission, disposal, licensing, destruction, deletion or de-identification of regulated health information;

E. "regulated entity" means an entity, not including a health care provider or health information exchange, that:

(1) controls the processing of regulated health information of an individual who is a New Mexico resident;

(2) controls the processing of regulated health information of an individual who is physically present in New Mexico while that individual is in New Mexico; or

(3) is located in New Mexico and controls the processing of regulated health information. A "regulated entity" may also be a service provider, depending upon the context in which the regulated entity processes or controls the processing of regulated health information;

F. "regulated health information" means information that is reasonably linkable to an individual or to a device and that is collected or processed in connection with the physical or mental health of an individual, including location or payment information that relates to an individual's past, present or future physical or mental health. "Regulated health information" includes information related to an individual's disability, diagnosis, health condition or treatment and any

underscored material = new
[bracketed material] = delete

inference drawn or derived about an individual's physical or mental health, disability, diagnosis or health condition or treatment that is reasonably linkable to an individual or a device. "Regulated health information" does not include de-identified information or any record, data or other information that is protected health information as defined by the federal Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated under that act;

G. "service provider" means a person or an entity that processes regulated health information on behalf of a regulated entity. A "service provider" may also be a regulated entity, depending upon the context in which the service provider processes regulated health information; and

H. "third party" means a person or an entity involved in a transaction related to the processing of regulated health information, other than an individual, a regulated entity or a service provider that is involved in the transaction. A "third party" may also be a regulated entity or service provider, depending upon the context in which the third party is involved in the processing of regulated health information.

SECTION 3. [NEW MATERIAL] REQUIREMENTS FOR REGULATED ENTITIES.--

A. A regulated entity shall:

(1) publicly provide, in a clear, concise and

underscored material = new
[bracketed material] = delete

easily understood manner, the regulated entity's privacy information and shall provide the privacy information separate and distinct from the provision of the regulated entity's terms of service, policies and community standards;

(2) publicly provide prominent, accessible and responsive tools to help an individual exercise the individual's privacy rights and report privacy concerns; and

(3) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of regulated health information as appropriate to the volume and nature of the regulated health information at issue.

B. All communications between a regulated entity and individuals whose regulated health information is in the possession or control of the regulated entity shall be reasonably accessible to individuals with disabilities. A regulated entity shall ensure accessibility:

(1) for notices by using digital accessibility tools and complying with generally recognized industry standards, including current standards set by the world wide web consortium or other similar standards-setting bodies as determined appropriate by the attorney general; and

(2) for communications other than notices by providing information about how an individual with a disability

underscored material = new
[~~bracketed material~~] = delete

may access the communication in an alternative format.

SECTION 4. [NEW MATERIAL] PROHIBITED PRACTICES.--

A. A regulated entity shall not, and shall not instruct a service provider or third party to:

(1) process the regulated health information of an individual, except:

(a) with consent from the individual for the processing for a specified purpose;

(b) as is strictly necessary for the regulated entity to provide the product, service or feature requested and only for the limited time that the collection of the information is strictly necessary to provide the product, service or feature; and

(c) as is strictly necessary to provide a communication, that is not an advertisement, by the regulated entity to an individual that reasonably anticipates the communication within the context of the relationship between the regulated entity and the individual;

(2) process any precise geolocation information of an individual that could reasonably indicate the individual's attempt to acquire or receive health services or supplies unless it is strictly necessary to provide the product, service or feature requested. Consensual geolocation information sharing among users shall not constitute consent to additional processing of geolocation information by the

underscored material = new
[~~bracketed material~~] = delete

regulated entity unless the additional processing is specifically authorized;

(3) process regulated health information for purposes of targeted advertising, first-party advertising or the brokerage of personal data without an individual's consent; and

(4) obtain consent to process regulated health information using any mechanism that has the purpose or substantial effect of obscuring, subverting or impairing an individual's decision-making abilities regarding providing consent to authorize processing of the individual's regulated health information. The request for consent to process an individual's regulated health information shall be obtained prior to and separately from the processing and shall clearly and conspicuously disclose:

(a) the categories of regulated health information to be collected or shared;

(b) the purpose of the processing of the regulated health information, including the specific ways in which the information will be used;

(c) the entities with which the regulated health information is shared; and

(d) how the individual can withdraw consent for future processing of the individual's health information. If the regulated entity is requesting consent

underscored material = new
[bracketed material] = delete

for multiple categories of processing activities, the entity shall allow the individual to provide or withhold consent separately for each category of processing activity, and the entity shall not include a request for consent for a processing activity for which an individual has withheld or revoked consent within the past calendar year.

B. A consent shall include:

(1) the types of regulated health information authorized to be processed;

(2) the nature of the processing activity;

(3) the specific purposes for the processing;

(4) the names of service providers or third parties to which the regulated entity may disclose the individual's regulated health information and the purposes for the disclosure, including the circumstances under which the regulated entity could disclose regulated health information to law enforcement;

(5) any monetary or other valuable consideration the regulated entity could receive in connection with processing the individual's regulated health information, if applicable;

(6) an acknowledgment that not providing consent will not affect an individual's experience of using the regulated entity's products or services;

(7) the expiration date of the consent, which

may be up to one year from the date the consent was provided;

(8) the mechanism by which the individual may revoke the consent prior to its expiration;

(9) the mechanism by which the individual may request access to or deletion of the individual's regulated health information;

(10) any other information material to an individual's decision making regarding consent for processing; and

(11) the signature, which may be electronic, of the individual who is the subject of the regulated health information or, in the case of a known minor, a parent or guardian authorized by law to take actions of legal consequence on behalf of the individual who is the subject of the regulated health information and the date that the consent is signed.

C. A regulated entity that receives consent for processing an individual's regulated health information shall provide an effective, efficient and easy-to-use mechanism by which an individual may revoke consent at any time through an interface that the individual regularly uses in connection with the regulated entity's product or service.

D. For individuals who have an online account with the regulated entity, the regulated entity shall provide, in a conspicuous and easily accessible place within the account settings, a list of all processing activities for which the

underscored material = new
[bracketed material] = delete

individual has provided consent and, for each processing activity, shall allow the individual to revoke consent in the same settings location with one motion or action.

E. Upon obtaining valid consent from an individual, the regulated entity shall provide that individual a copy of the consent. The consent shall be provided in a manner in which a copy of the consent can be retained by the individual.

F. The regulated entity shall limit its processing to the regulated health information that was clearly disclosed to an individual pursuant to Subsection B of this section at the time the regulated entity received consent from the individual.

G. If the regulated entity seeks to materially alter its processing activities for the regulated health information of an individual collected pursuant to the individual's consent, the regulated entity shall obtain a new consent for the new or altered processing activity.

SECTION 5. [NEW MATERIAL] RIGHT OF ACCESS--CORRECTION--DELETION.--

A. Regulated entities shall provide individuals the right to:

(1) access the individual's regulated health information that is processed by the regulated entity or by a service provider;

(2) access information pertaining to the

underscored material = new
[~~bracketed material~~] = delete

collection and processing of the individual's regulated health information, including:

(a) from where or from whom the regulated entity obtained the regulated health information;

(b) the types of third parties to which the regulated entity has disclosed or will disclose the regulated health information;

(c) the purposes of the processing;

(d) the specific types of regulated health information processed;

(e) the names of third parties to which the regulated entity disclosed the regulated health information and a log showing when the disclosure happened; and

(f) the period of retention by the regulated entity of the regulated health information;

(3) obtain the individual's regulated health information processed by a regulated entity in a structured, readily usable, portable and machine-readable format;

(4) transmit or cause the regulated entity to transmit the regulated health information to another regulated entity, when technically feasible;

(5) request a regulated entity to stop collecting and processing the individual's regulated health information;

(6) correct inaccurate regulated health

underscored material = new
[bracketed material] = delete

information stored by a regulated entity; and

(7) delete all the individual's regulated health information stored by the regulated entity; provided that a regulated entity that has collected regulated health information from an individual is not required to delete information to the extent it is exempt under the Health Data Privacy Act.

B. A regulated entity shall provide every individual whose regulated health information the entity possesses with a reasonable means to exercise the individual's rights as provided in this section to revoke consent using a request form that is:

(1) clear and conspicuous;

(2) available at no cost and with no transactional penalty to the individual to whom the information pertains; and

(3) in English and any other language in which the regulated entity communicates with the individual to whom the information pertains.

C. Upon an individual's revocation of consent, the regulated entity shall immediately cease all processing activities and delete all regulated health information for which consent was revoked, except to the extent necessary to comply with the regulated entity's legal obligations; provided that:

(1) if the regulated entity has reasonable doubts or cannot verify the identity of the individual making a request, the regulated entity may request additional personal information necessary to confirm the individual's identity. The regulated entity shall not process the additional personal information for any reason beyond confirming the individual's identity; and

(2) a regulated entity shall not de-identify an individual's regulated health information during the sixty-day period beginning on the date the regulated entity receives a request for correction or deletion from the individual.

D. A regulated entity shall make available an effective, efficient and easy-to-use mechanism, through an interface an individual regularly uses in connection with the regulated entity's product or service, by which the individual may request access to or to delete the individual's regulated health information.

E. Within thirty days of receiving an access request, the regulated entity shall make available a copy of all regulated health information about the individual that the regulated entity maintains or that service providers maintain on behalf of the regulated entity. An individual's request to delete or cancel the individual's online account shall be treated as a request to delete the individual's regulated health information, and within thirty days of receiving a

underscored material = new
[bracketed material] = delete

deletion request, the regulated entity shall:

(1) delete all regulated health information associated with the individual in the regulated entity's possession or control, except to the extent necessary to comply with the regulated entity's legal obligations; and

(2) unless it proves impossible or involves disproportionate effort that is documented in writing by the regulated entity, communicate such request to each service provider or third party that processed the individual's regulated health information in connection with a transaction involving the regulated entity occurring within one year preceding the individual's request.

F. Any service provider or third party that receives notice of an individual's deletion request shall within thirty days delete all regulated health information associated with the individual in its possession or control, except to the extent necessary to comply with its legal obligations.

SECTION 6. [NEW MATERIAL] DATA PROCESSING AGREEMENTS.--A service provider or third party that receives regulated health information from a regulated entity shall enter into a written data processing agreement with the providing regulated entity ensuring that the information will continue to be processed consistent with the provisions of the Health Data Privacy Act, including that:

A. regulated health information received by service providers or third parties shall be processed only for purposes specified in the data processing agreement;

B. service providers and third parties shall only process regulated health information that is adequate, relevant and necessary for the purposes for which it was collected or received;

C. service providers and third parties shall ensure that subcontractors comply with the same protection obligations as set forth in the data processing agreement;

D. service providers and third parties shall establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of regulated health information as is appropriate to the volume and nature of the regulated health information at issue; and

E. service providers and third parties shall allow, and cooperate with, reasonable assessments by the providing regulated entity or that entity's designated assessor for purposes of evaluating compliance with the obligations provided pursuant to the data processing agreement and consistent with the Health Data Privacy Act. Alternatively, the service provider or third party may arrange for a qualified and independent assessor to conduct an assessment of the service provider's or third party's policies and technical and

underscored material = new
[~~bracketed material~~] = delete

organizational measures in support of the obligations pursuant to the data processing agreement and consistent with that act using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The service provider or third party shall provide a report of the assessment to the providing regulated entity upon request and shall:

(1) notify the regulated entity at a reasonable time in advance before disclosing or transferring regulated health information to any other service provider. The notice may be in the form of a regularly updated list of other service providers that may access regulated health information;

(2) engage any other service provider or third party pursuant to a written, binding agreement that includes the contractual requirements provided in this section, containing at minimum the same obligations that the service provider or third party has entered into in the data processing agreement with regard to regulated health information; and

(3) prior to transferring regulated health information to a third party located outside of New Mexico, ensure that adequate data protection safeguards consistent with the Health Data Privacy Act are in place.

SECTION 7. [NEW MATERIAL] PROHIBITION ON WAIVING OF RIGHTS AND DENIAL OF SERVICE.--

underscored material = new
[~~bracketed material~~] = delete

A. A regulated entity shall not retaliate against an individual for exercising any of the rights guaranteed by the Health Data Privacy Act. Retaliation includes denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services.

B. No provision of any contract, agreement or terms of service shall waive, limit or otherwise undermine the rights conferred to individuals under the Health Data Privacy Act or any other applicable data protection laws. The invalidity or unenforceability of any provision in a contract involving a regulated entity, service provider or third party shall not affect the validity or enforceability of the remaining provisions of the contract or agreement.

SECTION 8. [NEW MATERIAL] VIOLATIONS--ENFORCEMENT--PENALTIES--CLAIMS FOR VIOLATIONS.--

A. A violation of the Health Data Privacy Act constitutes a rebuttable presumption of harm. A regulated entity that violates that act shall be:

(1) subject to injunctive relief to cease or correct the violation;

(2) liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) or up to two percent of the total annual revenue, whichever is higher, per affected individual for each negligent violation; or

underscored material = new
[bracketed material] = delete

(3) liable for a civil penalty of not more than seven thousand five hundred dollars ($7,500) or up to four percent of the total annual revenue, whichever is higher, per affected individual for each intentional violation.

B. Except as provided in Subsection C of this section, an individual who claims to have suffered a deprivation of the rights secured under the Health Data Privacy Act may maintain an action to establish liability and recover damages and equitable or injunctive relief in any New Mexico district court.

C. For a period of three years immediately following the effective date of the Health Data Privacy Act, an action brought under this section shall not be maintained against a regulated entity that controls or processes the personal data of fifteen thousand or more individuals in New Mexico unless the maintaining party first provides the regulated entity with a notice of violation that reasonably describes the entity's alleged violation or deprivation of rights under that act and provides a sixty-day opportunity to cure. If the regulated entity fails to cure the violation within sixty days of receipt of the notice of violation, the action may be maintained pursuant to this section without further notice. The opportunity to cure a violation pursuant to this subsection shall expire on July 1, 2027.

D. The attorney general or a district attorney may

underscored material = new
[bracketed material] = delete

institute a civil action in district court if the attorney general or district attorney has reasonable cause to believe that a violation has occurred or to prevent a violation of the Health Data Privacy Act.

E. In an action brought pursuant to Subsection A of this section, the court may award appropriate relief, including temporary, preliminary or permanent injunctive relief and civil penalties, depending on the circumstances of each individual case. When deciding whether to impose civil penalties or deciding on the amount of a penalty in an individual case, due regard shall be given to the following:

(1) the nature, gravity and duration of the violation, including the nature, scope or purpose of the processing concerned, the number of individuals affected and the level of damage suffered by those individuals;

(2) the intentional or negligent character of the violation;

(3) any action taken by the regulated entity to mitigate the damage suffered by an individual;

(4) any previous violations by the regulated entity;

(5) the categories of personal data affected by the violation; and

(6) any other aggravating or mitigating factor applicable to the circumstances of the violation, including

financial benefits gained or losses avoided, directly or indirectly, from the violation.

SECTION 9. [NEW MATERIAL] LIMITATIONS.--Nothing in the Health Data Privacy Act shall be interpreted or construed to:

A. impose liability in a manner that is inconsistent with Section 230 of the federal Communications Decency Act of 1996;

B. apply to information processed by local, state or federal governments or municipal corporations; or

C. restrict a regulated entity's, service provider's or third party's ability to:

(1) comply with federal or New Mexico law;

(2) comply with a civil or criminal subpoena or summons, except as prohibited by New Mexico law;

(3) cooperate with law enforcement agencies concerning conduct or activity that the regulated entity or service provider reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations;

(4) investigate, establish, exercise, prepare for or defend legal claims to the extent that the regulated health information is relevant to the parties' claims;

(5) take immediate steps to protect the life or physical safety of the individual or another individual in an emergency and where the processing cannot be manifestly based on another legal basis; provided that an individual's

underscored material = new
[bracketed material] = delete

access to health care services lawful in the state of New Mexico shall not constitute an emergency;

(6) prevent, detect, protect against or respond to security incidents relating to network security or physical security, including an intrusion or trespass, medical alert or request for a medical response, fire alarm or request for a fire response or access control;

(7) prevent, detect, protect against or respond to identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity targeted at or involving the regulated entity or service provider or its services, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action;

(8) assist another regulated entity, service provider or third party with any of the obligations under the Health Data Privacy Act;

(9) transfer assets to a third party in the context of a merger, acquisition, bankruptcy or similar transaction when the third party assumes control, in whole or in part, of the regulated entity's assets, only if the regulated entity, in a reasonable time prior to the transfer, provides an affected individual with a:

(a) notice describing the transfer, including the name of the entity receiving the individual's

regulated health information and the applicable privacy policies of such entity; and

(b) reasonable opportunity to withdraw previously provided consent or opt-ins related to the individual's regulated health information;

(10) request the deletion of the individual's regulated health information; and

(11) conduct medical research in compliance with Part 46 of Title 45, Code of Federal Regulations, or Parts 50 and 56 of Title 21, Code of Federal Regulations; or with respect to regulated health information previously collected in accordance with state law, process the regulated health information solely for the purpose that the regulated health information becomes de-identified data.

SECTION 10. [NEW MATERIAL] SEVERABILITY.--If any part or application of the Health Data Privacy Act is held invalid, the remainder of its application to other situations or persons shall not be affected.

SECTION 11. EFFECTIVE DATE.--The effective date of the provisions of this act is July 1, 2025.

underscored material = new
[bracketed material] = delete