SENATE BILL 53

57TH LEGISLATURE - STATE OF NEW MEXICO - SECOND SESSION, 2026

INTRODUCED BY

Angel M. Charley and Leo Jaramillo and Christine Chandler
and Marianna Anaya and Pamelya Herndon

AN ACT

RELATING TO PRIVACY; STRENGTHENING PRIVACY PROTECTIONS BY ENACTING THE COMMUNITY AND HEALTH INFORMATION SAFETY AND PRIVACY ACT; PROVIDING DEFINITIONS; PROVIDING DUTIES FOR COVERED ENTITIES; ESTABLISHING REQUIREMENTS FOR SERVICE PROVIDERS; PROHIBITING CERTAIN USES OF CONSUMER DATA; PROVIDING RIGHTS TO CONSUMERS; ESTABLISHING LIMITATIONS ON PROCESSING OF CONSUMER DATA; PROHIBITING WAIVERS OF RIGHTS AND RETALIATORY DENIALS OF SERVICE; 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 "Community and Health Information Safety and Privacy Act".

SECTION 2. [NEW MATERIAL] DEFINITIONS.--As used in the Community and Health Information Safety and Privacy Act:

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

A. "actual knowledge" means a covered entity knows that a consumer is a minor based upon:

(1) the self-identified age provided by the minor, an age provided by a third party or a closely related proxy that the covered entity knows or has associated with, attributed to or derived or inferred for the consumer, including for the purposes of advertising, marketing or product development; or

(2) the consumer's use of an online feature, product or service or a portion of an online feature, product or service that is directed to children;

B. "affiliate" means a legal entity that controls, is controlled by or is under common control with another legal entity;

C. "biometric data" means the data about a consumer generated by measurements of the consumer's unique biological characteristics such as a faceprint, a fingerprint, a voiceprint, a retina or an iris image or other biological characteristic that can be used to uniquely identify the consumer. "Biometric data" does not include:

(1) demographic data;

(2) a donated portion of a human body stored on behalf of a potential recipient of a living cadaveric transplant and obtained or stored by a federally designated organ procurement agency, including an artery, a bone, an eye,

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

an organ, tissue or blood or other fluid or serum;

(3) a human biological sample used for valid scientific testing or screening;

(4) an image or film of the human anatomy used to diagnose, provide a prognosis for or treat an illness or other medical condition or to further validate scientific testing or screening, including an x-ray image, a roentgen process, a computed tomography scan, a magnetic resonance imaging image, a positron emission tomography scan or a mammogram;

(5) information collected, used or stored for health care treatment, payment or operations pursuant to federal law governing health insurance;

(6) information collected, used or disclosed for human subject research that is conducted in accordance with the federal policy for the protection of human subjects at 45 CFR Part 46 or the good clinical practice guidelines published by the international council for harmonisation of technical requirements for pharmaceuticals for human use;

(7) a photograph or video; except that "biometric data" includes data generated, captured or collected from the biological characteristics of a consumer;

(8) a physical description, including height, weight, hair color, eye color or a tattoo description; or

(9) a writing sample or written signature;

D. "brokerage of personal data" means the exchange of personal data for monetary or other valuable consideration by a covered entity to a third party, but does not include:

(1) the disclosure of publicly available information;

(2) the disclosure of personal data to a service provider that processes the personal data on behalf of the covered entity;

(3) the disclosure of personal data to a third party for purposes of providing an online feature, product or service requested by a consumer;

(4) the disclosure or transfer of personal data to an affiliate of the covered entity; or

(5) the disclosure of personal data when a consumer:

(a) provides affirmative consent for the disclosure;

(b) directs the covered entity to disclose that consumer's personal data; or

(c) intentionally uses the covered entity to interact with a third party;

E. "collect" means to access, acquire or gather personal data;

F. "consumer" means a natural person who resides or is present in New Mexico, including those identified by a unique identifier;

G. "contextual advertising" means displaying or presenting an advertisement that does not vary based on the identity of the recipient and is based solely on:

(1) the immediate content of a web page or an online feature, product or service within which the advertisement appears;

(2) a specific request to a consumer for information or feedback if displayed in proximity to the results of that request for information; or

(3) a consumer's association with a geographic area that is equal to or greater than the area of a circle with a radius of five miles;

H. "control" or "controlled" means:

(1) ownership of or the power to vote more than fifty percent of the outstanding shares of a class of voting security of a covered entity;

(2) control over the election of a majority of the directors or individuals exercising similar functions of a covered entity; or

(3) the power to exercise a controlling influence over the management of a covered entity;

I. "covered entity" means a sole proprietorship, a partnership, a limited liability company, a corporation, an association, an affiliate or other legal for-profit entity that offers online features, products or services to consumers in New Mexico and, alone or jointly with others, determines the purposes and means of:

(1) collecting personal data directly from consumers;

(2) using personal data for targeted advertising; or

(3) engaging in the brokerage of personal data; provided that "covered entity" does not include an entity that processes the data of fifteen thousand or fewer consumers annually and does not engage in the brokerage of that data;

J. "dark pattern" means a user interface designed or manipulated with the purpose of subverting or impairing user autonomy, decision making or choice;

K. "default" means a preselected option adopted by a covered entity for an online feature, product or service;

L. "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 consumer or device linked to the consumer if the covered entity that possesses the data:

(1) takes reasonable physical, administrative and technical measures to ensure that the data cannot be associated with a consumer or be used to identify a consumer or a device that identifies or is reasonably linkable to a

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

consumer;

(2) publicly commits to process the data only in a de-identified fashion; and

(3) contractually obligates a recipient of the data to satisfy the requirements established pursuant to this subsection;

M. "derived data" means data that is created by the derivation of assumptions, conclusions, correlations, evidence, data, inferences or predictions about a consumer or a consumer's device from facts, evidence or other sources of information;

N. "expressly provided personal data" means:

(1) personal data provided by a consumer to a covered entity expressly for purposes of a profile-based feed to determine the order, relative prioritization, relative prominence or selection of information that is furnished to the consumer by the covered entity through an online product, service or feature, and includes:

(a) consumer-supplied filters, current precise geolocation information supplied by the consumer, resumption of a previous search, saved preferences and speech patterns provided by the consumer for the purpose of enabling the online product, service or feature to accept spoken input or selecting the language in which the consumer interacts with the online product, service or feature; and

(b) data submitted to a covered entity by the consumer in order to receive particular information, including social media profiles followed by the consumer, video channels subscribed to by the consumer or other content or sources of content on the online feature, product or service the consumer has selected; and

(2) does not include:

(a) the history of a consumer's connected device of browsing, device inactions, financial transactions, geographical locations, physical activity or online searches; or

(b) inferences about the consumer or the consumer's connected device, including inferences based on data described in Paragraph (1) of this subsection;

O. "first-party" means a consumer-facing covered entity with which the consumer intends or expects to interact;

P. "first-party advertising" means advertising or marketing by a first party using first-party data and not other forms of personal data and carried out:

(1) through direct communication with a consumer, including mail, email or text message communications;

(2) in a physical location operated by the first party; or

(3) through the display or presentation of an advertisement on the first party's own website, application or

other online content that promotes that first party's product or service;

Q. "first-party data" means personal data collected directly about a consumer by a first party, including data collected during a consumer's visit or use of a website, a physical location or an online feature, product or service operated by the first party;

R. "geofence" means technology that uses global positioning coordinates, cellular tower connectivity, cellular data, radio frequency identification, wireless communication data or any other form of spatial or location detection to establish a virtual boundary that is two thousand feet or less from the perimeter of a specific physical location to locate a consumer within that virtual boundary;

S. "minor" means a consumer who is younger than eighteen years of age;

T. "personal data" means information, including derived data, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable consumer, and includes sensitive personal data. "Personal data" does not include de-identified information or publicly available information;

U. "precise geolocation" means data that is derived from a device and that is used or intended to be used to reveal the present or past geographical location of a consumer or a consumer's device within a geographic area that is equal to or smaller than the area of a circle with a radius of two thousand feet;

V. "privacy-protective feed" means an algorithmic ranking system that does not use the personal data of a consumer, except for expressly provided personal data, to determine the order, relative prominence, relative prioritization or selection of information that is furnished to the consumer on an online feature, product or service;

W. "profile-based feed" means an algorithmic ranking system that determines the order, relative prominence, relative prioritization or selection of information that is furnished to a consumer on an online feature, product or service based, in whole or part, on personal data that is not expressly provided personal data;

X. "process" or "processing" means conduct or an operation or a set of operations performed on personal data, including the collection, use, access, sharing, sale, monetization, brokerage, analysis, retention, creation, generation, derivation, recording, organization, structuring, modification, storage, disclosure, transmission, disposal, licensing, destruction, deletion or de-identification of personal data;

Y. "profiling" means automated processing of personal data to evaluate certain aspects relating to a consumer, including analyzing or predicting aspects concerning the consumer's behavior, economic situation, health, interests, location, movement, performance at work, personal preferences or reliability. "Profiling" does not include the processing of data that does not result in an assessment or judgment about a consumer;

Z. "publicly available information" means information that has been lawfully made available to the general public from:

(1) federal, state or municipal government records;

(2) widely distributed media, including personal data intentionally made available by a consumer to the general public such that the consumer does not retain a reasonable expectation of the privacy of that personal data; or

(3) a disclosure that has been made to the general public as required by federal, state or local law; and

(4) "publicly available information" does not include:

(a) personal data that is derived data from multiple independent sources of publicly available information that reveals sensitive personal data with respect to a consumer;

(b) sensitive personal data of which the consumer retained a reasonable expectation of privacy, unless otherwise made publicly available by the consumer to whom the information pertains;

(c) personal data that is created through the combination of personal data with publicly available information; or

(d) information made available by a consumer on an online feature, product or service that is open to all members of the public, whether for a fee or for free, when the consumer has restricted the information to a specific audience in a manner that the consumer would retain a reasonable expectation of privacy of the information;

AA. "sensitive personal data" means personal data that includes:

(1) biometric or genetic data;

(2) data revealing citizenship, ethnic origin, immigration status or national origin;

(3) financial data, including a credit card number, a debit card number, a financial account number or information that describes or reveals the bank account balances or income level of a consumer; except that "sensitive personal data" does not include the last four digits of a debit or credit card number;

(4) a government-issued identifier, such as a social security number, passport number or driver's license number, that is not required by law to be displayed in public;

(5) data describing or revealing the past, present or future mental or physical health or condition of a consumer, including:

(a) diagnosis;

(b) disability;

(c) health care condition; or

(d) treatment;

(6) data revealing gender, gender identity, sex or sexual orientation;

(7) precise geolocation;

(8) religious affiliation; or

(9) union membership;

BB. "service provider" means a person or an entity that collects, processes, retains or transfers personal information on behalf of, and at the direction of, a covered entity or another service provider;

CC. "targeted advertising" means displaying or presenting an online advertisement to a consumer or to a device identified by a unique persistent identifier or to a group of consumers or devices identified by unique persistent identifiers when the advertisement is selected based in whole or in part on known or predicted preferences, characteristics, behavior or interests associated with the consumer or a device identified by a unique persistent identifier. "Targeted advertising" does not include first-party advertising or contextual advertising; and

DD. "third party" means a person or an entity involved in a transaction related to the processing of personal data, other than a consumer, a covered entity or a service provider that is involved in the transaction.

SECTION 3. [NEW MATERIAL] REQUIREMENTS FOR COVERED ENTITIES--ONLINE PLATFORMS--CONSUMER OPTIONS--MINORS.--

A. Except as provided in Subsection B of this section, a covered entity shall:

(1) configure all default privacy settings on the covered entity's online platforms offering features, products or services to settings that offer the highest level of privacy;

(2) publicly provide privacy information, terms of service, policies and community standards clearly and conspicuously. Privacy information must be separate and distinct from the provision of the covered entity's terms of service, policies and community standards;

(3) publicly provide prominent, accessible and responsive tools to help consumers exercise privacy rights and report concerns; and

(4) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and

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

nature of the personal data at issue.

B. When a covered entity does not have actual knowledge that a consumer using the covered entity's online platform to access a feature, product or service is a minor, the covered entity shall establish settings on that online platform that permit a consumer to:

(1) disable notifications, including during specific periods of time;

(2) choose between a privacy-protective feed and a profile-based feed; and

(3) disable contact by unknown individuals unless the consumer first initiates the contact or provides a mechanism to screen contact by unknown individuals.

C. When a covered entity has actual knowledge that a consumer using the covered entity's online platform is a minor, the covered entity shall establish default settings on the platform that:

(1) disable contact by unknown users unless the consumer first initiates the contact;

(2) disable notifications between the hours of 10:00 p.m. and 6:00 a.m. mountain standard time pursuant to federal law; and

(3) use a privacy-protective feed.

SECTION 4. [NEW MATERIAL] PROHIBITED PRACTICES--CONSUMER OPT-IN MECHANISM.--A covered entity that provides an online feature, product or service that involves the processing of personal data shall not and shall not instruct a service provider or third party to:

A. profile a consumer by default, unless profiling is necessary to provide the online feature, product or service requested and only with respect to the aspects of the online feature, product or service with which the consumer is actively and knowingly engaged;

B. process the personal data that is not sensitive personal data of a consumer except:

(1) as necessary to provide the specific online feature, product or service with which the consumer is actively and knowingly engaged, including any routine administrative, operational or account-servicing activity, including billing, shipping, delivery, storage, accounting, security or fraud detection;

(2) for a communication that is not an advertisement by the covered entity to the consumer that is reasonably anticipated within the context of the relationship between the covered entity and the consumer; or

(3) for the brokerage of personal data or to provide first-party advertising or targeted advertising; provided that the consumer has first provided opt-in consent as provided in Section 5 of the Community and Health Information Safety and Privacy Act to those purposes by clear and

conspicuous means and not through the use of dark patterns;

C. process a consumer's sensitive personal data:

(1) for purposes of targeted advertising, first-party advertising or the brokerage of personal data; or

(2) for other purposes, unless:

(a) the collection of that data is strictly necessary for the covered entity to provide the online feature, product or service requested and then only for the limited time that the collection of data is necessary to provide the online feature, product or service; or

(b) the consumer gives consent through an opt-in mechanism as provided in Section 5 of the Community and Health Information Safety and Privacy Act;

D. process a consumer's precise geolocation information or allow an individual or third party to monitor a consumer's precise geolocation or online activity without providing an obvious sign to the consumer that the consumer is being monitored or tracked;

E. implement a geofence around an entity that provides in-person health care services or in-person immigration services to identify or track consumers seeking health care services or supplies or immigration services;

F. use dark patterns to cause a consumer to provide personal data, beyond what is reasonably expected to provide the online feature, product or service, to forego privacy protections; or

G. process or transfer personal data to discriminate or otherwise make unavailable the equal enjoyment of goods or services on the basis of childbirth or condition related to pregnancy or childbirth, color, disability, gender, gender identity, mental health, national origin, physical health condition or diagnosis, race, religion, sex life or sexual orientation.

SECTION 5. [NEW MATERIAL] COVERED ENTITY--OPT-IN MECHANISM REQUIREMENTS.--

A. For purposes of a covered entity processing a consumer's sensitive personal data with an opt-in mechanism as required pursuant to Paragraph (2) of Subsection C of Section 4 of the Community and Health Information Safety and Privacy Act, a covered entity's opt-in mechanism shall clearly and conspicuously disclose:

(1) the categories of sensitive personal data to be collected or shared;

(2) the purpose of the processing of the sensitive personal data, including the specific ways in which the information will be used;

(3) the entities with which the sensitive personal data is shared;

(4) how the consumer can withdraw consent for future processing of the consumer's sensitive personal data;

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

(5) any monetary or other valuable consideration the covered entity could receive in connection with processing the consumer's sensitive personal data, if applicable;

(6) an acknowledgment that not providing consent will not affect a consumer's experience of using the covered 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 consumer may revoke the consent prior to its expiration;

(9) the mechanism by which the consumer may request access to or delete the consumer's sensitive personal data;

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

(11) the signature, which may be electronic, of the consumer who is the subject of the sensitive personal data 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 consumer who is the subject of the sensitive personal data and the date the consent is signed.

B. If a covered entity requests consent for multiple categories of processing activities, the entity shall allow the consumer 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 a consumer has withheld or revoked consent within the past calendar year.

C. A covered entity that receives consent to process a consumer's sensitive personal data shall provide an effective, efficient and easy-to-use mechanism by which a consumer may revoke consent at any time through an interface the consumer regularly uses in connection with the covered entity's product or service.

SECTION 6. [NEW MATERIAL] RIGHTS OF ACCESS--CORRECTION--DELETION.--

A. Covered entities shall provide a consumer the right to:

(1) access the consumer's personal data that is processed by the covered entity or a service provider in a clear and concise format;

(2) access all the information pertaining to the processing of the consumer's personal data, including:

(a) where or from whom the covered entity obtained the personal data;

(b) the names and types of third parties to which the covered entity has disclosed or will disclose any personal data;

(c) the purposes of processing the personal data;

(d) the categories of personal data; and

(e) the period of retention of the personal data;

(3) transmit the consumer's personal data to another covered entity, when technically feasible; and

(4) request a covered entity to stop processing, correct or delete the consumer's personal data.

B. A covered entity shall provide a consumer with a clear and conspicuous means to exercise the consumer's rights pursuant to Subsection A of this section in a request form that is made available at no cost and in the language in which the covered entity communicates with the consumer to whom the information pertains.

C. A covered entity shall comply with a consumer's request to exercise the consumer's rights pursuant to Subsection A or B of this section within forty-five days after receiving a verifiable request from a consumer.

D. A consumer's request to delete or cancel the consumer's online account shall be treated by a covered entity as a request to delete the consumer's personal data and, within thirty days of receiving a deletion request, the covered entity shall:

(1) delete all personal data associated with

the consumer in the covered entity's possession or control, except to the extent necessary to comply with the covered entity's legal obligations; and

(2) take reasonable measures to communicate the request to each service provider or third party that processed the consumer's personal data in connection with a transaction involving the covered entity occurring within one year preceding the consumer's request.

E. A service provider or third party that receives notice of a consumer's deletion request shall, within thirty days, delete all of the personal data associated with the consumer in its possession or control, except to the extent necessary to comply with legal obligations.

SECTION 7. [NEW MATERIAL] DATA PROCESSING AGREEMENTS.--A service provider that processes personal data on behalf of a covered entity or another service provider or a third party that receives personal data from a covered entity shall enter into a written data-processing agreement with the covered entity ensuring that the data will continue to be processed consistent with the Community and Health Information Safety and Privacy Act.

SECTION 8. [NEW MATERIAL] PROHIBITION ON WAIVING OF RIGHTS AND RETALIATORY DENIAL OF SERVICE.--

A. A covered entity shall not retaliate against a consumer for exercising a right guaranteed by the Community and

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

Health Information Safety and Privacy Act, or a rule promulgated under that act, including charging that consumer different prices or rates for goods and services, denying goods or services or providing a different level of quality of goods or services to that consumer.

B. Any provision or clause of a contract, terms of service or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way the rights under the Community and Health Information Safety and Privacy Act, including any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable, without affecting the validity or enforceability of the remaining provisions of the contract, terms of service or agreement.

SECTION 9. [NEW MATERIAL] VIOLATIONS--ENFORCEMENT--PENALTIES--CLAIMS FOR VIOLATIONS.--

A. A violation of the Community and Health Information Safety and Privacy Act constitutes a rebuttable presumption of harm. A covered 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) per affected consumer for each negligent violation; or

(3) liable for a civil penalty of not more than seven thousand five hundred dollars ($7,500) per affected consumer for each intentional violation.

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

C. The attorney general or a district attorney may 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 Community and Health Information Safety and Privacy Act.

D. In an action brought pursuant to Subsection B of this section, the court deciding whether to impose civil penalties or deciding on the amount of a penalty in a consumer case shall give due regard to the following:

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

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

(3) any action taken by the covered entity to

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

mitigate the damage suffered by a consumer;

(4) any previous violations by the covered 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 10. [NEW MATERIAL] EXCEPTIONS.--

A. A covered entity or service provider shall be deemed in compliance with the Community and Health Information Safety and Privacy Act, except for the provisions of Paragraph (4) of Subsection A of Section 3 of that act, solely with respect to data covered by the following federal data privacy laws, if the covered entity or service provider is in compliance with the data privacy requirements of those laws, as may be amended from time to time, and the regulations promulgated pursuant to those laws:

(1) Title V of the Gramm-Leach-Bliley Act;

(2) the Health Information Technology for Economic and Clinical Health Act;

(3) Part C of Title XI of the Social Security Act;

(4) the Fair Credit Reporting Act;

(5) the Genetic Information Nondiscrimination Act of 2008;

(6) regulations governing the confidentiality of alcohol and drug abuse patient records at 42 CFR Part 2;

(7) the Health Insurance Portability and Accountability Act of 1996; or

(8) the Family Educational Rights and Privacy Act of 1974, to the extent such covered entity is a school under that act or its regulations.

B. A covered entity or service provider shall be deemed in compliance with the provisions of Paragraph (4) of Subsection A of Section 3 of the Community and Health Information Safety and Privacy Act solely with respect to the data covered by the following federal laws, if the covered entity or service provider is required to comply, and is in compliance with the information security provisions of those laws and the regulations promulgated pursuant to those laws:

(1) Title V of the Gramm-Leach-Bliley Act;

(2) the Health Information Technology for Economic and Clinical Health Act;

(3) Part C of Title XI of the Social Security Act; or

(4) the Health Insurance Portability and Accountability Act of 1996.

C. The Community and Health Information Safety and

Privacy Act does not apply to the delivery or use of a physical product to the extent that the product is not an online feature, product or service.

SECTION 11. [NEW MATERIAL] LIMITATIONS.--Nothing in the Community and Health Information Safety and Privacy Act shall be interpreted or construed to:

A. apply to information processed by local, state or federal government or municipal corporations; or

B. restrict a covered entity's or service provider's ability to:

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

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

(3) investigate, establish, exercise, prepare for or defend legal claims to the extent that the personal data is relevant to the parties' claims;

(4) take immediate steps to protect the life or physical safety of a consumer or another individual in an emergency and when the processing cannot be manifestly based on another legal basis; provided that a consumer's access to health care services lawful in the state shall not constitute an emergency;

(5) 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;

(6) prevent, detect, protect against or respond to identity theft, fraud, harassment, malicious or deceptive activities or illegal activity targeted at or involving the covered 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;

(7) assist another covered entity, service provider or third party with any of the obligations in the Community and Health Information Safety and Privacy Act;

(8) transfer assets to a third party in the context of a merger, an acquisition, a bankruptcy or similar transaction when the third party assumes control, in whole or in part, of the covered entity's assets, only if the covered entity, in a reasonable time prior to the transfer, provides an affected consumer with notice describing the transfer, including the name of the entity receiving the consumer's personal data and the applicable privacy policies of the entity, and a reasonable opportunity to:

(a) withdraw previously provided consent or opt-ins related to the consumer's personal data; and

(b) request the deletion of the consumer's personal data; or

(9) process personal data previously collected in accordance with the Community and Health Information Safety and Privacy Act, solely for the purpose of the personal data becoming de-identified data.

SECTION 12. [NEW MATERIAL] SEVERABILITY.--If any part or application of the Community and Health Information Safety and Privacy Act is held invalid, the remainder or its application to other situations or persons shall not be affected.

SECTION 13. EFFECTIVE DATE.--The effective date of the provisions of this act is July 1, 2026.