

underscored material = new
[bracketed material] = delete

SENATE BILL

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

INTRODUCED BY

Angel M. Charley and Leo Jaramillo

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:

.232877.2

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

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

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

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

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

21 (1) demographic data;

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

.232877.2

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

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

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

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

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

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

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

25 (9) a writing sample or written signature;

.232877.2

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

4 (1) the disclosure of publicly available
5 information;

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

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

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

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

16 (a) provides affirmative consent for the
17 disclosure;

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

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

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

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

.232877.2

1 unique identifier;

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

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

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

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

14 H. "control" or "controlled" means:

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

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

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

23 I. "covered entity" means a sole proprietorship, a
24 partnership, a limited liability company, a corporation, an
25 association, an affiliate or other legal for-profit entity that

.232877.2

1 offers online features, products or services to consumers in
2 New Mexico and, alone or jointly with others, determines the
3 purposes and means of:

4 (1) collecting personal data directly from
5 consumers;

6 (2) using personal data for targeted
7 advertising; or

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

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

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

17 L. "de-identified data" means data that does not
18 identify and cannot be used to infer information about, or
19 otherwise be linked to, an identified or identifiable consumer
20 or device linked to the consumer if the covered entity that
21 possesses the data:

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

.232877.2

1 consumer;

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

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

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

12 N. "expressly provided personal data" means:

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

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

.232877.2

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

7 (2) does not include:

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

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

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

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

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

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

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

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

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

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

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

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

23 U. "precise geolocation" means data that is derived
24 from a device and that is used or intended to be used to reveal
25 the present or past geographical location of a consumer or a

.232877.2

1 consumer's device within a geographic area that is equal to or
2 smaller than the area of a circle with a radius of two thousand
3 feet;

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

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

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

24 Y. "profiling" means automated processing of
25 personal data to evaluate certain aspects relating to a

1 consumer, including analyzing or predicting aspects concerning
2 the consumer's behavior, economic situation, health, interests,
3 location, movement, performance at work, personal preferences
4 or reliability. "Profiling" does not include the processing of
5 data that does not result in an assessment or judgment about a
6 consumer;

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

10 (1) federal, state or municipal government
11 records;

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

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

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

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

24 (b) sensitive personal data of which the
25 consumer retained a reasonable expectation of privacy, unless

.232877.2

1 otherwise made publicly available by the consumer to whom the
2 information pertains;

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

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

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

14 (1) biometric or genetic data;

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

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

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

.232877.2

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

4 (a) diagnosis;

5 (b) disability;

6 (c) health care condition; or

7 (d) treatment;

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

10 (7) precise geolocation;

11 (8) religious affiliation; or

12 (9) union membership;

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

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

.232877.2

1 contextual advertising; and

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

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

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

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

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

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

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

.232877.2

1 nature of the personal data at issue.

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

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

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

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

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

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

20 (2) disable notifications between the hours of
21 10:00 p.m. and 6:00 a.m. mountain standard time pursuant to
22 federal law; and

23 (3) use a privacy-protective feed.

24 SECTION 4. [NEW MATERIAL] PROHIBITED PRACTICES--CONSUMER
25 OPT-IN MECHANISM.--A covered entity that provides an online

.232877.2

1 feature, product or service that involves the processing of
2 personal data shall not and shall not instruct a service
3 provider or third party to:

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

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

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

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

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

.232877.2

1 conspicuous means and not through the use of dark patterns;

2 C. process a consumer's sensitive personal data:

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

5 (2) for other purposes, unless:

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

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

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

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

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

.232877.2

1 protections; or

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

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

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

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

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

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

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

.232877.2

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

5 (6) an acknowledgment that not providing
6 consent will not affect a consumer's experience of using the
7 covered entity's products or services;

8 (7) the expiration date of the consent, which
9 may be up to one year from the date the consent was provided;

10 (8) the mechanism by which the consumer may
11 revoke the consent prior to its expiration;

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

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

18 (11) the signature, which may be electronic,
19 of the consumer who is the subject of the sensitive personal
20 data or, in the case of a known minor, a parent or guardian
21 authorized by law to take actions of legal consequence on
22 behalf of the consumer who is the subject of the sensitive
23 personal data and the date the consent is signed.

24 B. If a covered entity requests consent for
25 multiple categories of processing activities, the entity shall

1 allow the consumer to provide or withhold consent separately
2 for each category of processing activity, and the entity shall
3 not include a request for consent for a processing activity for
4 which a consumer has withheld or revoked consent within the
5 past calendar year.

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

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

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

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

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

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

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

.232877.2

1 (c) the purposes of processing the
2 personal data;

3 (d) the categories of personal data; and

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

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

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

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

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

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

25 (1) delete all personal data associated with

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

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

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

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

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

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

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

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

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

17 A. A violation of the Community and Health
18 Information Safety and Privacy Act constitutes a rebuttable
19 presumption of harm. A covered entity that violates that act
20 shall be:

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

23 (2) liable for a civil penalty of not more
24 than two thousand five hundred dollars (\$2,500) per affected
25 consumer for each negligent violation; or

.232877.2

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

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

10 C. The attorney general or a district attorney may
11 institute a civil action in district court if the attorney
12 general or district attorney has reasonable cause to believe
13 that a violation has occurred or to prevent a violation of the
14 Community and Health Information Safety and Privacy Act.

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

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

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

25 (3) any action taken by the covered entity to

1 mitigate the damage suffered by a consumer;

2 (4) any previous violations by the covered
3 entity;

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

6 (6) any other aggravating or mitigating factor
7 applicable to the circumstances of the violation, including
8 financial benefits gained or losses avoided, directly or
9 indirectly, from the violation.

10 SECTION 10. [NEW MATERIAL] EXCEPTIONS.--

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

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

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

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

25 (4) the Fair Credit Reporting Act;

.232877.2

1 (5) the Genetic Information Nondiscrimination
2 Act of 2008;

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

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

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

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

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

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

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

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

25 C. The Community and Health Information Safety and

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

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

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

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

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

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

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

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

.232877.2

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

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

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

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

25 (a) withdraw previously provided consent

1 or opt-ins related to the consumer's personal data; and

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

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

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

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

14 - 29 -
15
16
17
18
19
20
21
22
23
24
25