HCA Healthcare

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Colorado - Breach of Personal Information under Colorado’s Consumer Data Privacy Law and the Treatment of Personal Data under the Colorado Privacy Act (CPA)
PAGE: 1 of 23	**REPLACES POLICY DATED:** 8/18 (Model Policy), 2/1/20
EFFECTIVE DATE: July 1, 2023	**REFERENCE NUMBER:** IP.DP.CO.004
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities in the state of Colorado, including, but not limited to, hospitals, ambulatory surgery centers, home health and hospice, imaging and oncology centers, physician practices, shared services centers and corporate departments, Groups, Divisions and Markets (collectively Colorado Affiliates).

The Colorado Breach Law, effective September 1, 2018 heightens requirements for corporate and public entities handling personal information of Colorado residents. Effective September 1, 2018, the law aims to strengthen consumer data privacy by 1) shortening the time frame required to notify affected Colorado residents and the Attorney General of a data breach within 30 days of determining a data breach occurred; 2) requiring business and third-party entities to adopt “reasonable security procedures” to safeguard personally identifiable information (“PII”) handled; and 3) imposing data disposal rules for such entities.

The Colorado Privacy Act (CPA) applies to entities that conduct business in, or target products or services to Colorado, and control or process personal data of at least 100,000 consumers per calendar year; or sell personal data and control or process the personal data of at least 25,000 consumers. It does not apply to certain entities including state and local governments and state institutions of higher education, personal data governed by listed state and federal laws, listed activities, and employment records.

PURPOSE: To provide guidance regarding workforce members’ responsibility related to data breaches and establish the requirements for each Company-affiliated facility in Colorado to protect personal information/data as required for compliance with the Colorado Breach Law and the CPA.

POLICY: Under the Colorado Breach Law, if a breach of security may have occurred, a covered entity shall implement and maintain reasonable security measures to protect and secure personal information. If a breach of security may have occurred, a covered entity must promptly conduct a good faith investigation to determine the likelihood that personal information has been or will be misused. Unless the investigation determines that misuse of the personal information has not occurred and is not reasonably likely to occur, the covered entity must give notice to certain individuals, agencies and other entities.

Covered entities must notify each individual in Colorado whose personal information was, or was reasonably believed to have been, accessed as a result of a breach. Breaches involving 500 or more individuals must be reported to the Department of Legal Affairs and the Colorado Attorney General. If a single breach involves more than 1,000 individuals, the covered entity must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

The requirements in this policy are in addition to, and not in the place of, any requirements under Health Information Portability and Accountability Act (HIPAA) and any and all other Federal laws, regulations and interpretive guidelines, and Facility policies promulgated thereunder.

Governance and Accountability for CPA Compliance

The Company is responsible for ensuring that:

a. Personal data is collected and processed in accordance with the CPA;

b. An appropriate privacy governance framework is in place;

c. Appropriate privacy and security policies, procedures and standards are maintained; and

d. Consumers' rights are upheld.

The Corporate Information Protection and Security Department (IPS) in conjunction with the Corporate Information Technology Group (ITG Legal) will draft all required revisions to the online Privacy Policy. The IPS Privacy Team will work with Company stakeholders as appropriate to identify instances of collection, transmission, processing, or retention of personal data subject to the CPA. The Website Compliance Team and the Digital Patient Experience Team will insert the Policy, as applicable. Consumer requests will be routed to resources via an interactive form, toll-free number or email address provided in the online Privacy Policy. Identified resources will forward Consumer requests to business owners such as the Corporate Marketing Department, and certain business owners of applications that may store Colorado resident personal data, as needed, for resolution. Generally, facilities will not receive or process Consumer requests.

PROCEDURE - Colorado Breach Law**:**

1. <u>Notice to the Individual</u>

   a. Unless a prompt investigation determines that misuse of personal information has not occurred and is not reasonably likely to occur, covered entities must notify each individual in Colorado affected by the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the computerized data system that was breached, but no later than 30 days after the determination that a breach of security occurred.

   b. Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's state or federal regulator is in compliance with the notice requirement in this subsection. As such, to the extent the covered entity must otherwise notify individuals under federal law (*e.g.*, HIPAA), such notice will suffice, if provided no later than 30 days after the determination that a breach of security occurred.

c. If a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would impede a criminal investigation and the law enforcement agency notifies the covered entity not to send notice as required by this policy, the notice may be delayed for a specified period that the law enforcement agency determines is reasonably necessary.

d. Notice to the affected individuals is not required if, after a good faith investigation, the covered entity reasonably determines that misuse of the personal information has not occurred and is not reasonably likely to occur.

e. In the case of a breach of encrypted or otherwise secured personal information, notice to the affected individuals is not required if the encryption key, the confidential process, or other means to decipher the secured information was not acquired or reasonably believed to have been acquired.

f. The notice to an affected individual shall be by one of the following methods:

   i. Written notice sent to the mailing address of the individual in the records of the covered entity; or

   ii. Electronic notice, if a primary means of communication by the covered entity is by electronic means; or

   iii. Telephonic notice.

g. The notice to an individual with respect to a breach of security shall include, at a minimum:

   i. The date, estimated date, or estimated date range of the breach of security.

   ii. A description of the personal information that was acquired or reasonably believed to have been acquired as a part of the breach of security.

   iii. Information that the individual can use to contact the covered entity to inquire about the breach of security.

   iv. The toll-free numbers, addresses, and websites for consumer reporting agencies.

   v. The toll-free number, address, and website for the Federal Trade Commission.

   vi. A statement that the individual can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

vii. A statement directing the individual to promptly change his or her password and security question, or to take other steps appropriate to protect the individual's online account with the covered entity and all other online accounts for which the individual uses the same username, email address and password, or security question or answer.

h. Covered entities that are required to provide notice to an individual may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed $250,000, or because the covered entity does not have sufficient contact information to provide notice. Such substitute notice shall include the following:

   i. Email notice if the covered entity has email addresses for the individuals;

   ii. A conspicuous notice on the website of the covered entity if the covered entity maintains a website; and

   iii. Notification to a major statewide media.

2. Notice to Credit Reporting Agencies

   a. In the case where a single breach event affects more than 1,000 Colorado residents and unless a prompt investigation determines that misuse of personal information has not occurred and is not reasonably likely to occur, the covered entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal Fair Credit Reporting Act, specifically Equifax, Transunion, and Experian.

   b. Notification shall include the anticipated date of the covered entity's separate notification to Colorado residents, as well as the approximate number of Colorado residents to be notified.

   c. Notification shall be provided in the most expedient time possible and without unreasonable delay.

3. Notice to the Colorado Attorney General

   a. In the case where a single breach is reasonably believed to have affected 500 residents of Colorado or more and unless a prompt investigation determines that misuse of personal information has not occurred and is not reasonably likely to occur, the covered entity shall also notify the Colorado Attorney General.

   b. Notification shall be provided in the most expedient time possible and without unreasonable delay but in no event later than 30 days from the date of the determination that a breach occurred.

4. Notice By Third-Party Agents; Duties of Third-Party Agents; Notice by Agents (including Business Associates under HIPAA)

   a. In the event of a breach of security of a system maintained by a third-party agent that contains personal information, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable and without unreasonable delay, if misuse of personal information is likely to occur. Upon receiving notice from a third-party agent, a covered entity shall provide the required notices to individuals, consumer reporting agencies, the Colorado Attorney General, and to any other party required by law. A third-party agent shall provide the covered entity with all information that the covered entity needs to comply with its notice requirements.

5. Requirements for Destruction of Records with Personal Information

   a. Each covered entity or third-party agent shall take all reasonable measures to destroy, or arrange for the destruction of, any paper or electronic documents containing personal information and within its custody or control when such documents are no longer needed, unless otherwise required by state or federal law or regulation. Such destruction shall involve shredding, erasing, or otherwise modifying the personal information in the documents to make it unreadable or indecipherable through any means.

PROCEDURE – Colorado Privacy Act (CPA):

1. Consumer Personal Data Rights

   Consumers may exercise the following rights by submitting a request using the methods specified by the controller in the privacy policy, and the ability of the controller to authenticate the identity of the consumer making the request.

   a. Right to opt out. A consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of:

      i. Targeted advertising;

      ii. The sale of personal data; or

      iii. Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.

      iv. A consumer may authorize another person, acting on the consumer's behalf, to opt out of the processing of the consumer's personal data.

      v. A controller that processes personal data for purposes of targeted advertising or the sale of personal data may allow consumers to exercise the right to opt out of the processing of personal data concerning the consumer for purposes of targeted advertising or the sale of personal data through a user-selected universal opt-out mechanism that meets the technical specifications established by the attorney general pursuant to section 6-1-1313.

b. Right of access. A consumer has the right to confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data.

c. Right to correction. A consumer has the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

d. Right to deletion. A consumer has the right to delete personal data concerning the consumer.

e. Right to data portability. When exercising the right to access personal data pursuant to subsection (1)(b) of this section, a consumer has the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance.

2. <u>Responding to Consumer Requests</u>

a. A controller shall inform a consumer of any action taken on a request without undue delay and, in any event, within forty-five days after receipt of the request. The controller may extend the forty-five-day period by forty-five additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller shall inform the consumer of an extension within forty-five days after receipt of the request, together with the reasons for the delay.

b. A controller is not required to comply with a request to exercise any of the rights under subsection (1) of this section if the controller is unable to authenticate the request using commercially reasonable efforts, in which case the controller may request the provision of additional information reasonably necessary to authenticate the request.

c. A controller shall establish an internal process whereby consumers may appeal a refusal to take action on a request to exercise any of the rights.

i. Within forty-five days after receipt of an appeal, a controller shall inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support of the response. The controller may extend the forty-five-day period by sixty additional days where reasonably necessary, taking into account the complexity and number of requests serving as the basis for the appeal. The controller shall inform the consumer of an extension within forty-five days after receipt of the appeal, together with the reasons for the delay.

ii. The controller shall inform the consumer of the consumer's ability to contact the attorney general if the consumer has concerns about the result of the appeal.

d. A controller or processor is not required to do any of the following:

i. Reidentify de-identified data;

ii. Comply with an authenticated consumer request to access, correct, delete, or provide personal data in a portable format pursuant to section 6-1-1306 (1), if all of the following are true:

- The controller is not reasonably capable of associating the request with the personal data; or
- It would be unreasonably burdensome for the controller to associate the request with the personal data;
- The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and
- The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party, except as otherwise authorized by the consumer; or
- Maintain data in identifiable form or collect, obtain, retain, or access any data or technology in order to enable the controller to associate an authenticated consumer request with personal data.

e. The rights contained in section 6-1-1306 (1)(b) to (1)(e) do not apply to pseudonymous data if the controller can demonstrate that the information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

3. Privacy Policy

a. The privacy policy should include:

   i. The categories of personal data collected or processed by the controller or a processor;

   ii. The purposes for which the categories of personal data are processed;

   iii. How and where consumers may exercise the rights pursuant to section 6-1-1306, including the controller's contact information and how a consumer may appeal a controller's action with regard to the consumer's request;

   iv. The categories of personal data that the controller shares with third parties, if any; and

   v. The categories of third parties, if any, with whom the controller shares personal data.

b. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing.

c. A controller shall not require a consumer to create a new account in order to exercise a right; or based solely on the exercise of a right and unrelated to feasibility or the value of a service, increase the cost of, or decrease the availability of, the product or service.

d. Duty of purpose specification. A controller shall specify the express purposes for which personal data are collected and processed.

e. Duty of data minimization. A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed.

f. Duty to avoid secondary use. A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent.

g. Duty of care. A controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. The data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business.

h. Duty to avoid unlawful discrimination. A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

i. Duty regarding sensitive data. A controller shall not process a consumer's sensitive data without first obtaining the consumer's consent or, in the case of the processing of personal data concerning a known child, without first obtaining consent from the child's parent or lawful guardian.

4. Responsibility According to Role

a. Controllers and processors shall meet their respective obligations established under this Part 13. Processors shall adhere to the instructions of the controller and assist the controller to meet its obligations under this Part 13, taking into account the nature of processing and the information available to the processor, the processor shall assist the controller by:

i. Taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 6-1-1306;

ii. Helping to meet the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to section 6-1-716; and

iii. Providing information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 6-1-1309. The controller and processor are each responsible for only the measures allocated to them.

b. Notwithstanding the instructions of the controller, a processor shall:

i. Ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and

ii. Engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract in accordance with subsection (5) of this section that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

c. Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures.

d. Processing by a processor must be governed by a contract between the controller and the processor that is binding on both parties and that sets out:

i. The processing instructions to which the processor is bound, including the nature and purpose of the processing;

ii. The type of personal data subject to the processing, and the duration of the processing;

iii. The requirements imposed by this subsection (5) and subsections (3) and (4) of this section;

iv. At the choice of the controller, the processor shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

v. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this Part 13; and

vi. The processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational measures in support of the obligations under this Part 13 using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable. The processor shall provide a report of the audit to the controller upon request.

5. Limitations

When implementing and maintaining the procedures provided for in this policy, note the CPA, by statute, does not restrict a controller's or processor's ability to:

a. Comply with federal, state, or local laws, rules, or regulations;

b. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

c. Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local law;

d. Investigate, exercise, prepare for, or defend actual or anticipated legal claims;

e. Conduct internal research to improve, repair, or develop products, services, or technology;

f. Identify and repair technical error that impair existing or intended functionality;

g. Perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller;

h. Provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;

i. Protect the vital interests of the consumer or of another individual;

j. Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action; or

k. Process personal data for reasons of public interest in the area of public health, but solely to the extent that the processing:

   i. Is subject to suitable and specific measures to safeguard the rights of the consumer whose personal data are processed; and

   ii. Is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law; or

   iii. Assist another person with any of the activities set forth in this subsection.

l. Apply where compliance by the controller or processor with this Part 13 would violate an evidentiary privilege under Colorado law; or

m. Prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Colorado law as Part of a privileged communication.

6. Exemptions

The CPA exempts certain categories of personal data based on regulation of such information under existing federal laws and statutes. Personal data processed under an exemption shall be processed solely to the extent that the processing is necessary, reasonable, and proportionate to the specific exempted purpose or purposes listed or as otherwise authorized by the CPA. If a controller processes personal data pursuant to an exemption, the controller bears the burden of proof as to why the personal data at issue is exempt.

a. Protected health information that is collected, stored, and processed by a covered entity or its business associates;

b. Health-care information that is governed by Part 8 of article 1 of title 25 solely for the purpose of access to medical records;

c. Patient identifying information, as defined in 42 CFR 2.11, that are governed by and collected and processed pursuant to 42 CFR 2, established pursuant to 42 U.S.C. sec. 290dd-2;

d. Identifiable private information, as defined in 45 CFR 46.102, for purposes of the federal policy for the protection of human subjects pursuant to 45 CFR 46; identifiable private information that is collected as Part of human subjects research pursuant to the ich e6 good clinical practice guideline issued by the international council for harmonisation of technical requirements for pharmaceuticals for human use or the protection of human subjects under 21 CFR 50 and 56; or personal data used or shared in research conducted in accordance with one or more of the categories set forth in this subsection (2)(d);

e. Information and documents created by a covered entity for purposes of complying with HIPAA and its implementing regulations;

f. Patient safety work product, as defined in 42 CFR 3.20, that is created for purposes of patient safety improvement pursuant to 42 CFR 3, established pursuant to 42 U.S.C. secs. 299b-21 TO 299b-26;

g. Information that is:

i. De-identified in accordance with the requirements for de-identification set forth in 45 CFR 164; and

ii. Derived from any of the health-care-related information described in this section.

h. Information maintained in the same manner as information under subsections (2)(a) to (2)(g) of this section by:

i. A covered entity or business associate;

ii. A health-care facility or health-care provider; or

iii. A program of a qualified service organization as defined in 42 CFR 2.11.

i. An activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by:

i. A consumer reporting agency as defined in 15 U.S.C. sec. 1681a (f);

ii. A furnisher of information as set forth in 15 U.S.C. sec. 1681s-2 that provides information for use in a consumer report, as defined in 15 U.S.C. sec. 1681a (d); or

iii. A user of a consumer report as set forth in 15 U.S.C. sec.1681b.

This section applies only to the extent that the activity is regulated by the federal "Fair Credit Reporting Act", 15 U.S.C. sec. 1681 et seq., as amended, and the personal data are not collected, maintained, disclosed, sold, communicated, or used except as authorized by the federal "Fair Credit Reporting Act", as amended.

j. Personal data:

i. Collected and maintained for purposes of article 22 of title 10;

ii. Collected, processed, sold, or disclosed pursuant to the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq., as amended, and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with that law;

iii. Collected, processed, sold, or disclosed pursuant to the federal "Driver's Privacy Protection Act of 1994", 18 U.S.C. sec. 2721 et seq., as amended, if the collection, processing, sale, or disclosure is regulated by that law, including implementing rules, regulations, or exemptions;

iv. Regulated by the federal "Children's Online Privacy Protection Act of 1998", 15 U.S.C. secs. 6501 to 6506, as amended, if collected, processed, and maintained in compliance with that law; or

v. Regulated by the federal "Family Educational Rights and privacy act of 1974", 20 U.S.C. sec. 1232g et seq., as amended, and its implementing regulations.

k. Data maintained for employment records purposes;

l. An air carrier as defined in and regulated under 49 U.S.C. sec. 40101 et seq., as amended, and 49 U.S.C. sec. 41713, as amended;

m. A national securities association registered pursuant to the federal "Securities Exchange Act of 1934", 15 U.S.C. sec. 78o-3, as amended, or implementing regulations;

n. Customer data maintained by a public utility as defined in section 40-1-103 (1)(a)(I) or an authority as defined in section 43-4-503 (1), if the data are not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law;

o. Data maintained by a state institution of higher education, as defined in section 23-18-102 (10), the state, the judicial department of the state, or a county, city and county, or municipality if the data is collected, maintained, disclosed, communicated, and used as authorized by state and federal law for non-commercial purposes. This subsection (2)(o) does not affect any other exemption available under this Part 13;

p. Information used and disclosed in compliance with 45 CFR 164.512;

q. A financial institution or an affiliate of a financial institution as defined by and that is subject to the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq., as amended, and implementing regulations, including regulation p, 12 CFR 1016;

r. Information made available by a third party that the controller has a reasonable basis to believe is protected speech pursuant to applicable law; and

s. The processing of personal data by an individual in the course of a purely personal or household activity.

7. Data Protection Assessments

a. A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities. For purposes of this section, "processing that presents a heightened risk of harm to a consumer" includes the following:

i. Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

ii. Financial or physical injury to consumers;

iii. A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person;

iv. Selling personal data; and

v. Processing sensitive data.

b. A controller shall make the data protection assessment available to the attorney general upon request.

8. Enforcement

a. The attorney general and district attorneys have exclusive authority to enforce this Part 13 by bringing an action in the name of the state or as parens patriae on behalf of persons residing in the state to enforce this Part 13 as provided in this article 1, including seeking an injunction to enjoin a violation of this part notwithstanding any other provision of this article 1, nothing in this part 13 shall be construed as providing the basis for, or being subject to, a private right of action for violations of this part 13 or any other law.

b. For purposes only of enforcement of this Part 13 by the attorney general or a district attorney, a violation of this Part 13 is a deceptive trade practice. Each violation can result in a civil penalty of $20,000.

c. Prior to any enforcement action the attorney general or district attorney must issue a notice of violation to the controller if a cure is deemed possible. If the controller fails to cure the violation within sixty days after receipt of the notice of violation, an action may be brought pursuant to this section.

DEFINITIONS - Colorado's Consumer Data Privacy Law:

"Breach of security" or "breach" means unauthorized acquisition or use of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the covered entity.

"Covered entity" means a person that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. "Covered entity" does not include a person acting as a third-party service provider.

"Personal information" or "PI" means a Colorado resident's first name or first initial and last name plus at least one of the following: social security number, document (student ID, military ID, passport, driver's license) number, medical information, health insurance identification number, or biometric data. "Personal information" also includes a Colorado resident's username, email address, account number, credit or debit card number, plus any access codes, security questions and answers, or passwords that would permit access to an account. Note, this definition is narrower than the definition of "Personal Data" under the CPA as provided below. For the purposes of this policy, references to "personal information" correspond to the definition provided under the Colorado Breach Law and references to "Personal Data" correspond to the broader definition under the Colorado Privacy Act.

"Third-party service provider" means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity.

DEFINITIONS - Colorado Privacy Act:

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

"Authenticate" means to use reasonable means to determine that a request to exercise any of the rights in section 6-1-1306 (1) is being made by or on behalf of the consumer who is entitled to exercise the rights.

"**Authorized Agent**" as referred to in C.R.S. § 6-1-1306(1)(a)(II) means a person or entity authorized by the Consumer to act on the Consumer's behalf.

"**Biometric Data**" as referred to in C.R.S. § 6-1-1303(24)(b) means Biometric Identifiers that are used or intended to be used, singly or in combination with each other or with other Personal Data, for identification purposes. Unless such data is used for identification purposes, "Biometric Data" does not include (a) a digital or physical photograph, (b) an audio or voice recording, or (c) any data generated from a digital or physical photograph or an audio or video recording.

"**Biometric Identifiers**" means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics that can be processed for the purpose of uniquely identifying an individual, including but not limited to a fingerprint, a voiceprint, scans or records of eye retinas or irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics.

"**Bona Fide Loyalty Program**" as referred to in C.R.S. § 1-6-1308(1)(d) is defined as a loyalty, rewards, premium feature, discount, or club card program established for the genuine purpose of providing Bona Fide Loyalty Program Benefits to Consumers that voluntarily participate in that program, such that the primary purpose of Processing Personal Data through the program is solely to provide Bona Fide Loyalty Program Benefits to participating Consumers.

"**Bona Fide Loyalty Program Benefit**" is defined as an offer of superior price, rate, level, quality, or selection of goods or services provided to a Consumer through a Bona Fide Loyalty Program. Such benefits may be provided directly by a Controller or through a Bona Fide Loyalty Program Partner.

"**Bona Fide Loyalty Program Partner**" is defined as a Third Party that provides Bona Fide Loyalty Program Benefits to Consumers through a Controller's Bona Fide Loyalty Program, either alone or in partnership with the Controller.

"Business associate" has the meaning established in 45 CFR 160.103.

"Child" means an individual under thirteen years of age.

"Consent" means a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data.

"Consumer" means an individual who is a Colorado resident acting only in an individual or household context and does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context.

"Controller" means a person that, alone or jointly with others, determines the purposes for and means of processing personal data. For the purposes of this policy, the Company will, in most instances, likely be acting as a "controller" for the policies, processes, and procedures described in relation to the Company's compliance with the CPA.

"Covered entity" has the meaning established in 45 CFR 160.103.

"**Data Broker**" is defined as a Controller that knowingly collects and sells to Third Parties the Personal Data of a Consumer with whom the Controller does not have a direct relationship.

"**Data Right**" or "**Data Rights**" means the Consumer Personal Data rights granted in C.R.S. § 6-1-1306(1).

"Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

"**Decisions that produce legal or similarly significant effects concerning a consumer**" means a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.

"De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data:

a. Takes reasonable measures to ensure that the data cannot be associated with an individual;

b. Publicly commits to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and

c. Contractually obligates any recipients of the information to comply with the requirements of this subsection

"**Disability**" or "**Disabilities**" has the same meaning as set forth in C.R.S. § 24-85-102(2.3).

"**Employee**" means any person, acting as a job applicant to, or performing labor or services for the benefit of an Employer, including contingent and temporary workers and migratory laborers.

"**Employer**" means every person, entity, firm, partnership, association, corporation, migratory field labor contractor or crew leader, receiver, or other officer of court, and any agent or officer thereof, of the above-mentioned classes, employing any person.

"**Employment Records**" as referred to in C.R.S. § 6-1-1304(2)(k) means the records of an Employee, maintained by the Employer in the context of the Employer-Employee relationship having to do with hiring, promotion, demotion, transfer, lay-off or termination, rates of pay or other terms of compensation, as well as other information maintained because of the Employer-Employee relationship.

"Health-care facility" means any entity that is licensed, certified, or otherwise authorized or permitted by law to administer medical treatment in this state.

"Health-care information" means individually identifiable information relating to the past, present, or future health status of an individual.

"Health-care provider" means a person licensed, certified, or registered in this state to practice medicine, pharmacy, chiropractic, nursing, physical therapy, podiatry, dentistry, optometry, occupational therapy, or other healing arts under title 12.

"HIPAA" means the federal "Health Insurance Portability and Accountability Act of 1996", as amended, 42 U.S.C. secs. 1320d to 1320d-9.

"**Human Involved Automated Processing**" means the automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing.

"**Human Reviewed Automated Processing**" means the automated processing of Personal Data where a human reviews the automated processing, but the level of human engagement does not rise to the level required for Human Involved Automated Processing. Reviewing the output of the automated processing with no meaningful consideration does not rise to the level of Human Involved Automated Processing.

"Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly, in Particular by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier.

"**Intimate Image**" means any visual depiction, photograph, film, video, recording, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, that depicts an identified or identifiable person's private parts, or a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy.

"**Noncommercial Purpose**" as referred to in C.R.S. § 6-1-1304(2)(o) includes, but is not limited to, the following activities when conducted by: (a) a state institution of higher education, as defined in

C.R.S. § 23-18-102(10), the state, the judicial department of the state, or a county, city and county, or municipality; or (b) a Processor acting on behalf of one or more of the foregoing:

a. Processing activities related to the delivery of services and benefits;

b. Research purposes;

c. Budgeting;

d. Improving operations or the delivery services or benefits;

e. Auditing operations or service or benefit delivery;

f. Sharing Personal Data between these categories of entities for any of these purposes; or

g. Any other purpose related to speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

"Personal data" means information that is linked or reasonably linkable to an identified or identifiable individual and does not include de-identified data or publicly available information. As used in this policy, "personal data" is broader than the definition of "personal information" as defined by the Colorado Breach Law.

"Publicly available information" means information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public.

"Process" or "processing" means the collection, use, sale, storage, disclosure, analysis, deletion, or modification of personal data and includes the actions of a controller directing a processor to process personal data.

"Processor" means a person that processes personal data on behalf of a controller.

"Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Protected health information" has the meaning established in 45 CFR 160.103.

"Pseudonymous data" means personal data that can no longer be attributed to a specific individual without the use of additional information if the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to a specific individual.

“**Revealing**” as referred to in C.R.S. § 6-1-1303(24)(a) includes Sensitive Data Inferences. For example:

a. While precise geolocation information at a high level may not be considered Sensitive Data, precise geolocation data which is used to infer an individual visited a mosque and is used to infer that individual’s religious beliefs is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a). Similarly, precise geolocation data which is used to infer an individual visited a reproductive health clinic and is used to infer an individual’s health condition or sex life is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

b. While web browsing data at a high level may not be considered Sensitive Data, web browsing data which, alone or in combination with other Personal Data, infers an individual’s sexual orientation is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

"Sale", "sell", or "sold" means the exchange of personal data for monetary or other valuable consideration by a controller to a third Party. "Sale", "sell", or "sold" does not include the following:

a. The disclosure of personal data to a processor that processes the personal data on behalf of a controller;

b. The disclosure of personal data to a third Party for purposes of providing a product or service requested by the consumer;

c. The disclosure or transfer of personal data to an affiliate of the controller; and

d. The disclosure or transfer to a third Party of personal data as an asset that is Part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third Party assumes control of all or Part of the controller's assets; or

e. The disclosure of personal data that a consumer directs the controller to disclose or intentionally discloses by using the controller to interact with a third Party or intentionally made available by a consumer to the general public via a channel of mass media.

"Sensitive data" means:

a. Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status;

b. Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or

c. Personal data from a known child.

"**Sensitive Data Inference**" or "**Sensitive Data Inferences**" means inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status.

"**Solely Automated Processing**" means the automated processing of Personal Data with no human review, oversight, involvement, or intervention.

"Targeted advertising" means displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests and does not include:

a. Advertising to a consumer in response to the consumer's request for information or feedback;

b. Advertisements based on activities within a controller's own websites or online applications;

c. Advertisements based on the context of a consumer's current search query, visit to a website, or online application; or

d. Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

"Third Party" means a person, public authority, agency, or body other than a consumer, controller, processor, or affiliate of the processor or the controller.

"Universal Opt-Out Mechanism" or **"Universal Opt-Out Mechanisms"** means mechanisms that clearly communicate a Consumer's affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for purposes of Targeted Advertising or the Sale of Personal Data pursuant to C.R.S. § 6-1-1306 (1)(a)(I)(A) or (1)(a)(I)(B), which meets the technical specifications set forth in 4 CCR 904-3, Rule 5.06 pursuant to C.R.S. § 6-1-1313(2).

REFERENCES:

1. Colorado's Consumer Data Privacy Law (or Colorado Breach Law as referenced in this policy)
2. Colorado Privacy Act
3. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Standards for Notification in the Case of Breach of Unsecured Protected Health Information, 45 CFR Parts 160 and 164

4. Protected Health Information Breach Risk Assessment and Notification, IP.PRI.011