DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** California Consumer Privacy Act of 2018 (CCPA) as Amended by the California Privacy Rights Act (CPRA) and Data Breaches
PAGE: 1 of 31	**REPLACES POLICY DATED:** 1/1/2020, 8/1/2020, 5/1/2021,10/1/2021
EFFECTIVE DATE: January 1, 2023	**REFERENCE NUMBER:** IP.DP.CA.001
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities, including, but not limited to hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, shared services centers, home health agencies, and hospice agencies that conduct business in California as well as all members of their workforce, including, but not limited to employees, physicians, contractors, and volunteers.

A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information (PI), or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' PI, that does business in the State of California, and that satisfies one or more of the following thresholds:

1) As of January 1, of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

2) Alone or in combination, annually buys, sells, or shares the PI of 100,000 or more consumers or, households.

3) Derives 50 percent or more of its annual revenues from selling or sharing consumers' PI.

PURPOSE: To establish Company policy for compliance with the California Consumer Privacy Act of 2018 (CCPA) as amended by the California Privacy Rights Act (CPRA) and the requirements for each Company-affiliated facility in California when it may have failed to protect the privacy and security of medical information, and other PI under California state law; to outline the applicable state notification requirements in the event of a reportable incident; and to provide guidance regarding workforce members' responsibilities related to potential security breaches involving PI and the potential improper access to, use or disclosure of medical information.

Note: This policy replaces the state-specific facility model policy for California – Data Breaches.

POLICY:

Governance and Accountability for Data Breaches of Personal Information (PI)/Personal Identifiable Information (PI/PII) and/or Medical Information

Any Company-affiliated facility must notify the patient or their personal representative, and if required, the California Department of Public Health (CDPH) and the California Attorney General's Office when required under applicable California law, as a result of the breach of the security of a system containing unencrypted PI or the unlawful or unauthorized access to, use or disclosure of medical information.

Each facility will be responsible for reporting violations regarding their patients regardless of the offender (SSC, Supply Chain, Business Associate, Physician, Employee, Corporate, Division, Contractor, etc.).

Governance and Accountability for CPRA Compliance

The Company is responsible for ensuring that:

A. PI is collected and processed in accordance with the CPRA;

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 will draft all required revisions to the online Privacy Policy and the Corporate Information Technology Group or Division Marketing leadership 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 at that location will forward Consumer requests to business owners such as the Corporate Marketing Department, and certain business owners of applications that may store California resident PI, as needed, for resolution. Generally, facilities will not receive or process Consumer requests.

Exemptions

The obligations imposed on businesses by the CPRA shall not restrict a business's ability to:

A. Comply with federal, state, or local laws or comply with a court order or subpoena to provide information.

B. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. Law enforcement agencies, including police and sheriff's departments, may direct a business pursuant to a law enforcement agency- approved investigation with an active case number not to delete a consumer's PI, and upon receipt of that direction, a business shall not delete the PI for 90 days in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer's PI. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's PI for additional 90-day periods. A business that has received direction from a law enforcement agency not to delete the PI of a consumer who has requested deletion of the consumer's PI shall not use the consumer's PI for any

purpose other than retaining it to produce to law enforcement in response to a court- issued subpoena, order, or warrant unless the consumer's deletion request is subject to an exemption from deletion under this title.

C. Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

D. Cooperate with a government agency request for emergency access to a consumer's PI if a natural person is at risk or danger of death or serious physical injury provided that:
   1. The request is approved by a high-ranking agency officer for emergency access to a consumer's PI.
   2. The request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis.
   3. The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.

E. Exercise or defend legal claims.

F. Collect, use, retain, sell, share, or disclose consumers' PI that is deidentified or aggregate consumer information.

G. Collect, sell, or share a consumer's PI if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's PI occurred in California, and no PI collected while the consumer was in California is sold. This paragraph shall not prohibit a business from storing, including on a device, PI about a consumer when the consumer is in California and then collecting that PI when the consumer and stored PI is outside of California.

H. The obligations imposed on businesses by Sections 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, and 1798.135 shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the PI of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

This title shall not apply to any of the following:

A. Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164

of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

B. A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).

C. PI collected as part of a clinical trial or other biomedical research study subject to, or conducted in accordance with, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration, provided that the information is not sold or shared in a manner not permitted by this subparagraph, and if it is inconsistent, that participants be informed of that use and provide consent.

   For purposes of this subdivision, the definitions of “medical information” and “provider of health care” in Section 56.05 shall apply and the definitions of “business associate,” “covered entity,” and “protected health information” in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

D. This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any PI bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code. This shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act. This exemption does not apply to Section 1798.150 of the CPRA (private right of action).

E. This title shall not apply to PI collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial

Code), or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.). This exemption does not apply to Section 1798.150 of the CPRA (private right of action).

F. This title shall not apply to PI collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This exemption does not apply to Section 1798.150 of the CPRA (private right of action).

G. Sections 1798.105 and 1798.120 of the CPRA shall not apply to a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business that the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.

   For the purposes of this subdivision:

   1. "Business controller information" means the name or names of the owner or owners, director, officer, or management employee of a business and the contact information, including a business title, for the owner or owners, director, officer, or management employee.
   2. "Commercial credit reporting agency" has the meaning set forth in subdivision (b) of Section 1785.42.
   3. "Owner" means a natural person that meets one of the following:
      (i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.
      (ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.
      (iii) Has the power to exercise a controlling influence over the management of a company.
   4. "Director" means a natural person designated in the articles of incorporation of a business as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.
   5. "Officer" means a natural person elected or appointed by the board of directors of a business to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.
   6. "Management employee" means a natural person whose name and contact information is reported to or collected by a commercial credit reporting agency as the primary manager of a business and used solely within the context of the natural person's role as the primary manager of the business.

H. The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 of the CPRA shall not apply to household data.

I. This title does not require a business to comply with a verifiable consumer request to delete a consumer's PI under Section 1798.105 to the extent the verifiable consumer request applies to a student's grades, educational scores, or educational test results that the business holds on behalf of a local educational agency, as defined in subdivision (d) of Section 49073.1 of the Education Code, at which the student is currently enrolled. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception. This title does not require, in response to a request pursuant to Section 1798.110, that a business disclose on educational standardized assessment or educational assessment or a consumer's specific responses to the educational standardized assessment or educational assessment if consumer access, possession, or control would jeopardize the validity and reliability of that educational standardized assessment or educational assessment. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception. For purposes of this subdivision:
    1. "Educational standardized assessment or educational assessment" means a standardized or non-standardized quiz, test, or other assessment used to evaluate students in or for entry to kindergarten and grades 1 to 12, inclusive, schools, postsecondary institutions, vocational programs, and postgraduate programs that are accredited by an accrediting agency or organization recognized by the State of California or the United States Department of Education, as well as certification and licensure examinations used to determine competency and eligibility to receive certification or licensure from a government agency or government certification body.
    2. "Jeopardize the validity and reliability of that educational standardized assessment or educational assessment" means releasing information that would provide an advantage to the consumer who has submitted a verifiable consumer request or to another natural person.

J. Sections 1798.105 and 1798.120 shall not apply to a business' use, disclosure, or sale of particular pieces of a consumer's PI if the consumer has consented to the business' use, disclosure, or sale of that information to produce a physical item, including a school yearbook containing the consumer's photograph if:
    1. The business has incurred significant expense in reliance on the consumer's consent.
    2. Compliance with the consumer's request to opt out of the sale of the consumer's PI or to delete the consumer's PI would not be commercially reasonable.
    3. The business complies with the consumer's request as soon as it is commercially reasonable to do so.

K. A company service provider, or contractor to is not required to:
    1. Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered PI.
    2. Retain any PI about a consumer if, in the ordinary course of business, that information about the consumer would not be retained.

3. Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with PI.

Disclosure and Transparency Requirements

A. The Company must disclose the following information in its online privacy policy and in any California-specific description of consumers' privacy rights on its internet website and in response to consumer right to know requests:

1. A list of the categories of PI it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the PI collected.
2. The categories of sources from which consumers' PI is collected.
3. The business or commercial purpose for collecting, selling, or sharing consumers' PI.
4. The categories of third parties to whom the business discloses consumers' PI.

B. In two separate lists, the Company must also disclose the following information in its online privacy policy and in response to consumer right to know requests:

1. A list of the categories of PI it has sold or shared about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the PI sold or shared, or if the business has not sold or shared consumers' PI in the preceding 12 months, the business shall prominently disclose that fact in its privacy policy.

2. A list of the categories of PI it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the PI disclosed, or if the business has not disclosed consumers' PI for a business purpose in the preceding 12 months, the business shall disclose that fact.

   The privacy policy must be updated at least once every 12 months.

C. Notice at Collection – At or before the point of collection of a consumer's PI, the Company must:

1. Inform consumers via website homepage, online privacy policy, or via paper version of the notice, as to the categories of PI to be collected and the purpose for which the categories of PI will be collected or used and whether that information will be sold or shared.
2. Inform Consumers the length of time the Company intends to retain each category of PI.

California Residents - Consumer Rights

A. Consumers' Right to Know and Access What PI is Being Collected:

1. A consumer shall have the right to request that a business that collects PI about the consumer disclose to the consumer the following:
   i. The categories of PI it has collected about that consumer.
   ii. The categories of sources from which the PI is collected.
   iii. The business or commercial purpose for collecting, selling, or sharing PI.
   iv. The categories of third parties to whom the business discloses PI.
   v. Upon receipt of a verifiable consumer request from the consumer, the Company is required to provide the specific pieces of PI it has collected about that consumer.

The Company is not obligated to retain any PI collected for a single, one-time transaction, if such information is not sold or retained by the Company; collect PI that it would not otherwise collect in the ordinary course of its business; retain PI for longer than it would otherwise retain such information in the ordinary course of its business; or to re-identify or otherwise link information that is not maintained in a manner that would be considered PI.

B. Consumers' Right to Delete PI

1. A consumer shall have the right to request that the Company delete any PI about the consumer which the Company has collected from the consumer.

2. If the Company receives a verifiable consumer request from a consumer to delete the consumer's PI it shall delete the consumer's PI from its records, notify any service providers or contractors to delete the consumer's PI from their records, and notify all third parties to whom the Company has sold or shared the PI to delete the consumer's PI unless this proves impossible or involves disproportionate effort.

3. The Company may maintain a confidential record of deletion requests solely for the purpose of preventing the PI of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes, solely to the extent permissible under this title.

4. The Company, service provider or contractor acting pursuant to its contract with the Company, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's PI if it is reasonably necessary for the Company, service provider, or contractor to maintain the consumer's PI in order to:
   i. Complete the transaction for which the PI was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a Company's ongoing Company relationship with the consumer, or otherwise perform a contract between the Company and the consumer.

ii. Help to ensure security and integrity to the extent the use of the consumer's PI is reasonably necessary and proportionate for those purposes.

iii. Debug to identify and repair errors that impair existing intended functionality.

iv. Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

v. Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

vi. Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the Company's deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent.

vii. To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the Company and compatible with the context in which the consumer provided the information.

viii. Comply with a legal obligation.

C. Consumers' Right to Correct Inaccurate PI

1. A consumer shall have the right to request the Company that maintains inaccurate PI about the consumer to correct that inaccurate PI, taking into account the nature of the PI and the purposes of the processing of the PI.

2. A Company that receives a verifiable consumer request to correct inaccurate PI shall use commercially reasonable efforts to correct the inaccurate PI as directed by the consumer.

D. Right to Opt-Out of the Sale or Sharing of PI – The right to opt-out refers to the right of a consumer to direct a business that sells or shares PI about the consumer to third parties not to sell or share the consumer's PI. If the Company sells or shares consumers' PI to third parties then it must provide notice to consumers that this information may be sold or shared and that consumers have the right to opt-out of the sale or sharing of their PI.

E. Right to Opt-In to the Sale of PI (Minors) – The right to opt-in refers to the requirement that the Company not sell or share the PI of a consumer who is less than 16 years of age unless the Company has received an affirmative authorization for the sale or sharing of the consumer's PI. If a minor is, at least 13 years of age and less than 16 years of age, the minor can provide the affirmative authorization directly to the Company. If a minor is under the age of 13, a parent or

guardian must provide the affirmative authorization. An affirmative authorization is required from a consumer who has previously opted out of the sale of their PI.

F. Right to Limit the Use and Disclosure of Sensitive PI - A consumer shall have the right, at any time, to direct a business that collects sensitive PI about the consumer to limit its use of the consumer's sensitive PI to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer.

G. Right to Non-Discrimination – The right to non-discrimination refers to the prohibition against discriminating against consumers who exercise their rights under the CPRA, including, but not limited to, (a) denying goods or services to the consumer, (b) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties, (c) providing a different level or quality of goods or services to the consumer, or (d) suggesting the consumer will receive a different price or rate for goods or services or different level or quality of goods or services. This right does not prohibit the Company from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

H. Accessibility – The Company must ensure that notices and information provided to consumers are accessible to consumers with disabilities and are available in the language primarily used to interact with the consumer.

I. Financial Incentives – If the Company offers financial incentives, it shall notify consumers of the financial incentives, obtain a consumer's prior opt-in consent, which clearly describes the material terms of the financial incentive program and which may be revoked by the consumer at any time.

<u>Training</u>

A. The Company will provide training to key stakeholders who are involved in any processing of PI. Those stakeholders include the following:
   1. Marketing;
   2. National Contact Center Management (NCCM);
   3. Information Technology Group (ITG);
   4. Far West Division Ethics and Compliance Officer (ECO), Operations Counsel, Human Resources; and
   5. Other identified stakeholders.

B. The Company will provide training to all workforce members who are responsible for handling consumer inquiries about the Company's privacy practices or the Company's compliance with the CPRA and data breaches to ensure that such workforce members are informed of all

requirements in the CPRA how to direct consumers to exercise their rights and to ensure all of the requirements for breach notification and timely reporting are met.

C. Training will be provided to newly acquired entities impacted by CPRA.

D. Training will be made available via different methods (e.g., HealthStream course, WebEx, PowerPoint).

E. Training will be provided by Information Protection and Security

F. Training will occur:
   1. When new amendments or regulations are made to the Act and the changes have an impact on the key stakeholders; and
   2. During new acquisition due diligence training.

Private Right of Action

A. For the purposes of the private right of action only, "PI" has the narrower meaning given to it under California Civil Code § 1798.81.5.

B. Any consumer whose non-encrypted PI, non-redacted PI or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as the result of the Company's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PI may institute a civil action for any of the following (a) to recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty dollars ($750) per consumer per incident or actual damages, whichever is greater, and (b) injunctive or declaratory relief.

C. Actions may be brought by a consumer if, prior to initiating any action against the Company for statutory damages on an individual or class-wide basis a consumer provides the Company 30 days' written notice identifying the specific provisions of the CPRA the consumer alleges have been or are being violated.
   1. In the event a cure is possible, if within the 30 days the Company actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the Company.
   2. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of the CPRA.
   3. If the Company continues to violate the CPRA in breach of the express written statement provided to the consumer, the consumer may initiate an action against the Company to enforce the written statement and may pursue statutory damages for each breach of the

express written statement, as well as any other violation of the CPRA that postdates the written statement.

Administrative Enforcement

A. The Company's failure to cure any alleged violation within the time period specified by the California Privacy Protection Agency, if any, after being notified of alleged noncompliance by California Privacy Protection Agency is a violation of the CPRA.

B. Any business, service provider, contractor, or other person that violates the CPRA shall be liable for an administrative fine of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation or violations involving the PI of consumers whom the business, service provider, contractor, or other person has actual knowledge are under 16 years of age in an administrative enforcement action brought by the California Privacy Protection Agency.

PROCEDURE:

A. The Company will implement procedures to enable consumers to exercise the rights granted by the CPRA.

B. The Company will use reasonable efforts to disclose and deliver information, as required by the CPRA and this Policy, to a consumer free of charge within 45 days of receiving a verifiable consumer request. The time-period to provide the required information may be extended once by an additional 45 days when reasonably necessary, or by up to 90 additional days where necessary, taking into account the complexity and number of the requests, provided the consumer is provided notice of the extension within the first 45-day period and provided with the reasons for the delay.
   1. The disclosure shall cover the 12-month period preceding the Company's receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the Company, if the consumer maintains an account with the Company, or by electronic webform, via email or toll-free number at the consumer's option if the consumer does not maintain an account with the Company, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The Company may require authentication of the consumer that is reasonable in light of the nature of the PI requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through the account.
   2. The Company is not obligated to provide the information required to the same consumer more than twice in a 12-month period.
   3. If the Company does not take action on the request of the consumer, the Company will inform the consumer, without delay, and at the latest within the time-period permitted for

response as set forth above, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the Company.

4. If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the Company may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request.

C. The Company will ensure that all individuals responsible for handling consumer inquiries about the Company's privacy practices and/or the Company's compliance with the CPRA are informed of all requirements of the CPRA provisions and how to direct consumers to exercise their rights under the CPRA.

D. The Company will make available to consumers the following methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, an interactive webform, a toll-free telephone number and an email address. If the Company maintains an Internet website, the company will make the Internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

E. The Company will include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" in:
   1. Its online privacy policy or policies if the Company has an online privacy policy or policies.
   2. Any California-specific description of consumers' privacy rights.

F. The Company will respect a consumer's decision to opt-out of the sale or sharing of the consumer's PI for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's PI.

G. The Company will implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PI from unauthorized access and exfiltration, theft, or disclosure.

H. Workforce members of any Company-affiliated facility in California shall report any suspected unauthorized acquisition of unencrypted, computerized PI or suspected unlawful or unauthorized access to, use or disclosure of medical information:

I. The circumstances of the suspected violation will be reviewed to determine if the incident must be reported under California Health and Safety Code Section 1280.15 or California Civil Code Section 1798.82. In evaluating whether a security or privacy incident is reportable under California law, the following shall be assessed:

1. An unlawful or unauthorized access to, use or disclosure of medical information must be reported under **Health and Safety Code Section 1280.15** if:
   a. the Company-affiliated facility is licensed by the California Department of Public Health (CDPH) under Health and Safety Code Section 1250 (as a hospital, skilled nursing facility, psychiatric health facility, etc.), as a clinic under Health and Safety Code Section 1204, as a home health agency licensed under Health and Safety Code Section 1725 or as a hospice under Health and Safety Code Section 1745;
   b. there has been an unlawful or unauthorized access to, or use or disclosure of, a patient's medical information; and
   c. the unlawful or unauthorized access to, or use or disclosure, of a patient's medical information did not involve internal paper records, emails or faxes misdirected within the same facility within the course of coordinating care or delivery of services.

2. A breach of the security of the system is reportable under **Civil Code Section 1798.82** if:
   a. there was an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of PI maintained; and
   b. the acquisition did not involve a good faith acquisition of PI by an employee or agent for business purposes.

J. Reportable Incidents under Health and Safety Code Section 1280.15
   1. Notification to Patient:
      a. Timing and Mechanics: The Company-affiliated facility shall report in writing, by first class mail, a breach of a patient's medical information under Health and Safety Code Section 1280.15 as outlined in section I 1. a.-c. above to the affected patient or the patient's personal representative at the last known address, or by electronic mail, if the patient or the patient's representative agrees and such agreement has not been withdrawn, pursuant to Part 164.404(d) of Title 45 of the Code of Federal Regulations no later than 15 business days after the unlawful or unauthorized access, use or disclosure has been detected.
      b. Content: The content of the notice to patients or the patient's representative shall be written in plain language and include a brief description of what happened, including the facility's name and address, the date of the breach and the date of the discovery of the breach, if known; a description of the types of medical information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, diagnosis, or other types of information); any steps the patient should take to protect himself or herself from potential harm resulting from the breach; a brief description of what the facility involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and contact procedure for individuals to ask question or learn additional information, which shall include a toll-free telephone number, an email address, internet website address, or postal address. To the extent reporting is also required under HIPAA; a single notice to the patient can be used as long as it satisfies both the HIPAA and state law requirements and timelines.

c. Penalties: If the health care facility does not report a breach of a patient's medical information to a patient or the patient's representative, the Department may assess a penalty in the amount of $100 (one hundred dollars) for each day that the breach is not reported to the patient or the patient's representative, not to exceed the limits set forth in Health and Safety Code section 1280.15.

d. Other Administrative Penalties: CDPH may impose an administrative penalty if it determines that the health care facility has committed a breach of a patient's medical information. The penalty assessed for any violation, including penalty adjustment factors, shall not exceed the maximum penalty specified in Health and Safety Code section 1280.15.

When an administrative penalty has been determined by CDPH, the base penalty is $15,000 for each violation subject to the penalty adjustment factors provided in section 79904.

For each subsequent occurrence of a breach of a patient's medical information relating to a particular reported event, CDPH may assess an administrative penalty in an amount equal to 70% of the initial violation's final penalty amount. The administrative penalty for the subsequent occurrence shall be subject to the penalty adjustment factors pursuant to section 79904, if applicable, not to exceed the statutory maximum of $17,500 per subsequent occurrence. For additional penalty adjustment factors, see section 79904.

See section 79905 to assess administrative penalties for small and rural hospitals, primary care clinics, and skilled nursing facilities for a breach of a patient's medical information pursuant to Health and Safety Code section 1280.15.

2. Notification to CDPH:
   a. Timing and Mechanics: The health care facility, excluding a business associate, shall report any incident reportable under Section I, 1a-c. above in writing and signed by a representative of the health care facility by electronic mail, telephone, facsimile transmission, first-class mail, or through an internet website maintained by CDPH not later than 15 business days after the breach has been detected.
   b. Content: Pursuant to Chapter 13, Section 79902, the report should include the following:
      i. Name and address of the health care facility where the breach occurred;
      ii. Date and time that each breach occurred;
      iii. Date and time that each breach was detected;
      iv. Name of patient(s) affected;
      v. Description of the medical information that was breached, including the nature and extent of the medical information involved, including the types of individually identifiable information (as defined in Civil Code section 56.05), and the likelihood of reidentification;
      vi. Description of the events surrounding the breach;

vii. Name(s) and contact information of the individual(s) who performed the breach, any witness(es) to the breach, and any unauthorized person(s) who used the medical information or to whom the disclosure was made, to the extent known;
viii. Date that patient or patient's representative was notified, was attempted to be notified, or will be notified of breach;
ix. The contact information of a health care facility representative whom the Department may contact for additional information;
x. Description of any corrective or mitigating action taken by the health care facility;
xi. Any other instances of a reported event that includes a breach of that patient's medical information by the health care facility in the previous six years.
xii. A copy of the notification sent to the patient or patient's representative, pursuant to section 79902(b), and any additional information provided to the patient or patient's representative relating to the breach; and
xiii. Any audit reports, witness statements, or other documents that the health care facility relied upon in determining that a breach occurred.
xiv. The health care facility shall report any additional information relevant to the breach, as it become available, beyond the 15 business days.

c. Penalties – If the health care facility fails to report a breach of a patient's medical information to CDPH, CDPH may assess a penalty in the amount of $100 (one hundred dollars) for each day that the breach is not reported to CDPH, not to exceed the limits set forth in Health and Safety Code section 1280.15.
d. A breach shall not be deemed reported to the Department unless the health care facility has provided, or made a good faith effort to provide the items required in Section J, 2b i – xiv above.
i. Any items required for reporting not available to the health care facility at the time of the reporting shall be provided to CDPH as they are available.
ii. Any unreasonable delays in reporting by the health care facility pursuant to this subdivision are subject to an administrative penalty assessed pursuant to Section J, 2c.

3. The facility shall delay the reporting in Section I 1. a., if a law enforcement agency or official provides the facility with a written or oral statement that compliance with the reporting requirements would likely impede the law enforcement agency's investigation. If this occurs, consult with Information Protection and Security for further guidance.

K. Reportable Incidents under California Civil Code Section 1798.82
1. If an incident is reportable under California Civil Code Section 1798.92 (as outlined in Section I, 2. a.-b. above), and also must be reported under the HIPAA Breach Notification Rule, the notice provided under HIPAA will be deemed compliant with the notice requirements of Civil Code Section 1798.82.
2. If notice is required under Civil Code Section 1798.82 but is not required under HIPAA, the following specific provisions shall apply:

a. Notice must be made in the most expedient time possible and without unreasonable delay. Notice may be delayed if a law enforcement agency determines it will impede a criminal investigation.
b. Notice may be provided in writing (on paper), electronically in conformity with the federal E-SIGN Act, or by substitute notice if the costs of providing notice will exceed $250,000 or if more than 500,000 consumers are affected, or if the business does not have sufficient contact information. Substitute notice consists of all of the following: email notice (when the business has an email address), conspicuous posting on the website, and notification to major statement news media.
c. The notice shall be written in plain language, shall be titled “Notice of Data Breach” and shall present the information described under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” The text of the notice shall be no smaller than 10-point type. Include the following:
    (1) facility’s name and contact information;
    (2) types of information breached;
    (3) if known: the date, estimated date, or date range of breach;
    (4) the date of the notice;
    (5) whether notification was delayed as a result of a law enforcement investigation;
    (6) a general description of the breach incident, if known;
    (7) the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or driver’s license or California identification number; and
    (8) information regarding identify theft prevention services, if offered.
    (9) At the discretion of the person or business, the security breach notification may also include any of the following:
        i. Information about what the person or business has done to protect individuals whose information has been breached.
        ii. Advice on steps that people whose information has been breached may take to protect themselves.
        iii. In breaches involving biometric data, instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on data for authentication purposes.
d. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed PI, as defined above.
e. If the facility is required to issue a security breach notification pursuant to California Civil Code Section 1798.82 under Section I, 2. a.-b. above, to more than 500 California residents as a result of a single breach, the facility shall submit

electronically a sample copy of the notification, excluding any personally identifiable information, and complete and submit the Attorney General's Data Security Breach Form, to the Attorney General at https://oag.ca.gov/ecrime/databreach/report-a-breach.

f. In the case of a breach of the security of the system involving a user name or email address, in combination with a password or security question and answer that would permit access to an online account:
   (1) When no other PI as defined above is involved, the facility may provide notice in electronic or other form that directs the person whose PI has been breached; to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose PI has been breached using the same user name or email address and password or security question or answer.
   (2) Any such notice shall not be to the email address to which the login credentials have been compromised but instead, should be made by another method described in subdivision (j) of California Civ. Code section 1798.82 or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

L. In addition to complying with this policy, any Company-affiliated facility must also comply with the Protected Health Information Breach Risk Assessment and Notification Policy, Reference number IP.PR1.011.

DEFINITIIONS UNDER THE CPRA

1) **Advertising and marketing** means a communication by a business or a person acting on the business' behalf in any medium intended to induce a consumer to obtain goods, services, or employment.

2) **Aggregate consumer information** means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

3) **Biometric information** means an individual's physiological, biological or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that can be is used or is intended to be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not

limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a face print, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

4) **Business** means:
   a. A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' PI, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' PI, that does business in the State of California, and that satisfies one or more of the following thresholds:
      1. As of January 1, of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
      2. Alone or in combination, annually buys, sells, or shares the PI of 100,000 or more consumers or, households.
      3. Derives 50 percent or more of its annual revenues from selling or sharing consumers' PI.
   b. Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' PI. **Control or controlled** means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. **Common branding** means a shared name, service mark, or trademark that the average consumer would understand that two or more entities are commonly owned.
   c. A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that PI in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.
   d. A person that does business in California, that is not covered by paragraph (1), (2), or (3) and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

5) **Business purpose** means the use of PI for the business's operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (11) of subdivision (a) of Section 1798.185, provided that the use of PI shall be reasonably necessary and proportionate to achieve the purpose for which the PI was collected or processed or for another purpose that is compatible with the context in which the PI was collected. Business purposes are:

a. Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
b. Helping to ensure security and integrity to the extent the use of the consumer's PI is reasonably necessary and proportionate for these purposes.
c. Debugging to identify and repair errors that impair existing intended functionality.
d. Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's PI is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.
e. Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.
f. Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the PI of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with PI that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.
g. Undertaking internal research for technological development and demonstration
h. Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

6) **Collects, collected, or collection** means buying, renting, gathering, obtaining, receiving, or accessing any PI pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.
7) **Commercial purposes** means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.
8) **Consent means** any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of PI relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of PI processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a

given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

9) **Consumer** means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

10) **Contractor** means a person to whom the business makes available a consumer's PI for a business purpose, pursuant to a written contract with the business, provided that the contract: Prohibits the contractor from:
   a. Selling or sharing the PI.
   b. Retaining, using, or disclosing the PI for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the PI for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.
   c. Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business.
   d. Combining the PI that the contractor receives pursuant to a written contract with the business with PI that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the contractor may combine PI to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) and in regulations adopted by the California Privacy Protection Agency.
   e. Includes a certification made by the contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.
   f. Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.
   g. If a contractor engages any other person to assist it in processing PI for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing PI for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

11) **Cross-context behavioral advertising** means the targeting of advertising to a consumer based on the consumer's PI obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

12) **Dark** pattern means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation.

13) **Deidentified** means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:
    a. Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.
    b. Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.
    c. Contractually obligates any recipients of the information to comply with all provisions of this subdivision.

14) **Designated methods for submitting requests** means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

15) **Device** means any physical object that is capable of connecting to the Internet, directly or **indirectly**, or to another device.

16) **Homepage** means the introductory page of an internet website and any internet web page where **PI** is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information,'' or settings page, and any other location that allows consumers to review the notices required by this title, including, but not limited to, before downloading the application.

17) **Household** means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services.

18) **Infer or inference** means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

19) Intentionally **interacts** means when the consumer intends to interact with a person, or disclose PI to a person, via one or more deliberate interactions, including visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.

20) **Non-**personalized **advertising** means advertising and marketing that is based solely on a consumer's PI derived from the consumer's current interaction with the business with the exception of the consumer's precise geolocation.

21) **Person** means **an** individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

22) **Personal Information (PI)** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. PI includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

a. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
b. Any PI described in subdivision (e) of Section 1798.80.
c. Characteristics of protected classifications under California or federal law.
d. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
e. Biometric information.
f. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.
g. Geolocation data.
h. Audio, electronic, visual, thermal, olfactory, or similar information.
i. Professional or employment-related information.
j. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).
k. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
l. Sensitive Personal Information (SPI)

Personal information does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

Personal information does not include consumer information that is deidentified or aggregate consumer information.

23) **Precise geolocation** means any data that is derived from a device and that is used or intended to **be** used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.

24) **Probabilistic identifier** means the identification of a consumer or a consumer's device to a degree of **certainty** of more probable than not based on any categories of PI included in, or similar to, the categories enumerated in the definition of PI.

25) **Processing** means any operation or set of operations that are performed on PI or on sets of PI, whether or not by automated means.

26) **Profiling means** any form of automated processing of PI, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

27) **Pseudonymize or Pseudonymization** means the processing of PI in a manner that renders **the** PI no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the PI is not attributed to an identified or identifiable consumer.

28) **Research** means scientific analysis, systematic study and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge and that adheres or otherwise conforms to all other applicable ethics and privacy laws, or including, but not limited to, studies conducted in the public interest in the area of public health. Research with PI that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:
    a. Compatible with the business purpose for which the PI was collected.
    b. Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer*, by a business*.
    c. Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain*, other than as needed to support the research.*
    d. Subject to business processes that specifically prohibit reidentification of the information*, other than as needed to support the research*.
    e. Made subject to business processes to prevent inadvertent release of deidentified information.

f. Protected from any reidentification attempts.
g. Used solely for research purposes that are compatible with the context in which the PI was collected.
h. Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals as are necessary to carry out the research purpose.

29) **Security and integrity** means the ability of:
a. Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted PI.
b. Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.
c. Businesses to ensure the physical safety of natural

30) **Sell, selling, sale, or sold**, means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's PI by the business to a third party for monetary or other valuable consideration.

For purposes of this title, a business does not sell PI when a consumer uses or directs the business to intentionally disclose PI:

a. The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's PI or limited the use of the consumer's sensitive PI for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's PI or limited the use of the consumer's sensitive PI.
b. The business transfers to a third party the PI of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the PI of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

31) **Sensitive personal information** means PI that reveals:
a. A consumer's social security, driver's license, state identification card, or passport number.
b. A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

c. A consumer's precise geolocation.
d. A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.
e. The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.
f. A consumer's genetic data.
g. The processing of biometric information for the purpose of uniquely identifying a consumer.
h. PI collected and analyzed concerning a consumer's health.
i. PI collected and analyzed concerning a consumer's sex life or sexual orientation.

Sensitive PI that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive PI or PI.

32) **Service or services** means work, labor, and services, including services furnished in connection with the sale or repair of goods.

33) **Service provider** means a person that processes PI on behalf of a business and to that receives from or on behalf of the business a consumer's PI for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:
a. Selling or sharing the PI.
b. Retaining, using, or disclosing the PI for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the PI for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title.
c. Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.
d. Combining the PI that the service provider receives from, or on behalf of, the business with PI that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine PI to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

If a service provider engages any other person to assist it in processing PI for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing PI for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth above.

34) **Share, shared, or sharing** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other

means, a consumer's PI by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

a. For purposes of this title, a business does not share PI when a consumer uses or directs the business to intentionally disclose PI; or intentionally interact with one or more third parties. The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's PI or limited the use of the consumer's sensitive PI for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's PI or limited the use of the consumer's sensitive PI.
b. The business transfers to a third party the PI of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the PI of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

35) **Third party** means a person who is not any of the following:
   a. The business with whom the consumer intentionally interacts and that collects PI from the consumer as part of the consumer's current interaction with the business under this title.
   b. A service provider to the business; or
   c. A contractor

36) **Unique identifier or Unique personal identifier** means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children under 18 years of age over which the parent or guardian has custody.

37) **Verifiable consumer request** means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business

can verify, using commercially reasonable methods, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected PI. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, to delete PI pursuant to Section 1798.105, or to correct inaccurate PI pursuant to Section 1798.106, if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

DEFINITIONS FOR DATA BREACHES

1. **Access** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

2. **Breach** means each individual instance of unlawful or unauthorized access to, use, or disclosure of a specific patient's medical information.
   a. Breach excludes:
      i. Any paper record, electronic mail, or facsimile transmission inadvertently accessed, used, or disclosed within the same health care facility or health care system where the information is not further accessed, used, or disclosed unless permitted or required by law.
      ii. Any internal paper record, electronic mail or facsimile transmission outside the same health care facility or health care system sent to a covered entity (as defined under Part 160.103 of Title 45 of the Code of Federal Regulations, as of June 27, 2014) that has been inadvertently misdirected within the course of coordinating care or delivering services.
      iii. A disclosure of medical information in which a health care facility or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such medical information.
      iv. Any access to, use, or disclosure of medical information permitted or required by state or federal law.
      v. Any lost or stolen encrypted electronic data containing a patient's medical information that is in any way created, kept, or maintained by a health care facility where the encrypted electronic data has not been accessed, used, or disclosed in an unlawful or unauthorized manner. Any lost or stolen electronic data containing a patient's medical information that is in any way created, kept, or maintained by a health care facility that is not encrypted shall be presumed a breach unless it is excluded by section 79901(b)(1)(F).
      vi. A disclosure for which a health care facility or BA, as applicable, determines that there is a low probability that medical information has been compromised based on a risk assessment of at least the following factors:

(1) The nature and extent of the medical information involved, including the types of identifiers and the likelihood of re-identification;
(2) The unauthorized person who used the medical information or to whom the disclosure was made;
(3) Whether the medical information was actually acquired or viewed; and
(4) The extent to which the risk of access to the medical information has been mitigated.

3. **Breach of the Security of the System** means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the person or business. Good faith acquisition of PI by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

4. **Detect** means the discovery of a breach, or the reasonable belief that a breach occurred by a health care facility or BA. The breach shall be treated as detected as of the first business day on which such breach is known to the health care facility or BA or by exercising reasonable diligence would have been known to the health care facility or BA. A health care facility or BA shall be deemed to have knowledge of a breach if such a breach is known, or by exercising reasonable diligence would have been known, to any person other than the person committing the breach, who is a workforce member or agent of the health care facility or BA.

5. **Encrypted** means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

6. **Individually identifiable** means medical information that includes or contains any element of **personal** identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

7. **Medical information** means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.

   California's Confidentiality of Medical Information Act (CMIA) defines "medical information" and "individually identifiable" the same as above and includes elements of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that alone or in combination with other publicly available information, reveals the individual's identity.

8. **Medical staff** shall have the same meaning as provided in section 70703(a)(1)
9. **Patient representative** shall have the same meaning as provided in Health and Safety Code section 123105(e).
10. **Personal information (PI)** means:
    An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
    (1) Social security number.
    (2) Driver's license number or California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
    (3) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
    (4) Medical information.
    (5) Health insurance information.
    (6) Information or data collected through the use or operation of an automated license plate recognition system.
    (7) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
        i. A user name or email address, in combination with a password or security question and answer that would permit access to an online account.
        ii. For purposes of this section, "PI" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
        iii. For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional (as distinguished from the definition of medical information above, which applies to potential breaches under Health and Safety Code Section 1280.15).
        iv. For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records (California Civ. Code s. 1798.82).
11. **Unauthorized** means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act or any other statute or regulation governing the lawful access, use, or disclosure of medical information.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** California Consumer Privacy Act of 2018 (CCPA) as Amended by the California Privacy Rights Act (CPRA) and Data Breaches
PAGE: 31 of 31	**REPLACES POLICY DATED:** 1/1/2020, 8/1/2020, 5/1/2021,10/1/2021
EFFECTIVE DATE: January 1, 2023	**REFERENCE NUMBER:** IP.DP.CA.001
APPROVED BY: Ethics and Compliance Policy Committee	

REFERENCES:

1. California Privacy Rights Act of 2020, Civil Code §§ 1798.100 – 1798.199
2. California Breach Model Policy
3. California Breach Notification Law, Civil Code §1798.82
4. California Civil Code § 1798.81.5
5. California Electronic Communications Privacy Act, Penal Code §§ 1546 – 1546.4
6. California Health and Safety Code § 1280.15
7. Company Code of Conduct
8. Protecting & Mitigating Inappropriate or Unauthorized Access, Use and-or Disclosure of Personally-Identifiable Info, IP.GEN.002
9. Information Security Common Terminology
10. Information Security Standards
11. Information Security Roles and Responsibilities Policy, IP.SEC.006
12. Information Security Risk Acceptance and Accountability Policy, IP.SEC.009
13. Records Management Policy, EC.014
14. California Civil Code s. 56.05
15. California Civ. Code s. 1798.82
16. California Health and Safety Code s. 1280.15
17. California Senate Bill 541 (2009)
18. California AB 211 (2009)
19. California AB 1710 (2014)
20. Protected Health Information Breach Risk Assessment and Notification, IP.PRI.011
21. California AB 1130
22. California AB 25
23. California AB 874
24. California AB 1355
25. California AB 1564
26. California's Confidentiality of Medical Information Act (CMIA)
27. California Department of Public Health Medical Information Breach –11-009, Chapter 13, Article 1, Sections 79900 - 79905 (7/1/2021)