Advanced Benefit Consulting

Full-Day HIPAA Privacy & Security Training Series 2026

Session 2 – California State Privacy Laws Course Name: California State Privacy, Security and Artificial Intelligence Laws Related to Human Resources & The Health Insurance Industry

Presented By: Dorothy Cociu, RHU, REBC, GBA, RPA

President, Advanced Benefit Consulting & Insurance Services, Inc.

Copyright, Advanced Benefit Consulting, June, 2026. All Rights Reserved.

A Friendly Reminder for All Attendees

- To respect speaker content and attendee privacy, please refrain from using AI notetakers , recording devices or transcription tools during this and all Advanced Benefit Consulting webinars, seminars, Lunch & Learns and other presentations.

This presentation is copyright protected.

Thank you for your cooperation.

Session 2 – California State Privacy Laws

RECERTIFICATION PROVIDER
HRCI 2025
HRCI.ORG

- This class is a separate class for HRCI credit and offers 1 hour of HRCI California Credit. Must be signed in and be in attendance for in-person class, or if webinar must answer all poll questions. On-demand must pass a test at the end of this class.



This program has been pre-approved for 1 Hour of HRCI California recertification credit hours toward aPHR®, aPHRi™, PHR®, PHRca®, SPHR®, GPHR®, PHRi™ and SPHRi™ recertification through HR Certification Institute® (HRCI®).

Advanced Benefit Consulting

First, a Brief Reminder/ Summary From Session 1 (3 hour training)

- In part 1, we covered in detail HIPAA Privacy & Security concepts and requirements, including:
  - Protected Health Information (PHI)
  - Treatment, Payment & Healthcare Operations (TPO)
- In General, the HIPAA Privacy Rule Requires the Average Provider or Plan/Covered Entity to:
  - Notify patients about privacy rights and how their information can be used
  - Adopt and implement privacy procedures for its practice, hospital, or plan
  - Train employees so that they understand the privacy procedures
  - Designate an individual to be responsible for implementation
  - Secure patient records containing individually identifiable health information
  - Administrative, physical and technical security
  - Additional levels of security now needed for paper and electronic health information

Advanced Benefit Consulting

HIPAA Privacy Rule – Concept of Minimum Necessary

- The HIPAA Privacy Rule states that you can only provide the Minimum Amount of Information Necessary to Get Today's Job Done

Advanced Benefit Consulting

Key Terms & Concepts

- Protected Health Information (PHI)
- Covered Entities
- Permitted Uses
- Business Associates
- TPO

Advanced Benefit Consulting

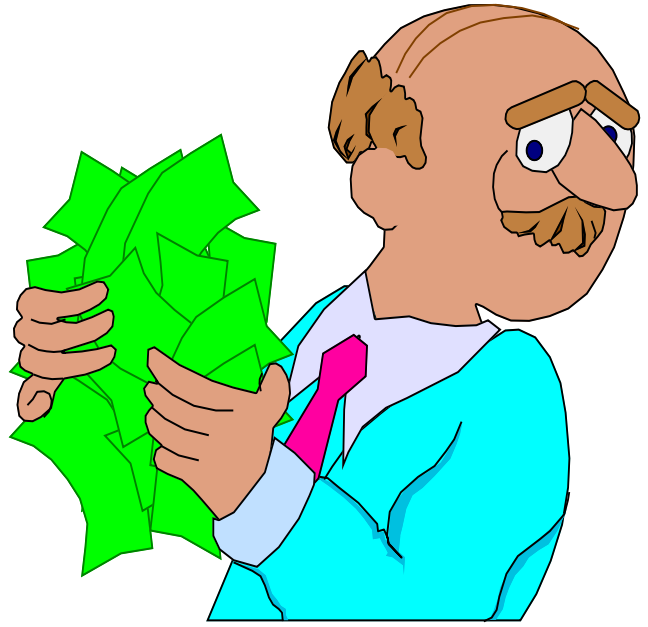
DOL Cybersecurity Guidance

- In part 1, we also discussed the DOL Cybersecurity Guidance, which deems plan fiduciaries responsible for cybersecurity, and requires them to have a formal process to select service providers (ie not owner's golf buddy), monitor their service providers, and more
- Released 3 sets of Guidance, in 2021 and updated 2014
  - Cybersecurity Program Best Practices"
  - "Tips for Hiring a Service Provider with Strong Cybersecurity Practices"
  - "Online Security Tips" (for participants)

Advanced Benefit Consulting

Covered Entity Handling of PHI

- *Think of handling PHI in terms of how you would protect a $100 bill in your possession*
- Each piece of PHI represents $100
  - Lock it up
  - Don't leave it lying around
  - Don't give it away
  - Make sure it's secure
  - Don't let anyone else have their hands on it unless they are authorized to!
  - Remember, it's a valuable piece of paper – as is all PHI you have in your possession!



In reality, the $100 is now $141!

Advanced Benefit Consulting

HIPAA Is Federal… Now Let’s Turn to California State Laws & Regulations

Advanced Benefit Consulting

State Law Obligations



- California laws more stringent than Federal HIPAA laws.
- **60 day vs 5 day breach notifications**
- Centers for Disease Control/communicable diseases (Confidentiality of Medical Information Act) state authority
- Specific State Laws (details to follow)
  - Social Security Law
  - Data Breach Law
  - Customer Records Law

California Privacy Laws



- California Dept. of Insurance Regulations
- Confidentiality of Medical Information Act
- Health & Safety Code/Health Care Service Plans
- Confidentiality of Social Security Numbers
- Insurance Information & Privacy Protection Act
- GLBA
- Customer Records

Confidentiality of Medical Information Act



- Confidentiality of Medical Information Act
  - In effect prior to HIPAA
  - Chapter 1 - Definitions
  - Applies to:
    - Providers of health care
    - Contractors (includes medical groups, IPA's, pharmacy benefits mgrs, medical svc organizations, but not health care service plans, providers, insurance institutions defined in the Insurance Information & Privacy Protection Act, and pharmaceutical benefits mgrs licensed under Knox-Keene Health Care Service Plan Act)
    - Health care service plans
    - Third Party Administrators
    - Pharmaceutical companies
    - (Cal. Civil Code 56-56.37)

Privacy Laws - Summary

- State Laws (California - Continued)
  - *The Confidentiality of Medical Information Act* (Cal. Civ. Code 56-56.37). Protects against the unauthorized disclosure of individually identifiable medical information. Applies to providers, health care service plans, employers, third party administrators, pharmaceutical benefits managers, and independent practice associations and related entities. Limited disclosure permitted where specifically cited. Disclosure may also be permitted if an authorization form is signed by patient. Obligates employers who receive medical information to "establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information." Agents who comply with the Ins. Info. & Priv. Act will not be deemed to have violated designated portions of this Act (Cal.Civ. Code 56.27). Amended in 2002 (eff. 1/03) to add provisions prohibiting pharmaceutical co's from disclosing medical information (AB 2191, chapter 853)

Confidentiality of Medical Information Act



- Chapter 2 – Disclosure of Medical Information by Providers, HMO's, or Contractors
- Providers, health care service plans, and contractors shall not disclose *medical information* regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining a written authorization, unless 1 of several conditions is met. The Act contains special provisions relating to outpatient psychotherapy treatment and records relating thereto.
- 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.
- *Requires HMO's to receive authorizations before providing customer service information/claims assistance to agents, employers or insureds*

Confidentiality of Medical Information Act

- Conditions which would permit the disclosure of medical information would include:
  - A provider, health care service plan, or contractor shall disclose medical information in response to an order, subpoena, or other request from a court, board, commission, administrative agency, arbitrator, law enforcement, or coroner
- A provider or health care service plan may disclose medical information in circumstances which include:
  - To providers, HCSP, contractors, or other health care professionals or facilities for purposes of diagnosis or treatment.
  - To an insurer, employer, HCSP, hospital service plan, benefit plan, gov’tal authority, contractor, or other responsible for paying health care services
  - To any person or entity providing billing, claims mgt, medical data processing or other admin svcs
  - To specified entities engaged in reviewing competence or qualifications of health care professionals
  - To private and public licensing and accreditation group, after removing identifiers

Confidentiality of Medical Information Act

- *Chapter 2.5: Disclosure of Genetic Test Results by a Health Care Service Plan*
  - *Sets forth the requirements for written authorization*
- *Chapter 3: Use and Disclosure of Medical Information by Employers*
  - Each employer who receives medical information shall establish appropriate procedures to ensure confidentiality and protection from unauthorized use and disclosure of that information. Procedures may include, but are not limited to, instruction regarding confidentiality of employees and agents handling files containing medical information, and security systems restricting access to files containing medical information
  - No employee shall be discriminated against in the terms or conditions of employment for refusing to sign an authorization for disclosure of medical information
  - No employer shall use, disclose, or knowingly permit its employees or agents to use or disclose medical information which the employer possess pertaining to its employees without a signed authorization from the patient

Confidentiality of Medical Information Act

- *Chapter 4: Relationship of Chapters 2 and 3*
- *Chapter 5: Use and Disclosure of Medical and Other Information by Third Party Administrators and Others*
- *Chapter 6: Relationship to Existing Law*
- *Chapter 7: Violations*

New California Law Summary for 2023-2024



- **S.B. 793: Insurance: Privacy Notices and Personal Information (Chapter 184)**
- California Governor signed S.B. 793, which *eases the notice requirements on insurance institutions and agents.* First, S.B. 793 codifies the GLBA annual notice regulation (adding new section 791.045 to the Insurance Code); the new code section also describes what must be included in the notice. Second, under the terms of the new law, *insurance institutions and agents no longer have to send out their privacy notice every year, if certain conditions are met.* **This latter change was made to reflect amendments Congress made to GLBA, and because there is a concern that if notices are sent too frequently, they are ignored.**
- What are the conditions that must be met? **After the initial privacy notice goes out, an annual notice does not have to be sent by the insurance institution or agent if (a) the privacy policy has not changed; (b) the privacy policy is easily accessible on their website; and (c) medical record, personal, or privileged information is not shared with nonaffiliated third parties.**
- The statute also specifies that the notice does not have to be provided to a former customer with whom the institution or agent no longer has a continuing relationship.

New California Law Summary 2023-2024



- **AB 254, Bauer-Kahan. Confidentiality of Medical Information Act: Reproductive or Sexual Health Application Information (Chapter 254)**
- The Confidentiality of Medical Information Act (CMIA) **prohibits a provider of health care, a health care service plan, a contractor, or a corporation and its subsidiaries and affiliates from intentionally sharing, selling, using for marketing, or otherwise using any medical information, as defined, for any purpose not necessary to provide health care services to a patient, except as provided. The CMIA makes a business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage the individual's information or for the diagnosis, treatment, or management of a medical condition of the individual, a provider of health care subject to the requirements of the CMIA.** ***Existing law makes a violation of these provisions that results in economic loss or personal injury to a patient punishable as a misdemeanor.***
- **This bill would revise the definition of "medical information" to include reproductive or sexual health application information, which the bill would define to mean information about a consumer's reproductive or sexual health collected by a reproductive or sexual health digital service, as specified.** The bill would make a business that offers a reproductive or sexual health digital service to a consumer (such as a period tracker or pregnancy app) for the purpose of allowing the individual to manage the individual's information, or for the diagnosis, treatment, or management of a medical condition of the individual, a provider of health care subject to the requirements of the CMIA.

Advanced Benefit Consulting

New California Law Summary 2023-2024



- AB 254 Continued…
- “Medical information” is now defined as follows: “’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 health application information, reproductive or sexual health application information, mental or physical condition, or treatment. ‘Individually identifiable’ means that the medical information 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 identity of the individual.”

- This bill would incorporate additional changes to Section 56.05 of the Civil Code proposed by AB 1697 to be operative only if this bill and AB 1697 are enacted and this bill is enacted last.

Advanced Benefit Consulting

New California Laws for 2023-2024

- **AB 1697, Schiavo. Uniform Electronic Transactions Act (Chapter 374)**
- Existing law, the Uniform Electronic Transactions Act, provides that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form. *The act exempts from its provisions, among other things, specific transactions, including an authorization for the release of medical information by a provider of health care, health care service plan, pharmaceutical company, or contractor and an authorization for the release of genetic test results by a health care service plan under the Confidentiality of Medical Information Act.*
- ***This bill would delete the exemption for the above-described authorizations under the Confidentiality of Medical Information Act and would make conforming changes.***
- Existing law requires that the authorization for release of medical information contain a specific end date.
- ***This bill would, instead, require that the authorization contain an expiration date or event, as defined, and would limit the duration of the authorization to one year or less, except as provided. The bill would also require that the person to whom the medical information pertains receives a copy of the authorization for that authorization to be valid.***

Advanced Benefit Consulting

Health and Safety Code/Health Care Service Plans



- Restrictions on disclosures to employers (Health Safety Code § 1374.8)
- Obligation to protect patient/enrollee medical information in compliance with Confidentiality of Medical Information Act (Health & Safety Code § 1364.5)

Confidentiality of Social Security Numbers



- Applies to any person or entity (not including a state or local agency), which includes health care service plans, insurers, pharmacy benefits managers, contractors, or those providing “administrative or other services relative to health care or insurance products or services, including third-party administration or administrative services only”
- SB 168, Cal. Civil Code 1798.85, SB 1730 (now chaptered at 786), amends 1798.85
- Catch Me if You Can – Roger Abignale

CA Social Security Law

- The law, which took effect beginning July 1, 2002 and was fully effective by July 1, 2005, applies to individuals and non-governmental entities. Companies may not do the following:
  - Publicly display or post SS#'s
  - Print SS#'s on ID cards or badges
  - Require people to transmit a SS# over the internet unless the connection is secure or the number is encrypted
  - Require people to log onto a website using a SS# w/o a password
  - Print SS#'s on anything mailed to a customer unless required by law or the document is a form or application

Frank Abagnale



Photographer: Chris Ratclife / Bloomberg 3/11/2015

"The technology works but we're always dealing with that **weakest link, the human beings.**"

March 11, 2015, London, U.K.

Advanced Benefit Consulting

Abagnale Interview on Technology Aiding Fraud

- The man who made $2.5 million in the 1960's as a teenager faking identities as an airline pilot, lawyer and doctor now works with the FBI and others on cybercrime. He even had a role in the investigation into the 2014 JPMorgan Chase & Co. hack…
- He's spent the past 4 decades working with the FBI spotting fraud, and says the advances in technology and the over-sharing trends propagated by social media sites like Facebook have made it much easier to create false identities with a few personal details. When he did it, he had to assume an entirely new identity and life.
- "What I did 50 years ago as a teenage boy is 4,000 times easier to do today because of technology," Abagnale said. "Technology breeds crime. It always has, and always will…."

"Catch Me If You Can" Con Man Says Technology Aids Fraud", BloombergBusiness, Suzi Ring, March 12, 2015

Advanced Benefit Consulting

Abagnale Interview on Technology Aiding Fraud

- "You need to teach your employees that whether you're the receptionist on the phone or you're the officer of the company," everyone's a target for a hacker.
- While security is tighter now, a new challenge is that often no human contact is needed to defraud someone…. It can all be done by computer from the other side of the planet.

"Catch Me If You Can" Con Man Says Technology Aids Fraud", Bloomberg Business, Suzi Ring, March 12, 2015

Advanced Benefit Consulting

Insurance Information and Privacy Protection Act

- Applies to:
  - Insurance institutions
  - Agents (including registered TPAs), and
  - Insurance-support organizations

  which, in the case of life or disability insurance:
  - Collect, receive, or maintain information in connection with *insurance transactions* which pertains to natural persons who are residents of California, or
  - Engage in insurance transactions with applicants, individuals, or policyholders who are residents of California.
  - Cal. Ins. Code 791-791.27

Insurance Information and Privacy Protection Act

- An insurance institution, agent, or insurance-support organization shall not disclose any personal information or privileged information about an individual collected or received in connection with an insurance transaction without a written authorization unless one of 22 conditions is met. A specific section addresses restrictions on disclosures by insurance entities to employers. Those subject to this Act are exempt from the Confidentiality of Medical Information Act.

Gramm-Leach-Bliley Financial Services Modernization Act ("GLBA")



- Financial Records Privacy Law affecting banks, financial institutions and insurance companies/licensed agents
  - Federal GLBA and Cal-GLBA
  - Notices required from banks, financial institutions, insurance companies, agents, other

Data Breach Notification Law (Original law 7-1-03)



- Data Breach Notification Law (7-1-03)
  - Must provide notice “to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person)

New California Data Breach Law Effective January 1, 2026

- ***S.B. 446 – Data Breach Notifications***: California has, for many years, its own data breach law. (Most other states also have their own data breach law.) S.B. 446 modifies existing state law to require that **data breach disclosures be made generally within 30 calendar days of discovery or notification of the data breach (with some exceptions)**. In addition, under existing law, disclosures also have to be made to the Attorney General in some instances.
- **S.B. 446 requires that mandatory submissions to the Attorney General be made within 15 calendar days of notifying affected consumers of the security breach.**

Advanced Benefit Consulting

Customer Records



- Destruction of customer records (Civil Code § 1798.81)
- Unauthorized acquisition of unencrypted personal information from a computer system (Civil Code § 1798.82)
- Written very broadly
- Applies to businesses with customer records containing personal information
  - Destruction, Security, Data Breach, Direct Marketing
- *ARRA/HITECH's security requirements are in sync with this!*

California Consumer Privacy Act (CCPA)

Effective January 1, 2020

(other effective dates also apply for certain provisions

Advanced Benefit Consulting

California Privacy Law Effective January, 2020

- The California Consumer Privacy Act (CCPA)
- Signed into law June, 2018
- Effective for the most part Jan. 1, 2020
- Extends the protections and rights for California residents (defined later)
- Applies to non-profit businesses that both collect and process the Personal Information of CA residents and do business in the state of CA

Advanced Benefit Consulting

California Consumer Protection Act (2020)

- Who has rights under the CCPA?
  - California residents, defined as any natural person “enjoying the benefit and protection of laws and government” of CA who is in California “for other than a temporary or transitory purpose” of “domiciled” in CA but “outside the State for a temporary or transitory purpose.”

Businesses Subject to CCPA

- *For-profit* entities that both collect and process the Personal Information of CA residents and do business in the State of CA.
- Physical presence in CA is not a requirement; making sales in the state would be sufficient
- **Must meet at least one of the following criteria for CCPA to apply:**
  - Must generate annual gross revenue in excess of $25 million
  - Business must receive or share personal information of more than 50,000 California residents annually, or
  - The business must derive at least 50% of its annual revenue by selling the personal information of CA residents

Types of Businesses Subject to CCPA

- Threatens established business models throughout the digital sector
- Companies that generate revenue from targeted advertising over internet platforms, such as Facebook, Twitter, Google, will be the most impacted
- Could also extend to internet service providers such as AT&T, Verizon, which collect broadband activity data (web browsing data) and could attempt to use it to generate behavioral profiles to enable digital advertising

Types of Firms Who Stand To Lose Even More

- Data brokers such as Acxiom, Epsilon, Experian, and Oracle, for example, generate profits by collecting quantities of data on individual consumers and selling it to third parties
  - Ad networks, marketers, retailers, or any other type of interested businesses

What is Personal Information Under CCPA?

- Broad definition: “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”
- **Includes: SSNs, drivers’ license numbers, and purchase histories, as well as “unique personal identifiers,” such as device identifiers or other online tracking technologies**
- Excludes: Information that is publicly available, aggregated or de-identified data, as well as medical or health information collected by a person or entity governed by the Confidentiality of Medical Information Act or HIPAA.

New Rights Given to Consumers by CCPA

- CCPA provides consumers with more control over their personal information in 4 ways:
  - Knowledge (must notify what is being collected)
  - Sale of personal information (consumers must be presented with a simple process to opt-out of having personal information sold to a third party; businesses must post a DO NOT SELL MY PERSONAL INFORMATION link on its homepage for opting out)

CCPA provides consumers with more control over their personal information in 4 ways *(cont):*

- Personal information removal (consumers may request that a business delete their personal information, and businesses must inform consumers they have this right; PI must also be deleted from third-party contractors)
- Service equality (business cannot discriminate against a consumer who exercises his or her rights under CCPA; CCPA prevents a business from charging a consumer a fee because he or she exercised a right under the CCPA; Businesses can offer consumers financial incentives to allow personal information collected)

Disclosure Responsibilities of CCPA

- Must proactively explain privacy notices when personal information is collected
- Must inform consumers of their rights under CCPA, categories of personal information collected, the ways that personal information is used, and the categories of personal information the business has sold to third parties in the last year.
- Disclosures must be updated every 12 months

Private Right of Action



- CCPA provides consumers a private right of action if their personal information "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices
- Consumers can file individual or class action lawsuits, and can recover between $100 and $750 in statutory damages per incident, or actual damages
- Allows consumers to seek injunctive and other forms of relief, and sets out different procedures for actions seeking actual versus statutory damages

Penalties for Non-Compliance



- Civil penalties of up to $2500 per violation and $7500 per intentional violation
- Once notified of a violation by the Attorney General, companies have 30 days to come into compliance in order to avoid penalties (data breach occurrence unclear)

Preparation

- Privacy notices, P&Ps, websites updated before the effective date
- Businesses must map the personal information it collections and locations where personal information is stored so it can promptly meet requests under CCPA

Updates on CCPA from 2023-2024 – Steps to Comply (Fisher-Phillips Law Firm 5-23)

- **1. Inventory and map all consumer data, including employee and job applicant data.**
- Understand pertinent defined terms such as what is "personal information" and "sensitive personal information," who is a California "consumer" (including employees and job applicants), and what constitutes "collection" under the regulations to frame the scope of any data inventory or mapping exercise.
- **2. Take appropriate steps to secure all consumer and employment-related data.**
- In support of the obligation to secure consumer data, you may be required to conduct an annual security assessment depending on risk factors and sensitivity of the data you collect or maintain.
- **3. Prepare and provide a "notice at collection" to all consumers (including employees and job applicants) at or before collecting any consumer data.**
- Review the content requirements for the Notice at Collection and update for compliance with the CCPA regulations effective March 29, 2023.

Advanced Benefit Consulting

Updates on CCPA from 2023-2024 – Steps to Comply (Fisher-Phillips Law Firm 5-23)

- 4. **Prepare and post a comprehensive privacy policy on your website.**
- Make sure it includes more than just the Notice at Collection, providing employees with a privacy policy pertaining to all employment-related data explaining how they can exercise their CCPA rights. Ensure the privacy policy includes all required content under by the CCPA, including, but not limited to, whether any data is sold (which includes any sharing of data with a third party that is not a "service provider" in exchange for valuable consideration).
- 5. **Deploy a process to receive and respond to consumer requests from all consumers (a process referred to by many privacy practitioners as DSR or data subject request, although the term is not used in the CCPA).**
- Implement a consumer request process that can address all the types of requests a consumer can make under the CCPA, including, but not limited to, the right to know, request to delete, request to correct and the request to opt out of the sale of personal information. Since January 1, 2023, consumers can submit a request to correct information and request to limit the use or disclosure of sensitive personal information.

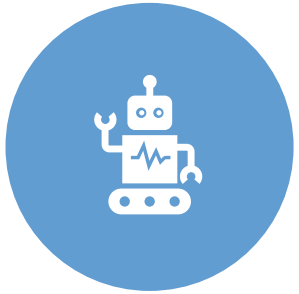
Advanced Benefit Consulting

Updates on CCPA from 2023-2024 – Steps to Comply (Fisher-Phillips Law Firm 5-23)

- **6. Implement data minimization rules.**
- This includes a data retention policy and workflow for purging stale data for which there is no legal or business reason to keep.
- **7. Train all managers and employees on all CCPA requirements in which they play any role.**
- This may include those responsible for CCPA compliance and anyone directly interacting with consumers and providing information, notices, and forms, or assisting with the business's response to any CCPA request.

Advanced Benefit Consulting

CCPA Final Regulations – July, 2025



Mandatory compliance requirements around automated decision-making technology (ADMT)



Comprehensive risk assessments & audits



Required cybersecurity audits



Created the California Privacy Rights Act (CPRA)

Advanced Benefit Consulting

California Privacy Rights Act (CPRA)
(created from final regs of CCPA)

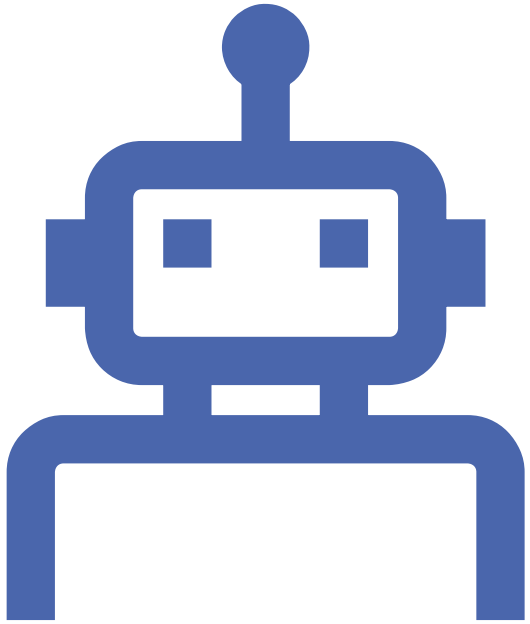
- Right to correction
- Right to limit collection of sensitive personal information (SPI)
- Right to access and opt-out of automated decision-making tools (ADMT)
- Right to data portability
- Penalties and Why Businesses Should comply

Advanced Benefit Consulting

Penalties - CPRA

- **Civil Penalties**
  - **Unintentional violations:** Up to $2,663 per violation.
  - **Intentional violations:** Up to $7,988 per violation.
  - **Violations against minors:** Up to $7,988 per violation for infringing upon the privacy of consumers under 16 years of age.
- **Private Right of Action (Data Breaches)**
- Consumers can sue businesses directly if their non-encrypted personal information is exposed due to a failure to implement reasonable security procedures.
- **Statutory Damages:** $100 to $750 per consumer, per incident, or actual damages, whichever is greater.
- **Additional Consequences**
  - **Loss of the "Cure Period":** Unlike older regulations, under the CPRA, businesses no longer automatically receive a 30-day grace period to fix technical non-compliance before facing formal administrative enforcement.

Advanced Benefit Consulting



Use of AI in Healthcare & Benefits

- As covered heavily in our May AI in HR & Benefits Webinar, AI is used frequently (and growing every day) in Human Resources, Benefits and Health Care Providers
- Individual v Enterprise AI Use
- Where are Your Risks?
- How many of your staff are using unapproved AI tools?
    - Risk extremely high for companies needing to protect PHI, PII, or anyone wanting to protect Intellectual Property
    - Tools like ChatGPT, Co-Pilot, Gemini, Claude, etc. Helpful but extremely risky if safeguards aren't implemented BEFORE USE

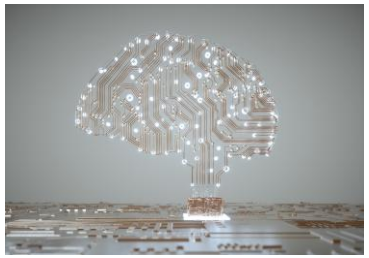
Advanced Benefit Consulting

California New AI Laws



- ***CRD Regulations: Automated-Decision Systems***: A new set of regulations—From the Civil Rights Department (CRD)—went into effect on **October 1, 2025**.
- **Common Use of AI with Automated-Decision Systems – Human Resources-Screening Applicants**
- These new regulations—the "Employment Regulations Regarding Automated-Decision Systems"—address growing concerns over the use of artificial intelligence (AI) in the workplace. CDR explains that, "**Automated-decision systems — which may rely on algorithms or artificial intelligence — are increasingly used in employment settings to facilitate a wide range of decisions related to job applicants or employees, including with respect to recruitment, hiring, and promotion.**" For example, the systems may be used to ***screen applicant resumes***. The regulations are intended to *protect against prohibited discriminatory practices* when these systems are used.

Advanced Benefit Consulting



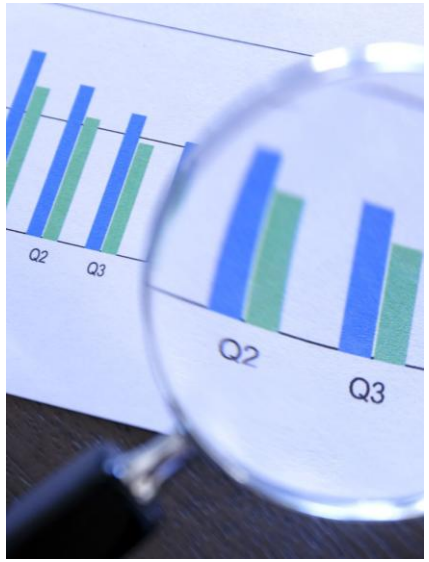
CRD Regulations: Automated-Decision Systems, Continued

- The regulations “clarify the application of existing antidiscrimination laws in the workplace in the context of new and emerging technologies, like artificial intelligence.” The Department states that the regulations aim to:
  - Make it clear that the use of an automated-decision system may violate California law if it harms applicants or employees based on protected characteristics, such as gender, race, or disability.
  - Ensure employers and covered entities maintain employment records, including automated-decision data, for a minimum of four years.
  - Affirm that automated-decision system assessments, including tests, questions, or puzzle games that elicit information about a disability, may constitute an unlawful medical inquiry.
  - Add definitions for key terms used in the regulations, such as “automated-decision system,” “agent,” and “proxy.”

S.B. 53 – Large Developers: The Transparency in Frontier Artificial Intelligence Act (TFAIA)



- Existing law generally regulates artificial intelligence, including by requiring, on or before January 1, 2026, and before each time thereafter, that a generative artificial intelligence system or service, or a substantial modification to a generative artificial intelligence system or service, released on or after January 1, 2022, is made publicly available to Californians for use, the developer of the system or service to post on the developer's internet website documentation regarding the data used by the developer to train the generative artificial intelligence system or service, as prescribed.
- Enacts the Transparency in Frontier Artificial Intelligence Act (TFAIA) that would, among other things related to ensuring the safety of a foundation model, require a large frontier developer to write, implement, and clearly and conspicuously publish on its internet website a frontier AI framework that applies to the large frontier developer's frontier models and describes how the large frontier developer approaches, among other things, incorporating national standards, international standards, and industry-consensus best practices into its frontier AI framework.
- Will also require a large frontier developer to transmit to the Office of Emergency Services a summary of any assessment of catastrophic risk, as defined, resulting from internal use of its frontier models, as specified.
- The TFAIA would require the Office of Emergency Services to establish a mechanism to be used by a frontier developer or a member of the public to report a critical safety incident, as defined, and would also require the Office of Emergency Services to establish a mechanism to be used by a large frontier developer to confidentially submit summaries of any assessments of the potential for catastrophic risk resulting from internal use of its frontier models, as prescribed.



TFAIA, Continued

- The TFAIA would exempt from the California Public Records Act a report of a critical safety incident submitted to the Office of Emergency Services, a report of assessments of catastrophic risk from internet use, and a covered employee report made pursuant to the whistleblower protections described below.
- The TFAIA would impose a civil penalty for noncompliance with the TFAIA to be enforced by the Attorney General, as prescribed.
- Will establish within the Government Operations Agency a consortium required to develop a framework for the creation of a public cloud computing cluster to be known as "CalCompute" that advances the development and deployment of artificial intelligence that is safe, ethical, equitable, and sustainable by, among other things, fostering research and innovation that benefits the public, as prescribed. The bill would require the Government Operations Agency to, on or before **January 1, 2027**, submit a report from the consortium to the Legislature with that framework and would dissolve the consortium upon submission of that report. The bill would make those provisions operative only upon an appropriation in a budget act, or other measure, for its purposes.
- This bill would, among other things related to protecting whistleblowers working with foundation models, prohibit a frontier developer from making, adopting, enforcing, or entering into a rule, regulation, policy, or contract that prevents a covered employee, as defined, from disclosing, or retaliates against a covered employee for disclosing, information to the Attorney General, a federal authority, a person with authority over the covered employee, or another covered employee who has authority to investigate, discover, or correct the reported issue, if the covered employee has reasonable cause to believe that the information discloses that the frontier developer's activities pose a specific and substantial danger to the public health or safety resulting from a catastrophic risk or that the frontier developer has violated the TFAIA.

The Evolution of Modern AI from Chatbot to Human Resources Assistant & Privacy Team Helper – it is more than just a tool; it's a digital worker

- What is AI and why does knowing the difference matter?
- Why use AI?
- Human Resources risks and opportunities AI adoption brings to the modern workplace, including bias
- Benefits risks and opportunities AI adoption brings to the health insurance and benefits space
- On-boarding, managing and off-boarding Artificial Intelligence members of your IT/Human Resources/Benefits team
- On-boarding, managing and off-boarding Artificial Intelligence members of your marketing staff, accounting/finance staff
- The importance of AI Governance in Privacy & Security Policies

Advanced Benefit Consulting

Onboarding, Managing, and Offboarding AI as a Member of the Team

- **AI Onboarding Essentials**
- Define the AI agent's role, authority limits, and data access with clear human accountability assigned.

- **Continuous AI Management**
- Monitor AI performance, compliance, and decision accuracy regularly with human-in-the-loop checkpoints.

- **Secure AI Offboarding**
- Revoke access and credentials, review logs to prevent unauthorized AI activity after retirement.



Advanced Benefit Consulting

What Is AI Governance?



> *"AI governance is the set of policies, processes, roles, and controls an organization uses to ensure that AI systems are developed, acquired, deployed, and retired in a way that is lawful, ethical, secure, and aligned with the organization's mission and risk tolerance."*

A working definition — not a legal one. It encompasses every stage of an AI system's existence, from the decision to acquire or build through to decommissioning. Governance is the connective tissue between AI ambition and organizational accountability.

Advanced Benefit Consulting

Monday Morning Task: Define How You Are Using AI & How You're Going to Do it Safely

- Best Practices:
  - Create an AI Use Committee; include HR, IT, C-Suite Reps, Trainers
  - AI Governance Determination
  - Write Down the Types of Policies you Need
  - Assign your team members duties; who is responsible for what
  - Develop IT strategies
  - Develop Written Policies which limit use and types of AI
  - AI Use Only with Company-approved AI Tools
  - Develop Ongoing Training



Advanced Benefit Consulting

Contact Us



- Advanced Benefit Consulting
- P.O. Box 6677, Fullerton, CA 92834
- dmcociu@advancedbenefitconsulting.com
- (714) 693-9754 x 102
- (866) 658-3835

Notice of Copyright

This presentation is copyright protected by Advanced Benefit Consulting & Insurance Services, Inc. Used with permission only. Copyright, 2026. All rights reserved.

Advanced Benefit Consulting & Insurance Services, Inc.

ORANGE COUNTY (brokerage and consulting)

P.O. Box 6677, Fullerton, CA 92834-6677

(866) 658-3835

Dorothy Cociu: dmcociu@advancedbenefitconsulting.com

714 693-9754 x 102

Privacy training available nationwide!

Legal Disclaimer

- The information herein should not be construed as legal or tax advice in any way. Regulations, guidance and legal opinions continue to change with this any new law. Dorothy Cociu of Advanced Benefit Consulting & Insurance Services, Inc. has gathered public information and has attempted to present it in an easily readable and understandable format. Situations vary. Technical corrections and future opinions may vary from what is presented in this presentation. This is meant for informational content only. Neither the presenters, Advanced Benefit Consulting, or its company affiliations or sources referred to make any warranty of any kind concerning this information. You should seek the advice of your attorney or tax advisor for additional or specific information.

Advanced Benefit Consulting