Healthcare AI 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers

USA – California: Trends & Developments
Lowell Brown and Douglas Grimm
ArentFox Schiff LLP

USA – CALIFORNIA

Trends and Developments

Contributed by:
Lowell Brown and Douglas Grimm
ArentFox Schiff LLP

ArentFox Schiff LLP is a law firm with one of the most highly respected healthcare practices in California and nationwide. The California team is based in ArentFox Schiff's Los Angeles office and works closely with its Chambers-ranked healthcare practice in Washington, D.C., and its healthcare teams in New York, Boston, and Chicago, forming a leading 80+ lawyer national group. The firm is a full-service practice advising many of California's major hospital systems and other health care clients on a full spectrum of matters, including regulatory matters, administrative and commercial litigation, transactions, medical peer review, and (government) investigations. ArentFox Schiff's California practice is best known for its medical staff and peer review practice, which includes both counselling and litigation. The team offers a wide range of services in the healthcare AI area, including regulatory compliance, AI-related contracts and licensing, privacy and data security, risk management, intellectual property, and dispute resolution and litigation.

Authors

Lowell Brown is a pre-eminent California medical staff lawyer at ArentFox Schiff LLP, with a Chambers Band 1 rating. His extensive experience in counselling healthcare providers includes practitioner credentialing, peer review, disciplinary hearings, and regulatory matters. Lowell has served as legal counsel in a number of landmark California Supreme Court and Court of Appeals decisions involving peer review issues. Lowell also has nearly 40 years of experience helping providers achieve success in a wide range of business, regulatory, and medico-legal matters. He is a member of the California Association Medical Staff Services and previously served as president of the California Society for Healthcare Attorneys.
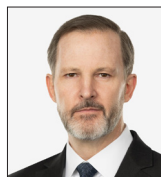
Douglas Grimm is a lawyer who heads ArentFox Schiff's national healthcare practice. A former chief executive officer of multiple acute-care hospitals throughout the USA, Douglas counsels hospitals and health systems, physician groups, pharmaceutical companies, and speciality providers on regulatory, transactional, and government enforcement challenges. A frequent author and lecturer on current issues facing health care providers, including AI, fraud and abuse enforcement trends, and telehealth, Douglas is a fellow of the American College of Healthcare Executives, a member of the Healthcare Financial Management Association and Health Care Compliance Association, and an advisory board member for the Center for Telehealth and e-Health Law.

ArentFox Schiff

555 South Flower St
43rd Floor
Los Angeles
CA 90071
USA

Tel: +1 213 629 7400
Web: afslaw.com

California State-Specific Legislation on Healthcare AI

California has established itself as a leader in the governance of artificial intelligence (AI), particularly within the healthcare industry. The state has enacted several laws that specifically address the use of AI in healthcare, often exceeding federal requirements with California-specific patient protections. The following sections outline the state's principal new AI laws, which have wide-ranging implications for healthcare providers, AI developers, and related stakeholders, including: notice to patients, physician autonomy, accountability for the emerging technology's use in patient care, consumer privacy and access to medical information, professional liability, and even the corporate practice of medicine.

California Health and Safety Code Provisions on Digital Health and AI

Assembly Bill 3030 (2024) – AI in Healthcare Act

Effective 1 January 2025, AB 3030 introduced requirements for healthcare entities utilising generative AI in patient communications related to clinical information, as outlined below.

- A prominent disclaimer must indicate that generative AI produced the communication, with specific display rules depending on the format:
  - (a) for written communications, the disclaimer must appear at the beginning of each message;
  - (b) for written communications involving continuous online interactions (eg, chat-based telehealth), the disclaimer must be displayed throughout the interaction;
  - (c) for audio communications, the disclaimer must be provided verbally at both the start and end of the interaction; and
  - (d) for video communications, the disclaimer must be displayed throughout the interaction.
- Clear instructions must be provided detailing how a patient can contact a human healthcare provider, an employee of the health facility, clinic, physician's office, or group practice, or other appropriate personnel.

An exemption applies if a communication generated by generative AI is subsequently read and reviewed by a human licensed or certified healthcare provider, who must document the review and any modifications made.

Senate Bill 1120 (2024) – Physicians Make Decisions Act

Effective 1 January 2025, SB 1120 addressed the use of AI in health insurance utilisation review and management functions. Unsurprisingly, the statute pays careful attention to physician autonomy, a concern for which California is well-known.

- Healthcare service plans and disability insurers are prohibited from denying, delaying, or modifying healthcare services based solely on artificial intelligence algorithms.
- Any denial, delay, or modification of care based on medical necessity must be reviewed and decided by a licensed physician or qualified healthcare provider with expertise in the specific clinical issues.
- AI tools used in utilisation review must base decisions on the enrollee's medical or clinical history, individual clinical circumstances, and other relevant clinical information, rather than solely on group datasets.
- The AI tool, including its algorithm, must be open to inspection for audit or compliance reviews.
- Periodic review and assessment of the AI tool's performance, use, and outcomes are required to maximise accuracy and reliability.
- Strict deadlines for authorisation decisions are imposed: five business days for standard cases, 72 hours for urgent cases, and 30 days for retrospective reviews.

Assembly Bill 2885 (2024) – Algorithmic Accountability Act

Effective 1 January 2025, AB 2885 seeks coherence in California AI law by standardising the definition of "artificial intelligence" across the state's legal framework and introducing certain governance requirements that you can find below.

- The Department of Technology must conduct an annual inventory of all "high-risk automated decision systems" proposed or used by state agencies. These systems are classified as high-risk if they have the potential to significantly influence indi-

viduals or groups through decisions affecting their rights, access to services, or legal status.

- The inventory must include descriptions of the AI systems, their intended applications, and the data used in their training or functioning.
- The law addresses concerns over AI-generated manipulative content, such as deepfakes, and aims to establish mechanisms to detect and mitigate the use of AI-generated deceptive content within state operations.
- State agencies must conduct audits of bias and fairness, evaluate their AI systems, and ensure transparent AI usage.
- Individuals are empowered with the right to know how AI tools impact them and the ability to dispute AI system decision-making.

California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) Amendments Relating to Health Data

The CCPA, as amended by the CPRA, provides augmented privacy protections for California residents. The CPRA introduced the concept of "sensitive personal information," which includes health data and "neural data" (information generated by measuring the activity of a consumer's central or peripheral nervous system). These protections apply to businesses that meet specific thresholds as defined in the law.

Key consumer rights under CCPA/CPRA relevant to healthcare AI include the following.

- Right to know – consumers have the right to know what personal information a business collects about them, how it is used, and with whom it is shared.
- Right to delete – consumers can request the deletion of personal information collected from them, with some exceptions.
- Right to opt-out – consumers have the right to opt out of the sale or sharing of their personal information, including for targeted advertising.
- Right to correct – consumers can request that businesses correct inaccurate personal information about them.
- Right to limit use and disclosure of sensitive personal information – consumers can direct businesses to limit the use and disclosure of sensitive

personal information (including health data) for specific purposes, such as providing requested services.

The California Attorney General's office has emphasised that AI applications must adhere to these privacy laws, warning that non-compliance may result in penalties under the Unfair Competition Law.

California Medical Information Act (CMIA)

The venerable Confidentiality of Medical Information Act (CMIA) might be considered a "pre-HIPAA" state statute. It regulates the use and disclosure of individually identifiable medical information by licensed healthcare professionals, providers, and their contractors. The CMIA generally prohibits the disclosure of medical information without patient authorisation, with specific exceptions. Violations can result in both civil and criminal penalties, including fines of up to USD250,000 per violation.

Not surprisingly, given the law's premise and the CMIA's mandates, the California Attorney General has emphasised that AI systems comply with its requirements for safeguarding and securely using patient data. The California Attorney General's office has stated that AI systems handling patient data must adhere to the CMIA, emphasising the need to limit access and improper use of sensitive information, including data used to train AI models.

Interplay Between California Laws

California's legislative approach often builds upon or supplements other frameworks, frequently imposing more stringent requirements. This deeply layered regulatory environment necessitates a careful and comprehensive compliance strategy for stakeholders.

- The CMIA's broader scope can apply to entities not explicitly covered by other privacy laws (eg, some digital health companies or mobile applications that store medical information).
- Recent legislation introduces state-specific requirements for transparency in AI-generated patient communications, regardless of other regulatory classifications.
- The "Physicians Make Decisions Act" (SB 1120) directly regulates the use of AI in health insurance

utilisation management to ensure human oversight in coverage decisions.

- The California Attorney General's legal advisories on AI in healthcare also serve to interpret how existing state laws, including consumer protection and anti-discrimination statutes, apply to AI systems, reinforcing compliance expectations beyond other mandates.

Liability and Malpractice Considerations for AI-Assisted Diagnosis and Treatment

The integration of artificial intelligence into clinical practice introduces complex liability and medical malpractice considerations that must be carefully managed. Traditional legal doctrines, designed for human-centric medical care, are being re-evaluated in the context of AI-assisted diagnosis and treatment, requiring healthcare providers to implement specific risk management protocols. Consider the standard of care, for example.

Standard of Care in an AI-Augmented Environment

Medical malpractice claims traditionally hinge on the "standard of care," defined as the level of skill and judgment that a reasonably competent physician would exercise under similar circumstances.

As AI tools become more prevalent and accurate, the standard of care itself may evolve. While litigators may argue that a physician was negligent for under-utilising advanced AI tools that could have improved diagnostic accuracy or treatment outcomes, physicians should document their clinical reasoning when choosing not to rely on AI recommendations to demonstrate appropriate medical judgment.

Conversely, if a physician relies on a faulty AI recommendation that leads to patient harm, questions arise about whether the reliance itself was negligent or if the liability extends to the AI developer. Healthcare providers must establish clear protocols for documenting their review and validation of AI recommendations to demonstrate appropriate clinical judgment.

The Medical Board of California emphasises that AI tools are generally not capable of replacing a physician's professional judgment, ethical responsibilities,

or accountability, reinforcing that human oversight remains paramount.

The legal system currently lacks extensive precedent for AI-assisted malpractice. The question of whether AI falls under traditional product liability laws (which typically apply to medical devices) or medical malpractice doctrines remains an open issue for courts.

Corporate Practice of Medicine and AI

California's famously stringent prohibition on the corporate practice of medicine (CPOM) is particularly relevant to AI in healthcare. This doctrine generally prohibits lay persons or entities from providing or engaging in clinical healthcare practices, ensuring that licensed professionals make medical decisions unhindered by fiscal or administrative management.

Now that AI has been grafted onto that ambitious regulatory scheme, the California Attorney General's office has, of course, stated that AI cannot replace or override healthcare providers' decisions and using AI to make decisions about patient treatment or to override medical needs may violate this ban.

Data Privacy and Security Requirements Specific to Healthcare AI

Much as the once-revolutionary electronic medical record, AI's integration into healthcare systems adds yet another revolutionary impact on the handling of sensitive patient data, necessitating strict adherence to privacy and security regulations. California's legal framework, encompassing both the CCPA/CPRA and CMIA, imposes significant obligations on healthcare AI stakeholders, including the following.

- The CCPA, as amended by the CPRA, is central to data privacy in the state, particularly with its expanded definition of "sensitive personal information" to include health data and "neural data." This means that AI systems processing such data must comply with consumer rights, including the right to know what information is collected, the right to delete it, and the right to opt out of its sale or sharing.
- The CPRA grants consumers the right to limit the use and disclosure of their sensitive personal information to specific, defined purposes.

- Using patient data to train AI models without proper authorisation or de-identification could constitute a CMIA violation.
- The California Attorney General's legal advisories reinforce these privacy obligations for healthcare AI. The advisories emphasise that AI applications must adhere to the CCPA, CPRA, CMIA, and HIPAA requirements, where applicable. AI developers and healthcare organisations deploying AI systems are required to:
  - (a) limit the collection and use of personal data to what is reasonably necessary and proportionate;
  - (b) obtain consumer consent where required and provide mechanisms for individuals to exercise their privacy rights;
  - (c) ensure rigorous testing and validation of AI systems to prevent errors and reduce harm, including ensuring training data is free from biases that could compromise accuracy or fairness;
  - (d) implement robust security measures to safeguard patient data, consistent with state requirements; and
  - (e) be transparent with patients about whether their information is used to train AI and how AI is utilised in decision-making.

Algorithmic Bias and Fairness Requirements
This previously arcane concept is now a particularly significant concern in the deployment of artificial intelligence in healthcare. California has taken a proactive stance to address algorithmic bias, recognising that biased AI systems can perpetuate or exacerbate existing health inequities.

Assembly Bill 2885 (AB 2885), the Algorithmic Accountability Act, mandates that the Department of Technology conduct a comprehensive inventory of "high-risk automated decision systems" used or proposed by state agencies. After all, algorithms are similar to recipes: They provide step-by-step instructions for accomplishing a complex task. Healthcare "recipes" are complex and carry profound consequences. These decision systems are deemed high-risk if they materially impact access to, or approval for, critical areas such as housing, education, employment, or healthcare.

The inventory requires a description of measures in place to mitigate risks, including the risk of inaccurate, unfairly discriminatory, or biased decisions. This includes performance metrics to gauge accuracy and risk assessments or audits for potential biases.

The California Attorney General's legal advisories explicitly address algorithmic bias within healthcare AI. The Attorney General emphasises that AI systems must align with state anti-discrimination laws. These laws prohibit discrimination based on protected characteristics such as sex, race, religion, or disability, and their applicability extends to AI systems, even if the discriminatory impact is unintentional.

The Attorney General warns that AI systems making "less accurate" predictions about protected classes could be considered discriminatory, regardless of data availability.

Healthcare entities are required to proactively design, acquire, and implement AI solutions that prevent past discrimination from being embedded or amplified by new technologies, and must maintain documentation of their bias testing and mitigation efforts. This includes avoiding uses of AI that could lead to discriminatory outcomes, such as using past claims data to deny patient access or conducting cost-benefit analyses based on stereotypes that undervalue certain patient populations.

Informed Consent and Transparency Obligations
The principles of Informed consent and transparency are woven into the fabric of healthcare. California's regulatory framework is actively extending these principles to artificial intelligence. The state aims to ensure that patients are fully aware when AI is involved in their care and have the means to understand and question its role.

The AI in Healthcare Act mandates specific disclosure requirements for health facilities, clinics, physicians' offices, and group practices that use generative AI to communicate patient clinical information.

Communications must include a prominent disclaimer indicating that generative AI produced the content. The disclaimer's placement and format vary depend-

ing on whether the communication is written (physical, digital, or continuous online interactions), audio, or video.

The communication must also provide clear instructions on how a patient can contact a human healthcare provider, an employee of the facility, or other appropriate person.

These disclosure requirements do not apply if the AI-generated communication is read and reviewed by a human licensed or certified healthcare provider before being sent. This provision aims to strike a balance between transparency and the efficiency benefits of AI.

In what might have been rightly seen in years past as the basis for a science fiction movie, California is also addressing AI's potential ability to impersonate healthcare professionals. Proposed legislation, such as Assembly Bill 489 (AB 489), seeks to explicitly prohibit AI and generative AI systems from misrepresenting themselves as titled healthcare professionals. This bill grants state boards the authority to pursue legal recourse against developers and deployers of AI systems that impersonate healthcare workers, reinforcing the principle that only licensed human professionals can provide medical advice or care.

The California Attorney General's legal advisories further underscore the importance of patient transparency. The advisories state that healthcare providers are required to notify patients when AI technologies are used in diagnostic or treatment decisions, fostering trust and enabling informed patient choices.

Reimbursement and Coverage Considerations for AI-Powered Healthcare Services

The integration of AI into healthcare services introduces new complexities for reimbursement and coverage, particularly concerning the role of AI in utilisation management. California has taken steps to regulate this area, aiming to ensure that AI tools enhance, rather than impede, patient access to medically necessary care.

Regulating the role of AI

The Physicians Make Decisions Act directly limits the ability of healthcare service plans and disability insurers to use AI for utilisation review and management functions.

The statute prohibits health plans from denying, delaying, or modifying healthcare services based solely on artificial intelligence algorithms. The law explicitly mandates that human judgment must remain central to coverage decisions, with clear documentation of the decision-making process.

Any determination of medical necessity, leading to an approval, modification, delay, or denial of care, must be reviewed and decided by a licensed physician or qualified healthcare professional with expertise in the specific clinical issues involved. This ensures that AI tools serve as aids, not replacements, for clinical judgment and decision-making.

AI tools used in utilisation review must base their decisions on the enrollee's medical or clinical history, individual clinical circumstances, and other relevant clinical information, rather than relying solely on group datasets. Healthcare organisations must maintain an auditable record of how individual patient data is weighted against population data in AI decision-making processes.

The law requires that AI tools, including their underlying algorithms, be open to inspection for audit or compliance reviews by regulatory bodies like the California Department of Managed Health Care (DMHC).

The DMHC is tasked with overseeing the enforcement of SB 1120, including auditing denial rates and ensuring transparency in AI-driven utilisation review processes. The law also imposes strict deadlines for authorisation requests, with administrative penalties for non-compliance.

These measures are intended to prevent inappropriate denials of benefits and ensure patients receive timely access to medically necessary services.

Enforcement Mechanisms and Penalties

Non-compliance with California's healthcare AI regulations carries enforcement risks and potential penalties, including administrative fines, civil litigation, and criminal charges, as applicable under state law. State agencies and the Attorney General's office possess broad authority to enforce AI-related laws in healthcare.

Violations of AB 3030's generative AI communication disclosure requirements are subject to specific enforcement mechanisms, as outlined below.

• For licensed health facilities, violations fall under the enforcement mechanisms described in Article 3 of Chapter 2 of the Health and Safety Code (Sections 1425-1429), which may include civil penalties of up to USD25,000 per violation.
• For licensed clinics, violations are subject to enforcement under Article 3 of Chapter 1 of the Health and Safety Code.
• For physicians, violations fall under the jurisdiction of the Medical Board of California or the Osteopathic Medical Board of California.

The DMHC and the California Department of Insurance (CDI) have the authority to assess administrative penalties for health plans and insurers that fail to meet the requirements of SB 1120, including timeframes for authorisation decisions or improper use of AI.

The California Privacy Protection Agency (CPPA) and the California Attorney General enforce the CCPA and CPRA. Penalties for non-compliance can be substantial, ranging from USD2,500 per non-intentional violation to USD7,500 per intentional violation or for offences involving the personal information of minors under the age of 16.

Individuals can bring private rights of action against entities that negligently release confidential medical information under CMIA, seeking actual damages, nominal statutory damages of USD1,000, and/or punitive damages upon proof of willful misconduct. Healthcare providers who knowingly and willfully obtain, disclose, or use medical information in violation of CMIA may be liable for an administrative fine of up to USD2,500 per violation. The Department of Public Health can also assess administrative penalties, including USD25,000 per patient whose medical information was unlawfully accessed, used, or disclosed, with subsequent occurrences incurring USD17,500 per incident, and daily penalties for failure to report.

Practical Compliance Strategies for Healthcare Organisations

Navigating California's healthcare AI regulatory landscape requires a proactive and multi-faceted compliance strategy. Organisations must integrate legal requirements into every stage of AI development, deployment, and ongoing operation.

Risk Assessment Frameworks for Healthcare Organisations

Healthcare organisations are obliged to take specific actions in order to assess risks related to the use of AI, such as:

• conduct algorithmic impact assessments (AIAs) to evaluate potential risks, including bias, discrimination, and privacy harms, before deploying AI systems, particularly high-risk ones;
• assess liability exposure for AI-assisted diagnoses and treatments, considering the evolving standard of care, corporate practice of medicine doctrines, and maintain appropriate professional liability insurance coverage that specifically addresses AI-related risks;
• develop detailed incident response plans for AI failures, data breaches, or adverse events, ensuring timely reporting and mitigation; and
• establish clear human oversight protocols for all AI-driven clinical and administrative decisions, ensuring that AI does not replace, but rather augments, human judgment.

Compliance Checklists for Healthcare AI Developers

Below, you can find compliance checklists for the developers of AI used within the healthcare sector.

• Implement mechanisms for prominent disclaimers and clear human contact instructions for generative AI patient communications, as required by AB 3030.

- Ensure AI used in utilisation management complies with SB 1120, mandating human oversight for medical necessity decisions and prohibiting sole AI-based denials.
- Adhere to AB 2885's requirements for high-risk automated decision systems, including inventory, bias audits, and transparency.
- Integrate privacy-by-design and security-by-design principles into AI system architecture.
- Implement robust data minimisation and de-identification techniques for training and operational data, consistent with CMIA.
- Establish secure data handling protocols, including encryption, access controls, and regular vulnerability assessments.
- Conduct regular audits of data inputs, outputs, and model performance to detect and mitigate bias and ensure accuracy.
- Develop comprehensive vendor management programs for third-party AI solutions, ensuring business associate agreements (BAAs) are in place, that vendors meet all regulatory requirements, and that regular compliance audits are conducted to verify ongoing adherence to applicable laws and regulations.

Strategies for Navigating Conflicting State Requirements
Adopt the "most stringent" standard
When state laws impose different requirements, organisations should generally adhere to the more stringent standard to ensure comprehensive compliance.

Develop a layered compliance approach
Organisations need to implement a compliance program that addresses all state requirements distinctly, recognising where California laws add specific obligations (eg, AB 3030's disclaimers, SB 1120's human oversight for utilisation review).

Conclusion
California's healthcare AI regulatory landscape is rapidly taking shape amid ongoing innovation and debate. That evolutionary process occurs through a legislative and enforcement approach that prioritises patient safety, data privacy, algorithmic fairness, and informed consent. The state's framework introduces unique and often more stringent requirements, including transparency in AI-generated patient communications, human oversight in health insurance utilisation review, and robust data privacy rights for health information.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com