Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Artificial Intelligence in Health: Overview of Selected State Liability Frameworks

August 10, 2026

A variety of artificial intelligence (AI) technologies are increasingly used for various health care or related purposes. These purposes include core clinical health care functions such as the diagnosis and treatment of diseases and the administration of health claims for the payment of such services. In addition, AI technologies are also being incorporated in other applications, such as for wellness and fitness, or in applications—such as a general use chatbot—that may not be specifically promoted for health care uses but have the capabilities, and may be used by the public, for health-care-related inquiries. While the use of AI in certain health care contexts is not new with many products subject to federal regulation—the Food and Drug Administration (FDA), for instance, approved AI-enabled medical devices as early as 1995—other applications of AI in or related to health care have generated questions regarding the application of existing regulatory frameworks.

As more consumers interact directly or indirectly with health-related AI technologies, some have claimed certain injuries stemming from them. The suits primarily allege various claims under state statutory and common law. This Sidebar provides an overview of the claims and injuries alleged in selected litigation involving alleged harm caused by health-related AI applications or AI-enabled products, an overview of the relevant state-level liability frameworks invoked by these suits, and selected observations and considerations for Congress.

Background on Selected Litigation and State Liability Frameworks

Litigation involving AI-enabled applications in or related to health has occurred in various contexts, including: (1) alleged use of AI-enabled applications by health plans to make coverage determinations; and (2) consumer-facing AI-enabled applications for various health-related uses, such as wellness, health screening, and chatbot exchanges. Litigants in these cases have asserted various claims, including those based on certain state laws related to consumer protection, privacy, and products liability.

Congressional Research Service
https://crsreports.congress.gov
LSB11467

AI and Coverage Determinations

Health insurers have increasingly employed AI tools to automate and expedite prior authorization of claims, post-service claims review, and other processes related to coverage determinations. In general, insurers make coverage determinations for a particular health service for insured individuals based on a finding of medical necessity. Federal law and regulations that govern insurance coverage determinations vary based on the type of health coverage or program. For instance, in the context of private-sector, employment-based health coverage, the Employee Retirement Income Security Act (ERISA) and accompanying regulations generally require applicable private health plans to maintain reasonable claims processing procedures, as well as an opportunity for "full and fair review" of denied claims. In the context of Medicare Advantage (MA), a program in which private health insurers contract with the federal government to provide covered benefits to Medicare beneficiaries, MA plans—in addition to being subject to similar claims processing requirements—must also base medical necessity determinations on factors specific to the enrollee under an April 2023 final rule. If an MA plan expects to issue an adverse determination regarding medical necessity, such determination must also be reviewed by a physician or other health care professional with appropriate expertise.

Litigants have filed suits challenging insurers' use of AI in coverage determinations in both the private health insurance and MA contexts. For instance, in a recent case concerning a private health insurance plan, plan participants allege that the defendant insurer wrongfully denied plaintiffs' claims through its use of an algorithm that allowed physician claims reviewers to automatically deny batches of claims, without meaningful review. In at least two comparable cases brought before the 2023 regulations took effect, MA plan enrollees similarly allege that their MA plans improperly used an unreliable AI model in lieu of physicians to make coverage determinations for post-acute care, and that the model led the plans to wrongfully deny enrollees' claims. The plaintiffs in each of these cases argued that the relevant plan's conduct violated, among other laws, various state statutory and common law requirements, including certain state consumer protection laws commonly referred to as Unfair and Deceptive Acts and Practices (UDAP) statutes.

To protect their residents as participants in commercial transactions, every state has enacted a UDAP statute that prohibits, to varying degrees, deceptive business practices; many of these statutes also prohibit unfair or unconscionable practices. Many of these statutes are structured based on model acts or the Federal Trade Commission Act (FTC Act), under which "unfair or deceptive acts or practices in or affecting commerce" are unlawful. To the extent a state's UDAP laws include a general prohibition of unfair or deceptive practices (as opposed to an enumerated list of prohibited acts), it can often be flexibly applied to a variety of conduct and industries. While state attorneys general are primary enforcers of state UDAP laws, many state UDAP laws also authorize consumers harmed by a prohibited practice to bring a private lawsuit against those who engage in such practice. Plaintiffs in the lawsuits described above, for instance, have invoked state UDAP laws to argue that the defendant insurers' alleged use of AI in lieu of a physician determination is an unfair and/or deceptive act. In industries like health insurance that are regulated at both the federal and state level, however, one limit to the application of state UDAP laws is the preemption doctrine—under which applicable federal law displaces conflicting state law. The defendants in these cases have generally argued that federal law preempts the plaintiffs' claims. The two district courts considering claims against MA plans have concluded that the Medicare statute's express preemption provision governing MA standards preempted the plaintiffs' state UDAP claims, but other common law claims, such as a breach of contract claim, were not preempted by the Medicare statute. In contrast, the district court concluded that ERISA—which includes a preemption provision with a savings clause—did not preempt similar state UDAP claims against the plaintiffs' private health insurer. Litigation in these cases remains ongoing.

AI and Other Health-Related Uses

Several other cases involve various consumer-facing applications or products incorporating AI for health-related uses that are alleged to have harmed consumers' privacy interests or directly injured users. These applications or products are promoted for a range of purposes, including promoting general health and wellness, providing health screening, and engaging in conversations that can include health-related topics. With respect to health and wellness, for instance, some examples of applications that have been the subject of suits include: (1) Flo App, a menstruation and ovulation tracking application marketed as using AI to predict reproductive cycles; (2) Skin360, a mobile application marketed as using AI to compare a scan of a user's face to a database of images to provide a skin assessment and related product recommendation; and (3) Whoop, a wearable product that measures and collects various user physiological data and provides "AI-driven," personalized health and fitness insights. In addition to health and wellness, suits have also involved a kiosk product that incorporated AI-powered software that conducted and collected temperature screenings with facial recognition features. Another set of lawsuits have involved a general-purpose AI chatbot application that interacts with users as anthropomorphic characters. According to plaintiffs in these cases, the application engages with minor users in conversations related to mental health.

Most of these lawsuits allege that the relevant application developer or manufacturer violated applicable state privacy laws in the way the application or product collected and/or shared user data with third parties. In the set of lawsuits involving the AI chatbot, the plaintiffs primarily allege that the chatbot's developers, in violation of state tort laws, defectively designed the chatbot in a manner that makes it particularly unsafe for youths who interact with the application's fictional characters, and failed to adequately warn users of those risks.

State Privacy Law

Some states have enacted certain privacy laws that may apply to certain AI-enabled applications based on an application's specific features or functions. Illinois's Biometric Information Privacy Act (BIPA), for instance, subjects a private entity's retention, collection, disclosure, and destruction of a "biometric identifier"—which refers to "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" that is not "captured from a patient in a health care setting"—to specified requirements, including making publicly available a written policy establishing retention and destruction guidelines. The law provides a private right of action to any person aggrieved by a violation of BIPA. At least two district courts have concluded that certain consumer claims alleging violations of BIPA—one involving Skin360 and another involving the temperature screening kiosk product with facial recognition features—may proceed against the relevant defendants. California's Confidentiality of Medical Information Act (CMIA), as another example, imposes requirements on sharing of medical information by "[a]ny 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 . . . for purposes of allowing the individual to manage the individual's information." The law, in addition to other remedies, provides a private right of action to a patient whose medical information has been used or disclosed in violation of the law. In the cases involving Flo App and Whoop, the plaintiffs allege that the relevant product manufacturer is subject to and has violated CMIA by sharing the collected data with third parties.

State Products Liability Law

State products liability law is a subset of tort law—a body of rules historically developed through judicial decisions aimed at remedying harms caused by another's wrongful or injurious actions. Rather than focusing on whether harm was caused by a defendant's careless act—the inquiry in a general tort case—

the inquiry in products liability cases focuses on whether harm was caused by a defective product. This focus imposes what is known as strict liability on a manufacturer to ensure that the manufacturer bears the costs of injuries resulting from its product. In a products liability suit, a plaintiff generally must prove that a product sold commercially by the defendant was defectively manufactured or designed, or should have included different warnings or instructions, and that such defect caused the plaintiff's injury.

With respect to AI technologies, which are often incorporated in software applications, a threshold question regarding the application of products liability law is whether an AI application is a "product." Historically, many courts have limited the application of products liability law to "tangible" products—such as a car or a drug—and have held that computer software—including video games and websites—is not a "product" for products liability purposes. In these courts' view, software applications either offered a "service" or were alleged to have caused injuries based on the ideas or expressions they contained. Extending strict liability in either circumstance, the courts reasoned, would not be appropriate because the relevant software defects were more akin to service failures resulting from human action or because such extension would impose liability based on the distribution of ideas, raising First Amendment concerns.

More recently, however, some courts examining the application of products liability law to software have concluded that in some circumstances, software applications or certain software functions may be "products" for products liability purposes. In these courts' view, a software application may be "sufficiently analogous to the distribution and use of tangible personal property that it is appropriate to apply the rules of strict liability" to the software developer, where the software reflects the developer's proprietary design, is mass-marketed and distributed by the developer in the stream of commerce, and is alleged to have caused harm based on design elements or functions over which the developer exercises control. In *Garcia v. Character Technologies, Inc.*, a district court considered whether products liability claims may be asserted against (1) a developer of a character AI chatbot and (2) Google—whose large language model (LLM) is alleged to underlie the AI chatbot to enable it to engage in open-ended conversations with users. Recognizing that the plaintiff's claimed injury stemmed from both the content of the chatbot's conversation with an underage user and the design and functionality of the chatbot, the court concluded that the AI chatbot is a "product" for products liability purposes "so far as Plaintiff's claims arise from defects" in the chatbot—such as its alleged lack of age verification and reporting mechanisms. The court, however, dismissed aspects of the plaintiff's products liability claim based on expressions made by the chatbot. The court also concluded that products liability claims may be asserted against Google as a component part manufacturer, given the alleged integration of its LLM into the chatbot that caused the chatbot to be defective.

Observations and Considerations for Congress

As Members of Congress examine potential measures to govern AI and its applications in health and other contexts, questions may arise about potential liability under existing frameworks. Litigation involving health-related AI applications under the state law regimes discussed above are generally in the early phases and have not resulted in merits findings. Thus, the extent to which such suits can provide remedies to injured consumers is unclear. That determination will depend on several factors, including how courts apply the relevant case law or interpret relevant statutes, what evidence the parties can adduce in support of their claims or defenses, and whether the parties opt to voluntarily settle the claims.

In the meantime, these fast-evolving technologies have also generated questions about the application of existing federal regulatory frameworks. For example, AI-enabled health care and related products have raised questions about what products are subject to FDA jurisdiction and the circumstances under which the agency should exercise enforcement discretion over products within its jurisdiction. Recognizing the rise of widely accessible general-purpose AI chatbots and an increase in the development of and potential demand for "AI therapists," FDA noted that "the regulatory status paradigm of generative AI-enabled

products is a spectrum from those that are not devices and are not within FDA's regulatory purview to those that are devices and are the focus of FDA's oversight"—a spectrum FDA recognized "has been a source of confusion to users," particularly when an AI product has not been specifically promoted for medical use. With respect to the regulation of general wellness products, FDA recently issued updated guidance that addresses the circumstances under which wearable products that use noninvasive sensing technology to estimate, infer, or output certain physiological parameters (such as oxygen saturation, heart rate variability, and blood pressure) are considered low-risk general wellness products over which the agency would exercise enforcement discretion. The updated guidance, however, does not address AI-enabled products.

The evolving AI technologies also highlight the parameters of certain existing federal frameworks. For example, with respect to privacy, the federal Privacy Rule issued pursuant to authority in the Health Insurance Portability and Accountability Act of 1996 (HIPAA Privacy Rule) imposes requirements and limits on the use and disclosure of protected health information. The HIPAA Privacy Rule—as an element of a series of requirements aimed at facilitating a transition by health care entities from paper-based to electronic health care administrative and financial transactions—applies only to specified covered entities and their business associates. Covered entities include (1) health care clearinghouses, (2) health plans, and (3) health care providers who carry out HIPAA-covered electronic transactions. Accordingly, while the HIPAA Privacy Rule likely applies to AI-enabled tools used by health plans and providers, to the extent such tools handle the protected health information of relevant enrollees and patients, the rule likely does not apply to many consumer-facing AI applications that are not covered entities, including those used for wellness purposes.

In response to the surge of AI technologies in health and potential uncertainties in the application of existing frameworks, some states have enacted legislation specific to addressing some of the relevant uses. Several states, for instance, have imposed additional requirements or limits on the use of AI applications in the mental health context, including by mental health professionals. Some states have imposed requirements that limit the use of AI applications in coverage determinations. Several states have enacted laws requiring "operators" of "companion chatbots" or "AI companions" to maintain a protocol for detecting and addressing suicidal ideation or expression of self-harm by users, or for preventing the production of such content to users.

At the federal level, President Trump has issued an Executive Order (EO) stating the intent of his Administration to "act with the Congress to ensure that there is a minimally burdensome national standard" governing AI that "forbid[s] State laws that conflict with the [national] policy" while "ensur[ing] that children are protected, censorship is prevented, copyrights are respected, and communities are safeguarded." The EO states that "[u]ntil such a national standard exists, . . . it is imperative that [the] Administration takes action to check the most onerous and excessive laws emerging from the States that threaten to stymie innovation." To that end, the EO directs the Attorney General to establish an "AI Litigation Task Force" responsible for "challeng[ing] State AI laws" inconsistent with the national policy described in the EO. It is unclear if any of the state laws specifically addressing health-specific AI applications are under review by the Task Force, which was established in January 2026. Meanwhile, Members of Congress have introduced legislation, such as S.4199, the Youth AI Privacy Act, and S. 5117, the Senior Chatbot Protection Act of 2026, that would regulate general use chatbots to varying degrees while generally preserving state laws that provide additional protections to users.

These developments highlight the breadth of issues raised by health-related AI use—from the regulation of the technology itself, the regulation of who may use the technology and how, and any privacy or other legal concerns raised by this use. The developments also highlight the different potential approaches to addressing the use of AI in the health context and potential questions related to interaction between potential federal and state laws when analyzing possible liability or other frameworks. In general, when Congress enacts or amends a federal regulatory scheme pursuant to one of its enumerated powers under

the U.S. Constitution, it can specify the extent to which relevant state requirements are preempted. The scope of such express preemption provisions may potentially range from only certain enumerated federal requirements to a broader field of federal regulation. Historically, however, many areas implicated by health-related AI use, products implicating public health, and issues of consumer protection are areas long subject to concurrent federal and state regulation. This regulatory status is often explicitly recognized in existing federal law, making broad preemption provisions more uncommon. Some existing federal laws also explicitly recognize certain areas—such as the practice of medicine—as within the province of state regulation. The developments arising from the rapid adoption of health-related AI-enabled products—including ongoing litigation asserting harms caused by such products and state-level legislative responses—highlight some of the ways health-related AI uses implicate those areas of concurrent federal and state regulation.

Author Information

Wen W. Shen
Legislative Attorney

Jennifer A. Staman
Legislative Attorney

Disclaimer