Predicting Digital Health Trends in 2026

Insights 01.06.26

As 2026 approaches, digital health is at a regulatory inflection point. Consumer-driven care models and bipartisan support for telehealth expansion continue to reshape how care is delivered, while payment parity policies have the potential to drive greater adoption of telehealth and integration of wearables and other digital health technologies into care management. Meanwhile, the growing use of general-purpose artificial intelligence has prompted lawsuits against model developers and spurred legislative efforts – including, in some cases, outright prohibitions on mental health chatbots. The ongoing debate over a comprehensive national artificial intelligence (AI) framework leaves providers and innovators navigating a patchwork of state laws and competing federal initiatives. In response, health care providers are developing governance models to address data privacy, consent, authorized uses, and patient education.

Telehealth retains bipartisan support, but is it enough?

In 2025 we saw the first-time federal telehealth waivers expired since being implemented during the Covid-19 pandemic. Without Congressional action on federal funding which aligned with the expiring waivers, providers had to temporarily halt telehealth arrangements through the duration of the government shutdown. While the waivers were ultimately extended and retroactively applied, the loss of access to care and confusion over reimbursement was of great concern to providers and patients. The lapse itself had more to do with federal government tensions rather than the merits of the extension as evidenced by the topic's consistent inclusion in government funding talks historically as well as countless Congressional hearings and efforts. With the government facing yet another cliff on January 30th for government funding and telehealth waiver extensions, the question is whether its broad bipartisan support is enough to ensure continuation of an extension outside of the politically charged short term environment. We expect that any funding extension that were to pass will include a telehealth extension for the same length of time as the funding agreement.

Behavioral Health will be front and center in the debate on how to regulate Health AI

Throughout 2025, state and federal policymakers responded to rising public concern about how artificial intelligence affects mental health. States enacted the first laws targeting clinical use, misrepresentation, and data privacy. At the same time, plaintiffs filed lawsuits against developers of AI chatbots, alleging that

PROFESSIONAL

MONICA MASSARO
Principal, Government Relations & Public Policy
Washington, D.C.

ANDREA FREY
Partner
San Francisco
San Diego

CLAIRE ERNST
Director, Government Relations & Public Policy
Washington, D.C.

ERIC M. FISH
Partner
Washington, D.C.

STEPHEN K. PHILLIPS
Partner
San Francisco

ALICIA MACKLIN
Partner
Los Angeles

product designs contribute to, or even encourage, self harm. Behavioral health has emerged as one of the few areas where regulating AI in health care is drawing bipartisan support. The Food and Drug Administration, which oversees certain AI enabled tools, has also begunreviewing Generative AI Digital Mental Health Medical Devices. Its goal is to establish comprehensive recommendations for risk mitigation, including standardized requirements for premarket evidence, and the implementation of rigorous post market monitoring. Looking ahead to 2026, stakeholders should anticipate a surge in activity as government agencies codify these processes. These initial frameworks in behavioral health are expected to serve as foundational models that could eventually be expanded to regulate AI applications across the broader healthcare landscape.

Evolving Data Sharing and Privacy Landscape

At the same time, data sharing and privacy obligations are becoming more complex as interoperability initiatives accelerate alongside enforcement activity. The Trusted Exchange Framework and Common Agreement (TEFCA) continues its phased rollout, expanding expectations for nationwide data exchange and alignment of technical, contractual, and governance frameworks with Qualified Health Information Network (QHIN) participation. Building on the focus toward addressing interoperability, the Trump Administration announced its establishment of a new Health Tech Ecosystem involving 60 data networks, health systems and providers, app developers, and payers who made voluntary commitments to adopt and align with a new interoperability framework designed to create a process for easily accessible and shareable medical information across newly created CMS Aligned Networks. In parallel with these initiatives, federal regulators have signaled intent to shift toward stricter enforcement of the information blocking rules. On the legislative front, there is also renewed interest in comprehensive federal privacy legislation, such as Senator Cassidy's proposed *Health Information Privacy Reform Act* (S. 3097), in tandem with state efforts such as New York's recently failed *Health Information Privacy Act* (S.929/A.2141), highlighting growing momentum to establish baseline protections for health and consumer data, particularly as AI and digital tools blur traditional distinctions between regulated protected health information under HIPAA and broader consumer data.

Trump Administration Leverages CMMI To Test Digital Solutions

The last year represented a clear shift in the way the CMS Innovation Center (CMMI) approaches new models – namely leveraging digital and AI solutions to achieve outcomes highlighted in its refreshed "strategic direction," including protecting federal spending and empowering patients to achieve their health goals. Two models in particular exemplify this shift: The WISeR (Wasteful and Inappropriate Service Reduction) Model would use AI to identify fraud, waste and abuse in claims and the ACCESS (Advancing Chronic Care with Effective, Scalable Solutions) Model would expand access to new technology-supported care to manage chronic disease. While both models are anticipated to go live in 2026, their full impact will take time to materialize. Nonetheless, CMMI remains a critical vehicle for advancing the Trump Administration's healthcare agenda, with future digital-centric models expected.

Trump's AI Executive Order Ushers in More Uncertainty Than Uniformity

Amid growing public pressure to regulate artificial intelligence and the absence of a comprehensive national strategy, state legislatures enacted several laws addressing transparency, consumer protection, and health care specific applications. Over concerns that a patchwork of state laws would impede adoption of AI, President Trump issued his Executive Order, " *Ensuring a National Policy Framework for AI*," on December 11, 2025. The intent of the Executive Order is to establish national uniformity and directs agencies to challenge "onerous" state laws. However, the extent to which these challenges focus on more general AI issues or are targeted to specific industries remains unknown. Additionally, it remains unclear whether there is sufficient statutory preemption authority to successfully challenge state laws.

The early indication is that the Executive Order has not prevented states from advancing new legislation, guided in part by the belief that their 10th Amendment authority provides a sufficient basis to act in the public interest. These state-level proposals range from broad measures targeting algorithmic discrimination, such as Washington's H.B. 2157, to narrowly tailored health care protections like Pennsylvania's H.B. 2100 governing chatbot use in mental health contexts, underscoring the persistence of overlapping and potentially conflicting rules. The constitutional questions raised by the Executive Order

may also invite litigation to determine whether regulation of artificial intelligence is a state or federal question. As a result, providers and digital health innovators must prepare for a fragmented, adversarial landscape that requires agility, close attention to privacy, disclosure, and bias review requirements, and a pragmatic 50-state compliance strategy rather than reliance on simplified federal oversight.

Adoption of AI Outpaces Oversight, Creating a Crisis for Healthcare Governance

As we move into 2026, instituting robust AI governance structures remains a critical priority as AI becomes more deeply embedded in clinical, operational, and patient engagement functions. Although 2025 saw the release of influential model frameworks from organizations such as the Guidance on Responsible Use of AI in Healthcare, a project between the Joint Commission and the Coalition for Health AI (CHAI), as well as the Health AI Partnership's AI Vendor Disclosure Framework and the American Medical Association's Tool Kit for Governance of Augmented Intelligence, adoption of the recommendations has been uneven, leaving significant gaps in oversight, understanding of system limitations, and management of risk. While most health systems now use AI in some form, few have mature governance structures, with wide variability driven by system size and resources, and growing concern over "shadow" uses of general-purpose AI outside formal oversight. Absent strong governance addressing responsible use, vendor vetting, data security, explainability, and contractual alignment, providers face heightened regulatory, reputational, and patient safety risks, making it likely that boards and executives will face increasing pressure to formalize AI governance to meet evolving legal requirements and sustain trust in a rapidly changing technological environment.

Corporate Practice Scrutiny on the Rise

As digital health and AI-enabled care models scale, states are renewing scrutiny of the corporate practice of medicine (CPOM) doctrine, particularly where technology companies play an expanded role in the support of clinical decision-making, care delivery, and revenue flows. Regulators in California and Oregon have taken especially assertive approaches, focusing on management services arrangements, ownership structures, and the degree of control exercised by non-physician entities over clinical operations, pricing, and physician judgment. For example, in California, SB 351 codifies limitations on the involvement of private equity groups and hedge funds in physician and dental practices, reinforcing long-standing CPOM enforcement principles. Oregon has gone further, enacting SB 951, among the nation's most restrictive CPOM regimes, explicitly targeting digital health companies and private equity-backed providers that rely on the affiliated professional corporation or "PC-MSO" (friendly physician) model – a structure historically used to engage physicians without direct ownership or employment. Together, these developments underscore growing regulatory concern that innovative care models not erode physician independence or patient protections. Digital health companies and other providers operating under PC-MSO arrangements, who already navigate a complex and often frustrating patchwork of CPOM laws, should anticipate increased scrutiny and potential challenges from regulators, competitors, and other market participants alleging impermissible influence over the practice of medicine, and should carefully reassess governance, contracting, and operational controls in light of this heightened enforcement environment.

Consumer Desire for Digital Health Care Upends Legacy Systems and Amplifies Calls for Modernizing Licensure

Consumer-driven digital health platforms are reshaping patient expectations around convenience, access, and personalization, creating tension with traditional healthcare models built on in-person visits, continuity of care, and institution-centered workflows. While legacy providers emphasize physical examinations, face-to-face interactions, and established protocols, digital health disrupts office-visit revenue models, challenges referral gatekeeping, and raises interoperability issues with existing electronic health record systems. These pressures are intensified by the emergence of "AI doctors," clinical-grade systems that support triage, diagnosis, and care planning, which blur the boundaries of medical practice and existing state regulatory frameworks. Growing calls from investors for the creation of Medical AI Practice Acts and new licensure and reimbursement pathways for AI-enabled platforms may prompt renewed federal and state regulatory efforts, such as resurrecting prior attempts by Congress to amend the FDA Act to permit artificial intelligence platforms to qualify as a practitioner eligible to prescribe drugs, or force state medical boards to consider regulatory frameworks to

address innovative care delivery models in a manner that keeps a licensed physician in the loop.

Final Thoughts

Looking ahead, 2026 is poised to bring significant federal and state regulatory movement in digital health. In addition to the trends above, the Assistant Secretary for Technology Policy (ASTP) is expected to release final rules under HTI-5, shaping interoperability and health technology implementation. Meanwhile, the Office of Civil Rights (OCR) is anticipated to issue final rules amending HIPAA, updating privacy standards to better address care coordination, patient access, and emerging digital tools. States, in an effort to strike a balance between fostering innovation and ensuring consumer safety, may increase the use of regulatory sandboxes, such as the one operating in Utah, to iterate on safety frameworks based upon concrete evidence of performance, rather than hypothetical harms. These developments, along with ongoing enforcement and guidance in areas such as AI, telehealth, and information blocking, signal a period of accelerated regulatory activity that will have broad implications for hospitals, providers, and digital health innovators alike.

RELATED CAPABILITIES

Digital Health

Government Relations and Public Policy

Antitrust and Unfair Business Practices

Health Information Privacy and Security

Behavioral Health Providers