Healthcare Trend Report: Digital Health

May 2026

Holland & Knight

www.hklaw.com

Table of Contents

Overview

Digital health has entered a "recalibration phase" following its post-pandemic correction, with the sector now firmly focused on delivering measurable outcomes and return on investment. Key drivers shaping this new landscape include the integration of artificial intelligence (AI) across workflows, a focus on chronic disease management and the drive for administrative efficiency. This shift has created a "haves and have-nots" theme in the market, where capital is concentrating in mature companies while early-stage ventures face tighter funding constraints.

As the sector evolves and more providers and payers implement digital health solutions, the government is determining how best to regulate. State and federal regulators have been active in determining how to properly monitor and support innovation while protecting patient care.

This report, prepared by Holland & Knight's Digital Healthcare Group, provides an overview of the transactional, regulatory and litigation trends facing the sector.

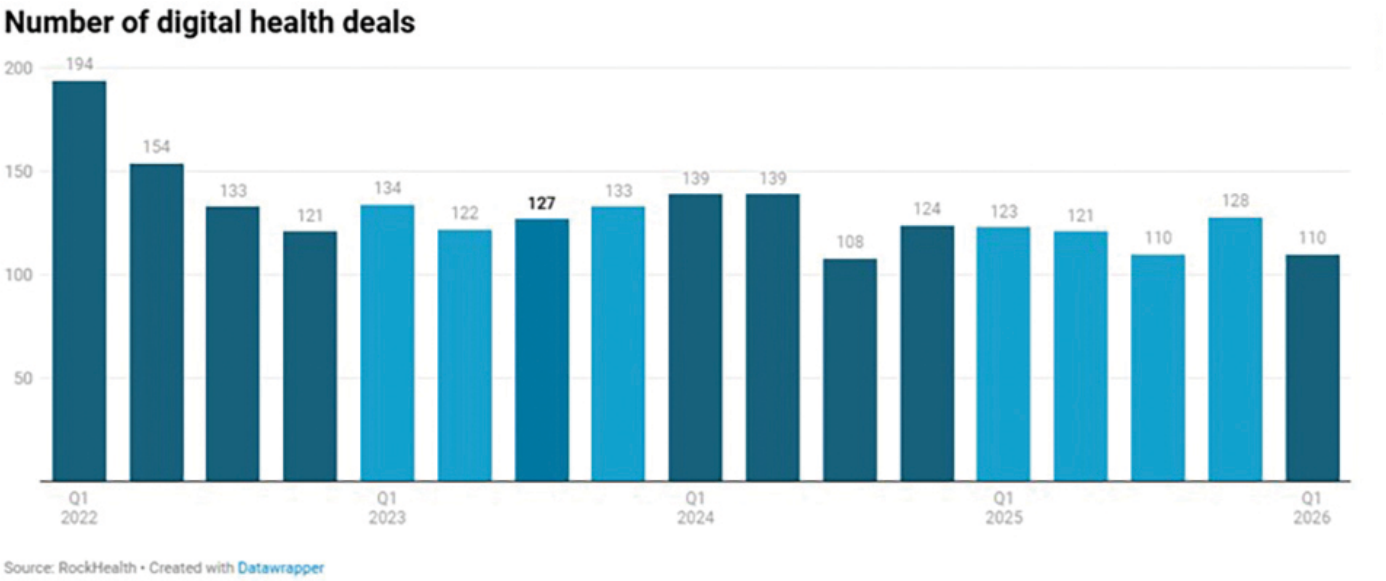
Investment and Transaction Trends

Global digital health funding experienced a significant rebound in 2025, with total investment rising 9 percent to reach $28.8 billion. This capital was increasingly concentrated in "mega-deals" exceeding $100 million, which accounted for more than 40 percent of the total funding and favored mature companies with proven traction. A notable "AI premium" emerged during this period as companies specializing in diagnostics and clinical documentation commanded significantly higher valuations than their peers.

The sector also saw a 61 percent surge in mergers and acquisitions (M&A) activity compared to 2024, driven largely by strategic acquirers looking to fill critical gaps in AI and workflow automation. This wave of consolidation hit telehealth and point-solution platforms particularly hard, leading to a mix of strategic mergers and distress sales. In 2026, the outlook remains optimistic as initial public offering windows begin to reopen for high-quality assets, while private equity firms shift their focus toward software and services platforms over hardware-centric models.

As of first quarter 2026, megadeals of $100 million or more were the driving force behind a strong increase in both digital health funding and average deal size.

Altogether, 110 companies received $4 billion during the quarter, according to seed fund Rock Health. This represents a $1 billion increase from $3 billion spread across 122 deals in first quarter 2025.



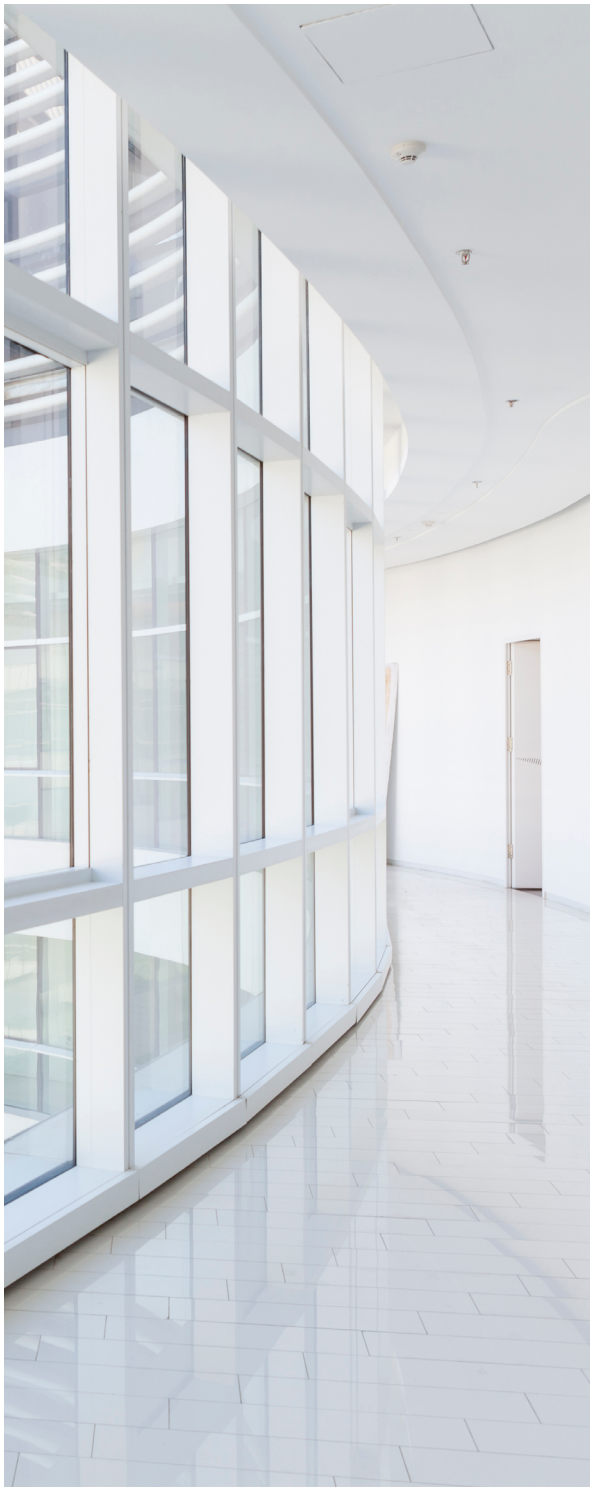
Holland & Knight's M&A Representation of Digital Health Companies in 2025

- Represented Minset AI Inc., an emerging company that created the first multiskilled agentic AI platform purpose-built for healthcare revenue cycle management, in connection with a seed funding round led by HealthX Ventures, a leading digital health venture capital firm
- Represented GetixHealth, a leading provider of revenue cycle management solutions to the healthcare industry and portfolio company of Trivest Partners, in its sale to H.I.G. Capital, a leading global alternative investment firm
- Represented Ensemble Health Partners, a private equity-backed full-service revenue cycle management company delivering holistic financial health for more than 250 healthcare providers across the country, in its add-on acquisition of a software development company of an AI platform that uses neuro-symbolic AI to analyze complex, unstructured data

Banker's Perspective: Insights from Houlihan Lokey

Houlihan Lokey provides premier M&A advisory, capital raising and financial restructuring services to healthcare technology providers. Leveraging deep domain expertise, the team helps clients navigate industry shifts to maximize shareholder value. Below, Managing Director Dudley Baker provides his perspective on deal trends shaping the sector.

- **M&A Spikes:** "In 2025, M&A activity returned to its highest levels since 2021, with private equity deal value surging nearly 25 percent year over year to reach $43.4 billion, the second-highest year on record. In particular, we saw a meaningful increase in M&A activity across the payer technology market in 2025 and expect that trend to continue in 2026, while revenue cycle management, post-acute care technology and specialty healthcare remained very active."
- **Valuation Gaps:** "The valuation gap between higher-quality and lower-quality assets remains significant as best-in-class businesses continue to command premium multiples. In 2026, we expect the bifurcation to be driven by perceived AI disintermediation risk, with top multiples being paid for businesses serving as vertical systems with highly regulated workflows and extensive marketplace networks."
- **Focus on Price Transparency and Reducing Costs:** "Among the Trump Administration's top priorities, we anticipate that the focus on reducing payer-provider abrasion and improving the member experience will continue to drive increased deal activity in 2026 around AI-powered tools that enable collaboration between all stakeholders. The Trump Administration's plan to launch a national provider directory has the potential to address a significant pain point for health plans and providers, transform member experience and streamline access to care."
- **Administrative Friction:** "The biggest challenges we see driving demand for differentiated solutions are related to administrative friction and poor visibility between stakeholders that limit collaboration, misalign incentives and create significant inefficiencies. Two areas where we see those challenges being especially pronounced are between providers and pharma manufacturers within the specialty healthcare ecosystem (i.e., therapy initiation) and between payers, providers and members due to significant data quality issues and challenges."



Evolving State and Federal AI Regulations

AI utilization in healthcare has rapidly transformed from peripheral use cases to core clinical and operational infrastructure. As a result of this rapid acceleration, AI adoption has outpaced legislation and overall policy development at the federal level, leaving state legislatures to take the lead in regulating AI deployment in the healthcare industry.

State-Level Activity: Near-Term Landscape, Long-Term Implications

In 2025, more than 250 AI-related healthcare bills were introduced in state legislatures, with a consistent focus on:

- patient disclosure and informed consent frameworks for AI-enabled care
- ensuring AI use does not lead to biased or otherwise discriminatory effects
- preservation of clinician accountability for AI-informed decisions
- ensuring AI technologies do not provide services that are reserved for licensed healthcare professionals
- restricting AI use by health insurers, particularly in coverage determinations and utilization review

Different state requirements, particularly around bias and discrimination requirements, pose a risk of creating a fragmented regulatory environment that could constrain AI deployment.

Federal Activity: Congress and the Administration

The U.S. Congress has not passed any significant legislation that directly impacts the use of AI in healthcare. Rather, it has focused its efforts on oversight and policy development, with a focus on supporting innovation, while addressing targeted risks such as child safety, intellectual property (IP) and infrastructure costs.

At the executive level, the Trump Administration released a National Policy Framework for Artificial Intelligence, which proposes that Congress establish a single federal approach for regulating AI use. The framework also calls for codifying elements of a December 2025 executive order, "Ensuring a National Policy Framework for Artificial Intelligence," which seeks to preempt state-level AI activity. Executive orders, however, do not carry the force of law needed for such preemption.

Federal Activity: HHS AI Actions

Under the current U.S. Department of Health and Human Services (HHS), AI-related activity remains incremental but directionally significant, with the U.S. Food and Drug Administration (FDA), Centers for Medicare & Medicaid Services (CMS), Centers for Disease Control and Prevention (CDC), and National Institute of Standards and Technology (NIST) advancing policy through targeted guidance and pilot programs rather than new rulemakings.

- FDA is advancing AI policy through guidance, targeted pilots and internal modernization efforts. Agency activity remains focused on clarifying how existing statutory and regulatory authorities apply to AI-enabled technologies, particularly in clinical and diagnostic contexts. Recent FDA actions of note include the use of pilots and enforcement discretion, such as the Technology-Enabled Meaningful Patient Outcomes (TEMPO) Pilot, which aims to utilize real-world evidence generation for certain digital health technologies, including AI-enabled tools, in coordination with CMS payment models.

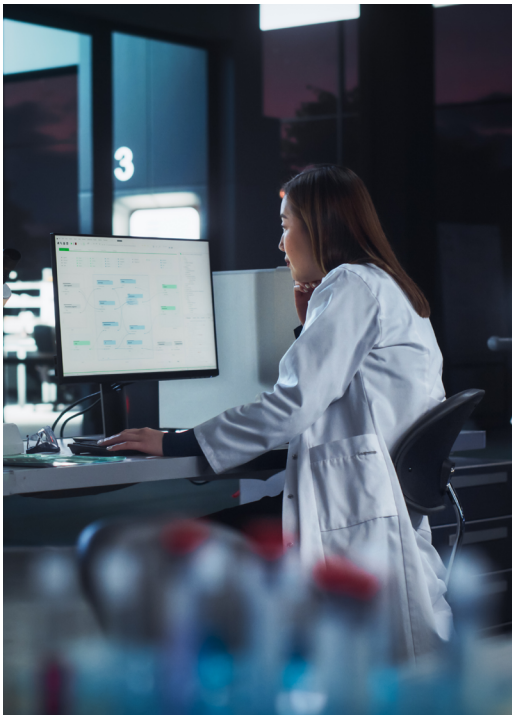
- CMS is shaping AI adoption primarily through payment models, demonstrations and administrative pilots rather than direct regulation. Through the Center for Medicare & Medicaid Innovation, CMS is testing how AI-enabled and data-driven tools can be integrated into care delivery and program administration. Recent CMS actions of note include introduction of the WISeR model, which pilots the use of AI and machine learning to support prior authorization and utilization review for select services in traditional Medicare. For more information, view Holland & Knight's CMS Payment Model Navigator.
- CDC is approaching AI through research guidance, internal governance and public health capacity building, with an emphasis on responsible use and public trust. Recent CDC actions of note include agentic research guidance – which addresses the use of "deep research" tools that autonomously plan and execute multistep research tasks, emphasizing human oversight and clearly defined use cases – and an agency-wide AI strategy.
- NIST continues to shape AI governance through voluntary standards, technical frameworks and stakeholder-driven processes rather than regulation. Recent NIST actions of note include the AI Standards "Zero Drafts" Pilot Project, which aims to accelerate standards development by producing preliminary, technically grounded drafts for submission into private sector-led standards development organizations.

Cross-Agency Themes

These actions reflect a coordinated approach within HHS, reinforced by the agency's AI strategy released in December 2025. The strategy outlines how HHS intends to integrate AI across departmental operations, with an emphasis on governance, responsible use, workforce readiness and operational efficiency.

Across HHS, several common priorities are emerging:

- auditability – the ability to understand and reconstruct how AI outputs are generated
- traceability of data sources, training methods and model versioning
- human oversight and interpretability, particularly in clinical and public health contexts
- ongoing performance monitoring, especially as models evolve over time



Strategic Outlook

Several trends are expected to shape the regulatory trajectory for AI in healthcare:

- **Continued State-Federal Divergence.** States are likely to remain active in the near term while federal policy evolves incrementally.
- **Increasing Separation Between Low- and High-Risk AI.** Lower-risk, consumer-facing tools will face lighter oversight, while clinical decision-making applications will be subject to greater scrutiny.
- **Persistent Gaps in Generative AI Policy.** Existing frameworks do not fully address newer use cases.
- **Continued Acceleration of Adoption.** AI is already embedded in key workflows, particularly in documentation and clinical support.

For ongoing updates on federal and state activity related to AI regulation, visit Holland & Knight's Health AI Navigator.

Shifting Telehealth Regulations

Telehealth Payment and Service Extensions

The Consolidated Appropriations Act of 2026 extended many of the Medicare telehealth flexibilities first adopted during the COVID-19 pandemic, offering greater certainty for providers and patients. Specifically, the law extends key Medicare telehealth waivers through December 31, 2027, including the removal of geographic restrictions, continued recognition of the patient's home as an originating site, expanded eligibility for a wide range of practitioners to furnish telehealth services, continued payment for audio-only visits, and flexibility around in-person requirements for behavioral and mental health services and hospice recertifications. The legislation also allows federally qualified health centers and rural health clinics to continue acting as distant site providers and extends the Acute Hospital Care at Home program through September 30, 2030. Additionally, the law directs CMS to create new billing codes or modifiers to better identify certain telehealth services, signaling increased oversight while preserving broad access to virtual care for several more years.

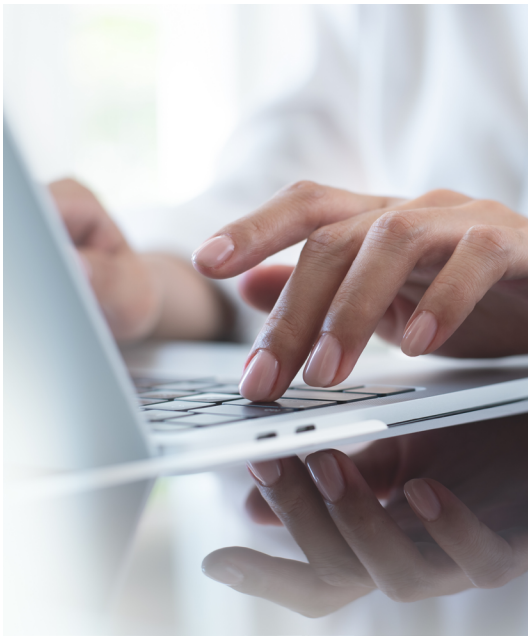
Similarly, the U.S. Drug Enforcement Administration (DEA), in coordination with HHS, issued a fourth temporary rule extending COVID-era telemedicine prescribing flexibilities for controlled substances through December 31, 2026, preventing a lapse that would have occurred at the end of 2025. The extension allows DEA-registered practitioners to continue prescribing Schedule II through Schedule V controlled substances via telemedicine without an initial in-person medical evaluation, preserving access to care for patients who rely on virtual treatment for behavioral health, substance use disorder, chronic pain and other conditions. DEA and HHS emphasized that the extension is intended to avoid a "telemedicine cliff" while the agencies complete their review of public comments and finalize permanent regulations designed to balance patient access with safeguards against diversion, giving providers additional time to prepare for future compliance requirements.

Telehealth Transaction Oversight

Across the country, states are increasingly recalibrating their telehealth frameworks to impose greater oversight on virtual care providers, particularly those operating at scale or backed by private equity. Though many pandemic-era access expansions have been preserved, legislatures and regulators are adding guardrails focused on licensing, prescribing practices, corporate ownership and quality-of-care standards. Recent state actions emphasize stricter enforcement of in-state licensure rules, clearer requirements for establishing a valid provider-patient relationship via telehealth, enhanced informed consent and patient identity verification obligations, and closer scrutiny of telemedicine prescribing, especially for controlled substances and high-risk services. These developments reflect a broader policy shift away from emergency flexibility toward permanent regulatory regimes designed to ensure that telehealth meets the same professional, ethical and consumer protection standards as in-person care while giving state medical boards and health agencies greater authority to supervise remote providers.

Most recently, Oregon's enactment of Senate Bill (SB) 951 represents one of the most aggressive state-level oversight measures affecting telehealth and digital health business models. Signed into law in June 2025, SB 951 significantly strengthens Oregon's corporate practice of medicine doctrine by sharply limiting the role of management services organizations (MSOs) and other non-licensed entities in owning, controlling or exerting de facto influence over medical practices, including those that furnish care via telemedicine. The law restricts MSO ownership interests, governance rights and contractual controls that could affect clinical, operational or financial decision-making, with phased compliance deadlines beginning January 1, 2026, for new entities and extending to 2029 for existing arrangements. Although SB 951 contains limited exceptions, it squarely targets private equity-backed and platform-based care models, signaling Oregon's intent to ensure that telehealth providers remain firmly under physician control and subject to heightened state oversight, a trend that other states are increasingly watching and, in some cases, beginning to emulate.

Data Security, Privacy and HIPAA Updates



Recent HIPAA Changes

As of February 16, 2026, covered entities were required to add certain language to their Health Insurance Portability and Accountability Act (HIPAA) notices of privacy practices dealing with substance use disorder records. The HHS Office for Civil Rights (OCR) issued updated model notices containing suggested language.

OCR, which is charged with enforcing the special federal protections for substance use disorder program records in 42 C.F.R. Part 2, recently added a new Part 2 breach reporting template on its website. If a Part 2 program experiences a breach of protected health information (PHI), it appears that the entity will have to submit two reports to OCR: the standard breach report and a Part 2 report.

Potential HIPAA Updates Coming

The following proposed changes to HIPAA could be finalized in 2026, according to the Office of Management and Budget:

- More than five years ago, OCR published proposed rules to promote coordinated care. The proposed regulatory changes were intended to make adjustments to HIPAA to reduce barriers that could impede a move to value-based healthcare. The proposed rules included several proposed changes relating to patients' rights to access their own PHI, reducing administrative burdens and facilitating certain information-sharing. The information blocking rules discussed in this publication contain requirements that sometimes appear to be in conflict with HIPAA, and the hope is that the final rules will help harmonize HIPAA and the interoperability requirements.
- The HIPAA Security Rule is more than two decades old and, in the view of many, well overdue for an upgrade. OCR issued proposed rules in January 2025 that, if finalized in their current form, would impose dramatic changes that could also be expensive and burdensome. For example, though current OCR guidance indicates that HIPAA covered entities are not responsible for the actions of their business associates, the proposed rules would require covered entities to exercise significant oversight and monitoring of their business associates' Security Rule compliance measures.

Increasing Pressure for De-Identified Data

The increasing demand for effective AI tools has increased the need for reliable data on which to train the tools. HIPAA allows PHI to be used and disclosed only for limited purposes, such as treatment, payment and healthcare operations, because using PHI to train AI tools is risky. Use of PHI for AI model development could also fall under HIPAA's broad definition of "research" and, thus, require written patient authorization or an institutional review board's waiver of the authorization requirement.

Once PHI is de-identified, HIPAA no longer applies. De-identification under HIPAA requires either the so-called "safe harbor method" or "expert determination method." Because the safe harbor method requires removal of at least 18 specific identifiers, including dates related to the individual, such as dates of treatment other than year, the safe harbor method often has limited utility. Finding qualified experts to opine on whether a data set is properly de-identified can be difficult, and we are finding that some purported expert determinations are expired or impose restrictions on the data set that may be difficult to follow.

Evolving State Privacy Laws

HIPAA preempts state privacy laws only if those laws conflict with HIPAA and provide fewer data protections or less patient access. Since the advent of the HIPAA Privacy Rule, there has been a patchwork of more stringent state privacy laws, but many states have renewed efforts to pass so-called "comprehensive" privacy laws designed to address health information. Many of these new laws carve out HIPAA covered entities or PHI. For digital health companies that are not subject to HIPAA, these laws significantly increase privacy-related regulatory complexity. There are also new laws that apply to HIPAA covered entities. For example, Florida and Texas have imposed new offshoring restrictions for certain patient data.

Interoperability and Accessibility

CMS Rules

The deadline for implementation of payer-side application programming interface (API) obligations related to prior authorizations is January 1, 2027. Most payers, other than employer-sponsored plans, are required to provide prior authorization information to patients and providers through updated API access. The objective is improved data sharing to reduce prior authorization delay and improper denials, reduce burden on healthcare providers, and provide transparency for patients and speedier access to care. Covered entities using the Fast Healthcare Interoperability Resources-based prior authorization process benefit from CMS enforcement discretion with regard to compliance reviews of HIPAA transaction standard violations. Acting CMS Administrator Amy Gleason kicked off an API-focused data exchange, the CMS Aligned Network, intended to further accelerate data sharing.

Information Blocking Enforcement

The HHS Assistant Secretary for Technology Policy is actively enforcing information-blocking complaints made against health IT developers through referral of cases of information blocking to the Office of Inspector General to pursue civil money penalties. Health IT developers are subject to penalties of up to $1 million per violation, and the regulation has no cap on penalties.

Cybersecurity Class Actions

In the last few years, hundreds of data security and privacy class actions and mass arbitrations have been filed around the country. Healthcare companies are frequent targets of such cases, and the statutory damages and other penalties sought by plaintiffs can be astronomical, even if there is no financial injury or other traditional harm. Claims are brought under a variety of statutes, including the Video Privacy Protection Act, state and federal wiretap acts, and state and federal consumer protection laws. Cases can also allege common-law violations such as invasion of privacy, breach of implied contract, unjust enrichment, breach of fiduciary duty or negligence.

Cases are often triggered by large data breaches. For example, if a HIPAA covered entity reports a breach involving 500 or more individuals to OCR, the incident is published on a public website by some federal and state authorities. Plaintiffs' attorneys can use that information to find potential defendants. Many plaintiffs' attorneys also file lawsuits based on common analytics and tracking technologies, including cookies and pixels, that run on a covered entity's public website and transmit a website visitor's IP address and other information to third parties that track online activity and website performance.

These types of litigation can be costly. Although some cases may be dismissed in preliminary stages, many class actions and mass arbitrations have settled for millions of dollars. Insurance carriers are increasingly reluctant to provide coverage for claims involving ad-tech and other tracking technologies. In addition, organizations may be subject to "nuisance" cases brought by a wave of small plaintiffs' firms or pro se plaintiffs who may have weak merits, but some organizations may feel compelled to repeatedly settle such cases to avoid potentially significant legal defense costs necessary to win on the merits of each case. Engaging in proactive measures to mitigate risk is critical in the current litigation environment.

Government Enforcement

The future of digital health hinges on three core pillars: clinical proof, operational integration and regulatory readiness. In an era of record False Claims Act (FCA) enforcement, with the U.S. Department of Justice (DOJ) recovering $5.7 billion from healthcare matters under the FCA in fiscal year 2025, companies that embed regulatory compliance as a strategic priority are better positioned to mitigate outsized liability risk, protect enterprise value and allow for sustainable growth. At the same time, these companies demonstrate strong governance and responsible stewardship of public and private funds.

Recent enforcement actions and investigations have targeted a wide range of digital health modalities, including telehealth and telemedicine services, remote patient monitoring, and electronic health record and other revenue optimization software.

Notably, however, DOJ scrutiny is not limited to cases in which digital health services are the primary focus of the alleged misconduct. As healthcare technology becomes increasingly integrated into clinical operations, billing and patient engagement, many DOJ matters now involve digital health tools as a critical component of the government's theories of liability – examining how the use, design or deployment of technology may have enabled, amplified or obscured the conduct at issue.

Examples of recent DOJ enforcement actions involving digital health include:

- **AI-Generated Fraudulent Patient Consents.** In 2025, the DOJ charged multiple defendants in the Northern District of Illinois in a $703 million scheme that used AI to create fake audio recordings of patients purportedly consenting to medical products.
- **Telehealth Scheme Uncovered via Proactive Data Analytics.** In late 2025, a federal grand jury indicted Done Global Inc., a digital health company that provided online diagnosis, treatment and refills of ADHD medication. The indictment alleges that Done Global illegally distributed more than 40 million pills of Adderall by exploiting telehealth. "Instead of leveraging technology to improve patient access to care and enhance communications, Done Global saw it as a way to boost profit," said one U.S. Attorney involved in the prosecution. Done Global's founder and CEO and clinical president were found guilty at trial.
- **Upcoding via Automated Billing Algorithms.** The DOJ secured several multimillion-dollar settlements under the FCA that relate to providers' use of automated software tools. In these investigations, the DOJ alleged that providers' automated billing and coding systems were designed to upcode claims to higher-complexity services than the services actually performed.

Healthcare organizations should establish AI governance committees, monitor technology performance, prioritize transparency, and align with emerging federal and state authorities and guidance. As enforcement risk continues to rise, companies that view compliance as an engine for durable growth will be better equipped to compete in an increasingly scrutinized healthcare marketplace.

About Holland & Knight's Digital Health Group

Holland & Knight's Digital Healthcare Group provides integrated legal counsel to healthcare providers, life sciences companies, digital health innovators and investors operating at the intersection of healthcare and technology. Drawing on a nationwide, multidisciplinary team of attorneys and advisors with deep experience in healthcare and life sciences, IP, data privacy and cybersecurity, regulatory compliance, transactions, litigation and public policy, the practice delivers forward-thinking solutions. This integrated approach enables clients to navigate rapidly evolving legal, regulatory and business challenges, as well as commercialize innovative technologies and manage risk in an industry increasingly utilizing and partnering with data, technology and software.

Authors

Mark H. Francis
Partner | New York
Data Strategy, Security & Privacy

Shannon Britton Hartsfield
Partner | Tallahassee
Data Strategy, Security & Privacy

Beth Neal Pitman
Partner | Birmingham
Healthcare Regulatory & Enforcement

Jessica R. Sievert
Partner | Jacksonville
Litigation

Dan Silverboard
Partner | Atlanta
Healthcare Regulatory & Enforcement

Shalyn Watkins
Senior Counsel | Newport Beach
Healthcare Regulatory & Enforcement

Sarah Starling Crossan
Senior Public Affairs Advisor | Washington, D.C.
Public Policy & Regulation

Holland & Knight

www.hklaw.com