

KIRKLAND & ELLIS

Kirkland Alert

2025 Healthcare Private Equity Outlook and Considerations

10 January 2025

As we move forward in 2025, stabilizing market and political conditions will likely continue to promote private equity investments throughout the healthcare sector. We expect continued investments to spur ongoing regulatory oversight and increased scrutiny. As discussed further in this outlook, we summarize the 2024 legal considerations affecting private equity in healthcare as well as potential 2025 forward-looking regulatory trends.

Trump's Second Term: Anticipated Healthcare Policy Shifts and Key Appointment

As the Trump administration begins its second term, significant changes in healthcare policy are anticipated. The administration is expected to focus on deregulation and a market-driven approach, reminiscent of Trump's previous term. Key appointments (subject to U.S. Senate advice and consent) include Robert F. Kennedy Jr. as Secretary of Health and Human Services, Dr. Mehmet Oz as Administrator of the Centers for Medicare and Medicaid Services, Dr. Jay Bhattacharya as Director of the National Institutes of Health, Dr. Marty Makary as Commissioner of the Food and Drug Administration, Dr. Janette Nesheiwat as Surgeon General, and Dave Weldon as Director of the Centers for Disease Control and Prevention.

Recent FTC Actions — Private Equity, Public Workshops and Expectations of the New Administration

The Federal Trade Commission's ("FTC") scrutiny of private equity's role in healthcare transactions may start to shift in 2025. Over the last several years, the FTC has focused on scrutinizing private equity, particularly in the healthcare sector. For

example, in March 2024, the FTC held a workshop on private equity in healthcare detailing its concerns with different private equity investment strategies. In May 2024, the FTC launched a joint public inquiry with the U.S. Department of Justice (“DOJ”) to identify private equity transactions and arrangements that may undermine competition.

As we look ahead with the new administration, changes in FTC leadership may influence current and future regulatory policies. Chair Khan’s formal term expired on September 25, 2024, and President-elect Trump selected Andrew Ferguson as the next FTC Chair. Nevertheless, any adjustments in the FTC’s regulatory focus may take time to implement.

State Regulators Ramp-Up Review of Healthcare Transactions

The applicability of state healthcare transaction review laws is a critical consideration for healthcare transactions including mergers, acquisitions, restructurings and certain debt arrangements.

Currently, 15 states have healthcare transaction review laws, each with unique requirements. Typically, these laws mandate the pre-closing submission of detailed filings to state attorneys general or regulatory agencies. Parties must wait for a notice period to expire or receive approval before closing the transaction. While most transactions are approved, some receive conditional approval, requiring adherence to ongoing requirements such as annual reporting and maintaining staffing levels. These reviews can significantly prolong transaction timelines, often by several months. Additionally, parties must submit substantial and potentially sensitive documents, which may become public.

As we approach 2025, more states are expected to consider these laws. Existing laws are also seeing increased scrutiny, with regulators expanding their interpretation of required information. For example, in December 2024, [Massachusetts passed](#), which was signed by Governor Healey on January 8, 2025, amendments to existing legislation which, among many things, broaden reporting requirements to include additional kinds of material change transactions, increase review periods, create new licensing requirements and expressly grant the ability to hold private equity investors liable for False Claims Act violations. Understanding the applicability of these laws is now a foundational issue in healthcare transactions.

CMS Updates

In 2024, the Centers for Medicare and Medicaid Services (“CMS”) continued to focus on increasing ownership transparency of institutional healthcare providers. This follows the requirement for disclosure of private equity or real estate investment trust entities with 5% or more ownership interest or managerial control over the provider. In addition, CMS revised Form CMS-855A to impose more robust ownership disclosure requirements on skilled nursing facilities (“SNFs”), which took effect on October 1, 2024. SNFs must now disclose all governing body members and additional disclosable parties, regardless of their ownership percentage, including those who exercise operational, financial, or managerial control or provide management or administrative services.

CMS also published a final rule on April 4, 2024 (the “Medicare Broker Compensation Final Rule”), eliminating administrative fees and capping commission-based Medicare broker compensation. A one-time \$100 increase was added to account for administrative expenses. Prior to this rule, agents and brokers were permitted to receive separate payments covering administrative fees based on fair market value rates, which were not subject to caps. On July 3, 2024, a federal court in Texas issued a stay on certain provisions of the Medicare Broker Compensation Final Rule, finding that CMS did not substantiate its decision to cap the fixed fee and include administrative fees.

Increased Scrutiny Over Corporate Ownership/Investment in Healthcare

Following federal and state trends of heightened scrutiny over corporate involvement in healthcare, certain states are reexamining the scope of their prohibitions against the corporate practice of learned professions (“Corporate Practice”).

Although not present in every state, the Corporate Practice doctrine mandates that only licensed healthcare professionals (e.g., physicians, dentists, optometrists, nurses, etc.), or entities wholly owned by licensed professionals, may practice clinical professions, or employ other licensed healthcare professionals. To comply with the Corporate Practice doctrine, private equity companies enter a series of contractual relationships with an entity owned by a licensed healthcare professional, commonly known as the “Friendly PC” model. Despite widespread use of this model, recent litigation has focused on its permissibility, which could create regulatory headwinds at the state level.

For example, in one California case, a physician owner claimed that its management services organization (“MSO”) mismanaged the practice’s business operations and improperly transferred the practice to a new physician after the physician owner refused to fire certain clinical personnel. The court found that the MSO had violated California’s Corporate Practice prohibition, unwound the MSO’s transfer of the practice and returned ownership to the physician owner. Another example includes a California court finding that a stock transfer agreement violated Corporate Practice because the agreement provided a non-licensed provider unrestricted ability to control ownership of a practice.

Fraud & Abuse Developments

The DOJ and its law enforcement partners continue to target pharmaceutical, payor, laboratory and behavior treatment businesses. These business segments will likely remain key enforcement areas in 2025. Increased healthcare spending underscores the DOJ’s efforts, particularly within the Medicare Advantage program. As government healthcare programs grow, regulators and enforcement professionals are increasingly employing data analytics to identify and investigate aberrant billing practices or financial patterns. Additionally, regulators are expanding incentives for whistleblowers or co-conspirators to come forward with information relating to alleged fraud. We expect increased civil investigative demand activity, more highly publicized and marquee investigations, and potentially more prosecutions as regulators seek to amplify their message of deterrence.

In addition, we expect the 2025 enforcement trends to mirror those of 2024. For instance, by July 2024, the DOJ charged more than 200 defendants in connection with alleged schemes to commit \$2.7 billion in healthcare fraud. Notable actions by the DOJ included:

- Charging an Arizona couple in an alleged \$900 million scheme to induce Medicare recipients to receive unnecessary amniotic allografts,
- Convicting a Houston man of a \$160 million Medicare fraud scheme involving fraudulent billing of expensive topical creams, and
- Settling with a pharmaceutical company for \$425 million to resolve allegations of kickbacks via co-pay assistance foundations controlled by the pharmaceutical company.

Health Data Privacy and Security

Health data privacy and security will remain top regulatory priorities in 2025. While states continue to develop patchwork solutions through assorted new legislation, federal agencies are taking a more coordinated approach with respect to rulemaking, guidance, and enforcement of existing laws and regulations. In the coming year, the healthcare industry must navigate an ever-evolving regulatory landscape while implementing security measures to protect patient data from sophisticated threats.

Major Health Data Breaches and Health Data Enforcement Trends

Several notable health data breaches occurred in 2024. The U.S. Department of Health and Human Services (“HHS”) has referred to healthcare organizations as a “one-stop shop” for hackers seeking identity, financial and health information. The HHS Office for Civil Rights (“OCR”) is currently investigating more than 450 HIPAA data breaches from 2024 alone, each impacting at least 500 people.

There were multiple breaches in 2024 including a ransomware attack on one of the largest processors of health data in the U.S. The attack caused outages across the healthcare sector, affected about 1 in 3 Americans and resulted in reported losses of almost \$2.5 billion.

In addition to HIPAA breaches, the FTC also took action against unauthorized disclosures of consumer health data by entities not subject to HIPAA, such as consumer health apps. For instance, in April 2024, an online mental healthcare company agreed to an FTC order restricting its uses and disclosures of consumer data after allegedly misleading consumers about its data sharing and security practices.

We expect that 2025 will likely see more breaches affecting the healthcare sector, prompting increased regulatory oversight and public scrutiny. Organizations that invest in strong security measures and rapid incident response protocols will be better positioned to protect patient data and mitigate potential financial and reputational damage.

Cybersecurity and Health Data

As breaches of sensitive health data continue to increase, we expect several new regulatory developments and expanded enforcement of health data privacy laws and regulations. Federal agencies refined their cybersecurity guidance in 2024 (into early 2025), as the OCR [published a proposed rule](#) and the National Institute of Standards

and Technology (“NIST”) issued an updated cybersecurity framework to help organizations reduce cybersecurity risk and manage cybersecurity threats and HIPAA compliance efforts.

The U.S. Food and Drug Administration (“FDA”) is also increasingly focused on medical device security, implementing new requirements for “cyber devices” under Section 524B of the Federal Food, Drug, & Cosmetic Act (“FD&C Act”). Manufacturers must demonstrate robust cybersecurity requirements in their premarket submissions, as noncompliance carries the risk of potential prosecution.

At the state level, New York broke new ground as the first state to mandate specific cybersecurity requirements for hospitals. This state law may serve as a harbinger for future state cybersecurity regulation.

Health Data Privacy Developments

After a year that brought significant cybersecurity incidents, we expect new developments with respect to the privacy of health information. Specifically, we expect to gain a clearer picture of how OCR will enforce its rules finalized in 2024, including the final rule that aligned substance use disorder patient records regulations with HIPAA and the HIPAA Privacy Rule to Support Reproductive Health Care Privacy. As the incoming administration may take a different approach to enforcement of these new requirements, we expect such rules to continue to evolve in the new year.

Online Tracking Technologies

A shift in online tracking technology regulation occurred in June 2024, when a Texas federal court ruled that metadata from public-facing “unauthenticated” hospital websites (e.g., websites that do not require a login from visitors) does not constitute protected health information (“PHI”) under HIPAA. However, the ruling indicated that HIPAA rules and the [FTC Health Breach Notification Rule](#) (“HBNR”) still apply to authenticated websites (e.g., websites requiring a login) like patient portals, leaving such websites open to ongoing regulatory scrutiny and legal exposure. This ruling comes as online tracking technologies have been a growing enforcement consideration for OCR and the FTC and have led to several plaintiff settlements.

Artificial Intelligence Considerations in the Healthcare Industry

The use of AI tools in healthcare continues to receive increased scrutiny across multiple fronts. Federal agencies are developing comprehensive governance frameworks in response to the 2023 White House AI Executive Order. Agencies have increasingly shown an interest in monitoring the use of AI tools in health insurance coverage determinations, the inappropriate use of consumer data in training AI models and discrimination resulting from care decision-making tools. The FDA has been focusing on AI's role in drug development and clinical decision support, and we also expect the agency to develop and publish AI best practices as it has discussed. At the same time, state laws continue to develop independently, adding additional complexity to the AI regulatory framework.

Healthcare organizations are now expected to establish clear AI policies. As the landscape continues to shift, developers and deployers of AI tools in the healthcare sector are increasingly considering AI policies concerning ethics and bias; fraud, waste and abuse; patient safety and malpractice concerns; and privacy.

Looking Ahead: Regulatory Overview and Outlook for Laboratory Developed Tests and Pharmacy Benefit Managers

The landscape for laboratory developed tests ("LDTs") has evolved rapidly over the last year. On May 6, 2024, the FDA announced its highly anticipated final rule concerning LDTs, categorizing them as regulated in vitro diagnostic products ("IVDs"). This regulation marks a significant shift in oversight, as the FDA ended its long-standing enforcement discretion over LDTs. Now, manufacturers of LDTs will be required to comply with the same regulatory provisions and approval frameworks that apply to traditional medical devices. This transition will occur over a four-year phase-in period, starting with the new rule that took effect on July 5, 2024. The multiyear phase-in compliance requirements allow continued patient access to LDTs as companies prepare for enhanced regulation.

This recent regulatory shift for LDTs intensifies existing industry concerns. The FDA's new rule faces several legal challenges from multiple industry organizations, questioning the agency's authority to regulate LDTs. These lawsuits argue that the FDA has improperly expanded the definition of "devices" and contend that LDTs should be considered intangible services rather than medical devices. In addition, LDT manufacturers must now navigate increased scrutiny regarding cybersecurity vulnerabilities, as more sophisticated LDTs may fall under the FDA's definition of "cyber devices." This requirement for LDTs suggests a broader regulatory trend that

emphasizes cybersecurity issues within the medical device sector, which is anticipated to be a priority in the new Trump administration.

In addition, we expect pharmacy benefit managers (“PBMs”) to continue to be a priority for governmental and administrative reform. In December 2024, Congress attempted to pass legislation to require PBMs to disclose their compensation to increase transparency, among other items, but this effort failed.

Contributions to this article were made by the Kirkland & Ellis Healthcare Team.

Authors

Lindsay M. Borgeson

Partner / New York

Anthony M. Del Rio

Partner / Chicago

Kate Hardey

Partner / Washington, D.C.

Robert Kantrowitz

Partner / New York

Kelly Kluka

Partner / Chicago

William S. Richmond

Partner / Washington, D.C.

Olivia Vanessa Seraphim

Partner / Washington, D.C.

Dennis Williams

Partner / New York

Related Services

Practices

- Healthcare & Life Sciences Transactions
- Transactional
- Healthcare & Life Sciences Regulatory

Suggested Reading

- 14 January 2025 Kirkland Alert Massachusetts Expands Review of Private Equity Investments in Healthcare
- 06 January 2025 Kirkland Alert OCR Proposes Changes to the HIPAA Security Rule
- 14 November 2024 Kirkland Alert New HSR Rules Are Effective February 10, 2025

This publication is distributed with the understanding that the author, publisher and distributor of this communication are not rendering legal, accounting, or other professional advice or opinions on specific facts or matters and, accordingly, assume no liability whatsoever in connection with its use. Pursuant to applicable rules of professional conduct, this communication may constitute Attorney Advertising.

© 2025 Kirkland & Ellis LLP.