Artificial Intelligence and What It Means for Healthcare Provider Compliance

Michael T. Batt is an attorney at Hall, Render, Killian, Heath & Lyman, P.C., where he assists healthcare providers with solutions to the challenges associated with implementing, managing, and interconnecting health information technology.

Brandon C. Helms is a shareholder at Hall, Render, Killian, Heath & Lyman, P.C. and assists clients in conducting internal investigations, drafting self-disclosures, responding to subpoenas, and defending against federal investigations and litigations.

Kaitlin A. Nucci is an attorney and advisor at Hall, Render, Killian, Heath & Lyman, P.C., where she focuses her practice on regulatory compliance, reimbursement, and managed care matters.

Michael T. Batt / Brandon C. Helms / Kaitlin A. Nucci

Artificial intelligence ("AI") refers to a class of technology tools that perform tasks mimicking human intelligence. AI is distinguished from traditional computing in that while traditional computing functions based on a set of written instructions, AI functions based on correlation and predictive analysis extrapolated from training data. Although AI may seem familiar to users, it presents new and unique risks to healthcare providers, and requires compliance professionals to carefully consider how the technology impacts their organization and compliance plan. This article will discuss the various technology and compliance related considerations that healthcare organizations should evaluate as AI is integrated into their systems.

As a technology, AI tools must be evaluated for all of the traditional IT concerns, including security, data privacy, and interoperability, among others. AI tools must be reviewed at the time of initial implementation to understand the accuracy of the tool as well as what data elements were available at the time of training that could potentially impact the accuracy of the result or amplify a historic bias. Additionally, AI has the ability to "learn," or modify itself so that as it receives direction from users it can adjust its output, often referred to as becoming "smarter". This means that AI tools must be continually observed to monitor for accuracy and to identify "drift" that may compromise the accuracy or magnify discriminatory bias.[1]

For purposes of compliance, in addition to all of the traditional technology concerns, AI presents some novel challenges:

1. AI tools look and feel a lot like traditional computing, however, they can introduce new concerns regarding accuracy of the output. The users must be educated and informed regarding what systems utilize AI in order for workforce members to reasonably anticipate errors or hallucinations, where

AI generates incorrect or misleading information.

2. Some AI tools are achieving diagnosis accuracy that is higher than humans. Notwithstanding this accuracy, the U.S. health system and associated reimbursement mechanisms contemplate that a human is always engaged in making treatment decisions. AI tools may not be deployed in a manner that replaces or automates a task that is required to be performed by a human. This means consideration must be given to each use case of AI to determine whether use of AI to augment or replace human decision-making is permissible.
3. The independence and autonomy of healthcare providers must be maintained. When leveraging AI to replace or create efficiency in human tasks, consideration must be given to whether sufficient resources are available that would permit the human to identify and correct errors or hallucinations of AI. Workflows, resources, and compensation arrangements must not impermissibly disincentivize or remove healthcare provider discretion or override the provider's professional judgment.
4. AI tools consume significant amounts of data, which can lead to data privacy concerns. AI models often analyze more data elements with respect to decision making than traditional computing, and retain the data for training and additional product development purposes. The AI tools themselves may be built on a technology stack that leverages multiple layers of subcontractors, each of who may require access to data and the right to retain data for further development purposes, significantly complicating compliance with data privacy laws. Additionally, AI tools may be introduced as a new product or service, or as an update or upgrade to existing technology, circumventing procurement and security vetting processes. AI tools and their associated data privacy and security concerns represent a significant challenge to existing data privacy and security procedures.

False Claims Act Risk

Of the myriad risks for healthcare companies using AI tools, the potential violation of the False Claims Act ("FCA")[2] has to rank near the top. There are three elements of any FCA violation: (1) a false claim, (2) knowingly presented to the government, and (3) the misrepresentation is material to the government's decision to pay.[3] While these concepts are well understood, their application to AI tools presents new wrinkles.

Take, for example, an AI coding software that reviews medical records and then selects HCPCS codes or diagnoses to be used for claims for payment. In this scenario, the introduction of AI has little impact on how OIG or DOJ would prove the first and third elements (falsity and materiality). OIG or DOJ would prove falsity by reviewing a sample of medical charts to determine whether the documentation supported the diagnoses or procedure codes at issue. Similarly for materiality, the government routinely requires refunds or brings enforcement actions when higher-reimbursing HCPCS codes, or risk-adjusting diagnosis codes for Part C plans, are not supported by documentation.[4]

Where things get trickier is the knowledge element: did someone submit false claims to the government knowing they were false?[5] If a provider only recently started using new AI coding software and had no way of knowing or suspecting that the coding software was upcoding HCPCS codes or diagnoses, it would be difficult for OIG or DOJ to prove that someone at the organization had knowledge that they were submitting false claims. On the other hand, if after several months of

implementing a new AI coding software, the provider's use of higher-reimbursing HCPCS codes suddenly skyrocketed, and a subsequent chart review established a high percentage of unsubstantiated claims, OIG or DOJ would likely argue that the provider acted with reckless disregard or deliberate ignorance that its claims were false.

Recent examples of FCA cases demonstrate that the risk here is concrete rather than theoretical. In the Northern District of California, a large Medicare Advantage Organization ("MAO") and its associated medical groups are litigating a *qui tam* action in which the government intervened and alleged that the MAO used data mining algorithms to identify missed diagnoses that the MAO used to falsely increase risk adjustment scores.[6] Likewise in California's Central District, the largest MAO in the country is litigating a *qui tam* action in which the government intervened; while the case does not appear to involve the use of AI tools, the government alleges that the defendants used third-party coding vendors to falsely increase risk scores.[7] In the near future, the third-party coding vendor will be replaced with coding software.

While these current cases focus on inflated Part C risk adjustment scores, as AI coding tools and other billing software proliferate, it is only a matter of time before FCA investigations and lawsuits expand to cover those new tools. Healthcare providers must be aware of the risks before they find themselves in the government's crosshairs.

Compliance for AI Tools

As providers increasingly integrate AI into clinical and operational processes, the need for a clear, actionable compliance framework has never been more urgent. When used as a supplemental tool, AI can be used to improve quality of care, clinical decision-making, efficiency, business and operational decision-making. But along with these opportunities comes the potential for significant risk. This potential for risk demands that organizations find new ways to integrate and monitor the compliance risks associated with the use of AI.

In September 2024, the criminal division of the U.S. Department of Justice ("DOJ"), issued an updated Evaluation of Corporation Compliance Programs,[8] which emphasizes the importance of managing emerging risks associated with new technologies such as AI. This guidance underscores the expectation that healthcare organizations proactively incorporate AI into their existing compliance programs—not as a standalone effort, but as an integrated component of broader governance and compliance management strategies.

The DOJ's focus on emerging technologies such as AI signals increased regulatory scrutiny. If a provider fails to govern the use of AI tools—whether in diagnostics, billing, patient communication, or clinical research—it could face liability under existing laws, from fraud and abuse to data privacy and security. The DOJ has made it clear that "willful blindness" to technological risks is no longer acceptable. Healthcare leaders must be able to demonstrate that their organizations are actively identifying and mitigating AI-related risks.

As AI tools proliferate, there is a growing need to ensure all stakeholders understand and participate in the AI approval process, as well as continuous monitoring of this technology. This is not merely an IT or research issue; AI can touch nearly every corner of a healthcare organization, including:

- **Clinical departments**, where AI may be used for diagnostics or treatment planning;
- **Research and clinical trials**, where AI plays a role in data analysis and protocol development;
- **Finance and revenue cycle**, where automation can impact coding, billing, and reimbursement;

- **Compliance and legal**, which oversee regulatory risk, as well as policy development and enforcement;
- **Data privacy and IT security**, given the sensitive data processed by AI systems.

Each of these departments needs to be asking, "What AI tools are we using? Are they approved? Are we managing risk appropriately?"

The good news is that compliance professionals do not need to reinvent the wheel. The seven elements of an effective compliance program outlined in the Office of Inspector General's ("OIG") 2023 General Compliance Program Guidance[9]—already familiar to most healthcare organizations—can be adapted to encompass AI governance. These include:

- **Written policies and procedures** that prescribe appropriate AI use and the procedures that must be followed before implementing any AI use;
- **Leadership oversight** through an AI governance committee or working group and an AI representative on the compliance committee;
- **Training and education** to ensure all employees, including physicians, understand appropriate uses of AI;
- **Effective lines of communication with the Compliance Officer** to ensure entity personnel are comfortable raising AI-related compliance questions and concerns;
- **Enforcing standards** for concerns or potential misuse of AI, as well as potential noncompliance with policies, procedures, and processes;
- **Risk assessment, auditing, and monitoring** to ensure AI tools are implemented and used in alignment with organizational standards, including destruction policies;
- **Response and prevention** strategies to correct and prevent future misuse.

This integrated approach ensures that AI compliance is not siloed but embedded in the organization's operational DNA. Healthcare organizations should also consider establishing an AI Governance Committee, with legal and compliance representatives participating as a dedicated resource and strategic partners to compliantly integrate AI use. This approach is designed to provide visibility and accountability, helping the organization manage AI risk while also encouraging innovation. Compliance should focus on partnering with, and not patrolling, the departments using AI. This approach is designed to gain the trust of key stakeholders who are involved in AI vetting, integration, and evaluation.

The integration of AI into healthcare is no longer a future challenge—it is a present reality. Each organization's compliance strategy must evolve in tandem. AI is a powerful tool for leveraging workforce members, but AI can also accelerate and expand potential compliance risks. While new risks are emerging, providers should already have much of the structure needed in place. The key is alignment: ensuring that AI governance is not treated as a separate initiative, but as part of the organization's ongoing commitment to compliance, quality, and patient safety.

AI governance is about constructing a process to engage stakeholders in understanding AI and its associated risks so that they can make informed decisions. Because of the impact on the workforce, the governance must consider both the technology and the impact the technology may have on the workforce that is using it. Healthcare organizations must also prioritize, study, understand, and control how humans will interact with, authorize, and take action at the direction of AI. An effective compliance program that integrates AI governance will allow healthcare organizations to minimize its associated risk, as well as appropriately and efficiently respond if something goes wrong.

Endnotes

1. *See* U.S. Dep't of Commerce, National Institute of Standards & Technology, AI Risk Management Framework (Jan. 2023), available at *https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf*.
2. *See* 31 U.S.C. §§ 3729–3733.
3. *See* 31 U.S.C. § 3729(a)(1)–(b); U.S. *ex rel*. Schutte v. SuperValu Inc., 598 U.S. 739, 747 (2023); United Health Servs., Inc. v. United States *ex rel*. Escobar, 579 U.S. 176, 187 (2016).
4. *See, e.g.*, Press Release No. 25-302, U.S. Dep't. of Justice, *Medicare Advantage Provider Seoul Medical Group and Related Parties to Pay over $62M to Settle False Claims Act Suit*, (Mar. 26, 2025), available at *https://www.justice.gov/opa/pr/medicare-advantage-provider-seoul-medical-group-and-related-parties-pay-over-62m-settle* (detailing settlement related to a Medicare Advantage provider using false diagnoses for spinal conditions to inflate risk adjustment payments); Press Release No. 24-203, U.S. Dep't. Justice, *False Claims Act Settlements and Judgments Exceed $2.68 Billion in Fiscal Year 2023* (Feb. 22, 2024), available at *https://www.justice.gov/archives/opa/pr/false-claims-act-settlements-and-judgments-exceed-268-billion-fiscal-year-2023* (providing a review of 2023 FCA settlements involving inflated Part C risk scores due to unsupported diagnoses).
5. Knowing means actual knowledge, deliberate ignorance of the truth or falsity of the information, or reckless disregard of the truth or falsity of the information. *See* § 3729(b)(1)(A).
6. *See* United States *ex rel*. Osinek v. Kaiser Permanente, No. 3:13-cv-03891-EMC (N.D. Cal.)
7. *See* United States *ex rel*. Poehling v. United Health Group, Inc., No. 2:16-cv-08697-FMO-PVC (C.D. Cal.).
8. *See* U.S. Dep't of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs* (Sept. 2024), available at *https://www.justice.gov/criminal/criminal-fraud/page/file/937501/download*.
9. U.S. Dep't. of Health and Human Servs., Office of Inspector General, General Compliance Program Guidance (Nov. 6, 2023), available at *https://oig.hhs.gov/documents/compliance-guidance/1135/HHS-OIG-GCPG-2023.pdf*.

Reprinted from Journal of Health Care Compliance, Volume 27, Number 4, July–August 2025, pages 5-8, 46, with permission from CCH and Wolters Kluwer.
For permission to reprint, e-mail permissions@cch.com.