CLIENT ALERTS & INSIGHTS

Navigating Legal Liability in AI Adoption: What Healthcare Executives Need to Know

JANUARY 29, 2025

Authors: Kathrin “Kat” Zaki, Nicholas Adamson

The adoption of artificial intelligence (AI) in healthcare has ushered in a new era of innovation that is transforming diagnostics, treatment planning and operational efficiencies. However, with great potential comes significant legal and ethical responsibilities. For healthcare executives, understanding the unique inherent risks associated with AI adoption is critical to leveraging its benefits while avoiding potential liabilities. Here’s what you need to know about AI in healthcare, the legal risks involved and strategies to mitigate these challenges.

I. AI Uses in Healthcare, Legal Risks and Liability Issues

AI adoption in many industries is still in its infancy, however, implementation in healthcare has been swift. In general terms, usage of AI in healthcare can be divided into two broad categories: clinical implementations and non-clinical implementations. Some current clinical uses of AI in the marketplace include lab reading technologies, drug trial administration, creation of initial risk assessments and technologies assisting with developing patient-specific care plans. Current non-clinical AI uses in healthcare include predictive language clinical note taking, patient visit write-ups, billing and coding technologies, and patient research technologies.

All of these implementations of AI carry unique risk factors, but below are some broad liability concerns all providers should consider.

Malpractice and Regulatory Compliance

Malpractice liability relating to AI largely arises in the context of using clinical or diagnostic AI software. While it is likely that AI could bear some liability risk in the malpractice and clinical context, more of this risk will undoubtedly fall on providers. At the end of the day, licensed providers will be the ones responsible for their implementation and oversight of AI and will be the only party in privity of contract with patients who may experience ineffective treatment consequent to AI usage.

Administrative and Non-clinical Regulatory Risks

While non-clinical AI uses carry less risk from a patient care standpoint, such uses could still invoke regulatory scrutiny. For example, if multiple hospital systems in one small area use the same AI tool to generate off the rack pricing, the AI tool might inadvertently function to price fix the costs of services in that area which would violate antitrust laws. Antikickback concerns are also abundant here given that AI assisted billing and coding impacts what is submitted to federal and state payors, which can give rise to liability if the billing contains errors of any kind. As such, providers need to understand to what extent their contracted vendors are leveraging AI technologies in order to effectively contract around these risks.

Data Privacy and Vendor Accountability

Data usage is an especially high-risk aspect of AI technologies. As discussed below, AI trains itself using data inputs provided from its clients. As such, if multiple healthcare systems are using the same AI technology, there is a chance that the underlying data is being passed to other providers using that technology, even if the data isn't immediately apparent on a first glance. As such, it is important to hold AI vendors accountable for keeping data separate and not using it to train models used in other practices. It is also important to use bespoke contractual tools and language to address these unique privacy concerns to avoid inadvertent PHI or other business information disclosure.

II. Mitigating AI Risks: A Strategic Approach

Addressing the risks of AI in healthcare requires a strategic focus on data governance, compliance, oversight, education and vendor management.

Data Governance

Preventing bias through data governance is a critical first step. AI models must be trained on diverse and representative datasets to avoid reinforcing systemic inequalities. Organizations should regularly audit their AI tools to ensure they deliver equitable outcomes across all patient demographics. Establishing cross-functional AI committees can provide valuable oversight, helping to identify blind spots and address potential issues before they lead to harm.

Regulatory Compliance Framework

Compliance with regulatory requirements is another cornerstone of risk management. Organizations must navigate the complex landscape of federal and state laws governing AI use. Staying aligned with HIPAA regulations is essential, particularly in managing how protected health information (PHI) is processed or stored by AI tools. With new proposed state laws, such as those in Utah, Illinois and Colorado, requiring disclosure of AI use, healthcare executives must proactively adopt practices that promote transparency and secure proper consent.

By adopting well-recognized frameworks such as the NIST AI Risk Management Framework or ISO standards, organizations can promote responsible AI use. Governance policies should be clear and tailored to the needs of the organization, whether applied enterprise-wide or to specific departments. Senior leaders must play an active role in overseeing AI initiatives, ensuring that policies are implemented effectively and adjusted as technologies and regulations evolve.

Education and Training

Education and training are equally important in mitigating AI risks. Employees and stakeholders need a clear understanding of AI's capabilities, limitations and ethical considerations to adequately safeguard information funneled through AI systems. This requires ongoing education tailored to the roles and responsibilities of staff. Tools that pose higher risks (e.g. diagnostic AI tools, AI notetaking tools for patient intake, etc.) should be accompanied by specialized training to ensure that users can identify and mitigate potential issues in their workflows.

Vendor Quality and Management

Selecting and managing vendor relationships is another area that demands careful attention. AI tools often come from third-party vendors, and organizations must thoroughly assess these tools to ensure they meet industry standards of safety, validity and fairness. Ideally, vendors should possess appropriate security certifications, such as SOC 2 or ISO 27001, to ensure robust data protection. Contracts with vendors should include clear terms for data usage, compliance with laws and routine monitoring. To safeguard against potential failures, agreements should also include provisions for incident response and termination in the event of non-compliance or poor performance.

By integrating these strategies into their operations, healthcare organizations can mitigate the risks associated with AI, setting the stage for a more trustworthy and effective deployment of this transformative technology.

III. Top Takeaways for Healthcare Executives:

1. ***Ensure Regulatory Compliance and Clinical Oversight:*** Stay updated on HIPAA, FDA and emerging state laws, and form cross-functional teams for oversight and accountability; in addition, ensure all clinical AI uses have provider oversight that is well documented.

2. ***Demand Transparency from Vendors:*** Be aware of what AI tools every vendor uses and require thorough documentation, indemnification and audit rights when negotiating vendor agreements. Ensure that BAAs and other privacy tools are tailored to the unique concerns of AI learning.

3. ***Prepare for Incidents:*** Regularly evaluate AI tools for performance and compliance, and develop a comprehensive process for addressing data breaches and model errors.

4. ***Invest in Training:*** Educate teams on safe and effective AI usage, including development of AI Use Policies and Procedures.

5. ***Prioritize Patient Trust:*** Be transparent about AI usage and its benefits for patient care, and ensure patients have the ability to opt in or out of AI use wherever possible.