


AI Law and Policy

Legal Considerations Involving Artificial Intelligence

Key Considerations Before Negotiating Healthcare AI Vendor Contracts



By Kathleen O'Neill, Carolyn Metnick, John Golembesky & Carolyn Young on March 24, 2025

 Listen to this post

The integration of artificial intelligence (AI) tools in healthcare is revolutionizing the industry, bringing efficiencies to the practice of medicine and benefits to patients. However, the negotiation of third-party AI tools requires a nuanced understanding of the tool's application, implementation, risk and the contractual pressure points. Before entering the negotiation room, consider the following key insights:

I. The Expanding Role of AI in Healthcare

AI's role in healthcare is rapidly expanding, offering a wide range of applications including real-time patient monitoring, streamlined clinical note-taking, evidence-based treatment recommendations, and population health management. Moreover, AI is transforming healthcare operations by automating staff tasks, optimizing operational and administrative processes, and providing guidance in surgical care. These technological advancements can not only improve efficiency but also enhance the quality of care provided. AI-driven customer support tools are also enhancing patient experiences by offering timely responses and personalized interactions. Even in employment recruiting, AI is being leveraged to identify and attract top talent in the healthcare sector.

With such a wide array of applications, it is crucial for stakeholders to understand the specific AI service offering when negotiating a vendor contract and implementing the new technology. This knowledge ensures that the selected AI solution aligns with the organization's goals and can be effectively integrated into existing systems, while minimizing each party's risk.

II. Pre-Negotiation Strategies

Healthcare AI arrangements are complex, often involving novel technologies and products, a wide range of possible applications, important data use and privacy considerations and the potential to significantly impact patient care and patient satisfaction. Further, the regulatory landscape is developing and can be expected to evolve significantly in the coming years. Vendors and customers should consider the following when approaching a negotiation:

Vendor Considerations:

1. **Conduct a Comprehensive Assessment:** Understand the problem the product is addressing, expected users, scope, proposed solutions, data involved, potential evolution, and risk level.
2. **Engage Stakeholders:** Schedule kick-off calls with the customer's privacy, IT, compliance, and clinical or administrative teams.
3. **Documentation:** Maintain summary documentation detailing model overview, value proposition, processing activities, and privacy/security controls.

4. **Collaborate with Sales:** Develop strategies with the sales team and consider trial periods or pilot programs. Plan for the progression of these programs. For example, even if a pilot program is free, data usage terms should still apply.

Customer Considerations:

1. **Evaluate Within AI Governance Scope:** Don't treat an AI contract like a normal tech engagement. Instead, approach this arrangement within a larger AI governance scope, including accounting for the introduction of ethical frameworks, data governance practices, monitoring and evaluation systems, and related guardrails to work in tandem with the product's applications.
2. **Engage Stakeholders:** Collaborate with legal, privacy, IT, compliance, and other relevant stakeholders from the outset.
3. **Consider AI-Specific Contracts:** Use AI-specific riders or MSAs and review standard vendor forms to streamline negotiations.
4. **Assess Upstream Contract Requirements:** Ensure upstream requirements can be appropriately reflected downstream.
5. **Perform vendor due diligence:** As with any nascent industry, some vendors will not survive or may significantly change their focus or products, which might impact support or the long-term viability of the service. Learn about your vendor and ask questions about their financial stability, privacy and security posture.

III. AI Governance and Risk Assessment

Evaluating AI-related risk requires understanding risk across the full lifecycle of an AI product, including its model architecture, training methods, data types, model access, and specific application context. In the healthcare space, this includes understanding the impact to operations, the effect on clinical care and any other impact to patients, the amount of sensitive information involved, and the degree of visibility and/or control the organization has over the model.^[1] For example, the risk is much larger with respect to AI that is used to assist clinical decision-making for diagnostics (e.g., assessing static imaging in radiology); whereas, technology used for limited administrative purposes carries a comparatively smaller risk. Here are three resources that healthcare organizations can use to evaluate and address AI-related risks:

A. HEAT Map

A HEAT map can be a helpful tool for evaluating the severity of risks associated with AI systems. It categorizes risks into different “heat” levels (e.g., informational, low, medium, high, and critical). This high-level visual representation can be particularly helpful when a healthcare organization is initially deciding whether to engage a vendor for a new AI product or platform. It can help the organization identify the risk associated with rolling out a given product and prioritize risk management strategies if it moves forward in negotiating an agreement with that vendor.

For example, both the customer and the vendor might consider (and categorize within the HEAT map) what data the vendor will require to perform its services, why the vendor needs it, who will receive the data, and what data rights the vendor might be asking for, how that data is categorized, whether any federal, state or global rules impact the acceptance of that data, and what mitigations are necessary to account for data privacy.

B. NIST AI Risk Management Framework

The National Institute of Standards and Technology (NIST) has created the NIST AI Risk Management Framework to guide organizations in identifying and managing AI-related risks.^[2] This framework offers an example of a risk tiering system that can be used to understand and assess the risk profile of a given AI product, and ultimately guide organizations in the creation of risk policies and protocols, evaluation of ongoing AI rollouts, and resolution of any issues that arise. Whether healthcare organizations choose to adopt this risk tiering approach or apply their own, this framework reminds organizations of the many tools at their disposal to manage risk during the rollout of an AI tool, including data protection and retention policies, education of users, incident response protocols, auditing and assessment practices, changes to management controls, secure software development practices, and stakeholder engagement.

C. Attestations and Certifications

Attestations and certificates (e.g., HITRUST, ISO 27001, SOC-2) can also help your organization ensure compliance with industry standard security and data protection practices. Specifically, HITRUST focuses on compliance with healthcare data protection standards, reducing the risk of breaches and ensuring AI systems that handle health data

are secure; ISO 27001 provides a framework for managing information security, helping organizations to safeguard AI data against unauthorized access and breaches; and SOC-2 assesses and verifies a service organization's controls related to security, availability, processing integrity, confidentiality, and privacy, in order to ensure AI services are trustworthy. By engaging in the process to meet these certification standards, the organization will be better equipped to issue-spot potential problems and implement corrective measures. Also, these certifications can demonstrate to the public that the organization takes AI risks seriously, thereby strengthening trust and credibility amongst its patients and business partners.

IV. Contract Considerations

Once parties have assessed their organizational needs, engaged applicable stakeholders/ collaborators, and reviewed their risk exposure from an AI governance perspective, they can move forward in negotiating the specific terms of the agreement. Here's a high-level checklist of the terms and conditions that each party will want to pay careful attention to in negotiations, along with a deeper dive into the considerations surrounding data use and intellectual property (IP) issues:

A. Key Contracting Provisions:

- Third-party terms
- Privacy and security
- Data rights
- Performance and IP warranties
- Service level agreements (SLAs)
- Regulatory compliance
- Indemnification (IP infringement, data breaches, etc.)
- Limitations of liability and exclusion of damages
- Insurance and audit rights
- Termination rights and effects

B. Data Use and Intellectual Property Issues

When negotiating the terms and conditions related to data use, ownership, and other intellectual property (IP) issues, each party will typically aim to achieve the following objectives:

Customer Perspective:

1. Ensure customer will own all inputs, outputs, and derivatives of its data used in the application of the AI model;
2. Confirm data usage will be restricted to service-related purposes;
3. Confirm the customer's right to access data stored by vendor or third-party as needed. For example, the customer might want to require that the vendor provide any relevant data and algorithms in the event of a DOJ investigation or plaintiff lawsuit;**[3]**
4. Aim for broad, protective IP liability and indemnity provisions; and
5. Where patient health information is involved, ensure that it is being used in compliance with HIPAA. Vendors want to train their algorithm on PHI. Unless the algorithm is only being trained for the benefit of the HIPAA-regulated entity and fits within a healthcare operations exception, a HIPAA authorization from the data subject will typically be required to train the algorithm for broader purposes.

Vendor Perspective:

1. Ensure vendor owns all services, products, documentation, and enhancements thereto;
2. Access customer data sources for training and improving machine learning models; and
3. Retain ownership over outputs. From the vendor's perspective, any customer data that is inputted into the vendor's model is modified by that model or product, resulting in the blending of information owned by both sides. One potential solution to this shared ownership issue is for the vendor to grant the customer a longstanding license to use that output.

V. Conclusion

In conclusion, negotiating contracts for AI tools in healthcare demands a comprehensive understanding of the technology, data use, risks and liabilities, among other considerations. By preparing effectively and engaging the right stakeholders and collaborators, both vendors and customers can successfully navigate these negotiations.

FOOTNOTES

[1] UC AI Council Risk Assessment Guide.

[2] NIST AI 600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (July 2024).

[3] Paul W. Grimm et al., *Artificial Intelligence as Evidence*, 19 Northwestern J. of Tech. and Intellectual Prop. 1, 9 (2021).

AI Law and Policy

Copyright © 2025, Sheppard, Mullin, Richter & Hampton LLP. All Rights Reserved.