CLIENT ALERT

Artificial Intelligence in Health Care – What You Need to Know

May.22.2018

Much has been said in recent years about the potential of artificial intelligence (AI) to improve clinical and consumer decision making, resulting in better health outcomes. But deploying AI technology in health care is not without its own challenges, risks, and potential liabilities.

Defining AI

Artificial intelligence is generally understood to mean a bundle of technologies that perform tasks that would normally depend on human intelligence, in which high-speed machines work and react like humans. A related concept is ***augmented intelligence***, where technology is designed to work with human intelligence and enhance it rather than replace it. ***Machine learning*** is a subset of AI, and is the computerized practice of using statistical algorithms to analyze data, learn from it, and then make a determination or prediction about an assigned task.

Benefits and Uses of AI in Health Care

AI has the potential to improve diagnosis and treatment of disease, reduce burden by helping providers focus on the patients that need help the most, and bring the latest in scientific discovery to the point of care—so that even a patient in a remote rural setting can receive care based on cutting-edge medical knowledge. Several challenges in the current health care landscape have the power to catapult AI to the forefront of the health care system: (1) frustrations with health care costs and quality; (2) provider administrative burden; (3) medical labor shortages; (4) the increasing number of health-monitoring devices and technologies; (5) the plethora of data; (6) the advent of personalized and precision medicine approaches; and (7) the proliferation and acceptance of AI technologies in patients' daily lives.

When combined, increases in patient-facing, clinician-facing, and "back-office" efficiencies have the ability to impact vast segments of the health care industry. While AI's potential uses are extensive, a few of these use cases are outlined below:

1. *Evidence-Based Medicine and Clinical Decision Support* – AI can rapidly analyze vast data inputs—including clinical studies and patient health records—to help providers determine the best clinical action, analyze images and test results, make more accurate diagnoses, and deliver better care. On December 8, 2017, the Food & Drug Administration (FDA) issued draft guidance on clinical and patient decision support, addressing its proposed regulatory approach for such software. (See our prior blog post here.) In an April 26, 2018 announcement, Commissioner Scott Gottlieb previewed the FDA's intent to employ a more streamlined approach to oversight of medical devices that incorporate AI. (See our prior blog post here.)
2. *Population Health* – AI can analyze health record and claims data (or other financial data) to identify patient populations with similar characteristics. Grouping patients in this manner could help providers and managed care plans leverage limited resources to focus on high-risk patients and prevent and/or treat disease in at-risk populations.

3. *Drug and Vaccine Development* – AI can be used to expedite drug development by analyzing reams of information, like laboratory and other data reports. Some companies have already started using AI to streamline these processes.

Navigating Compliance at the Edge of Innovation

Despite the incredible potential of AI in health care, health care organizations seeking to deploy AI-based solutions will need to navigate the existing, yet limited, regulatory landscape. During the May 10, 2018 White House Summit on Artificial Intelligence for American Industry, the Trump Administration proposed "removing regulatory barriers to the deployment of AI-powered technologies," touting a clear intent to relax regulation in this space. Moreover, much of the AI governance landscape—or what little exists—is based on a patchwork of regulations from various agencies, sub-regulatory guidance, and aspirational ethical standards developed by third-party organizations.

In light of this reality, entities involved with AI will need to be particularly vigilant regarding the following issues:

1. *Data Access, Control, and Privacy.* – AI and machine learning require access to massive amounts of data. This must be done in compliance with HIPAA and Federal Trade Commission (FTC) rules in the United States and the General Data Protection Regulation (GDPR) in the European Union. For example, depending on the circumstances, acquiring de-identified data may be necessary and HIPAA de-identification may limit the value of data for AI innovation. Even if use of data is compliant with these regulatory requirements, entities often withhold such information if they are not comfortable or don't benefit from the disclosures. While this may have been a risk mitigation strategy for data holders in the past, "information blocking" is now prohibited and violations carry excessive fines. Entities should also clarify intellectual property, licensing and data usage provisions—who owns the data, and who owns or can use the algorithms trained on the data set. Where data ownership is not established by regulatory regime, entities should establish ownership and/or use via contract. Failure to secure access to the core data over a period of time may limit the value of AI systems in the future.
2. *Paramount Cybersecurity Protections.* – Health care data is valuable, and we have already seen sophisticated social engineering attacks exploit security vulnerabilities in an effort to obtain health information. Entities must ensure that they have adequate cybersecurity protections in place when leveraging large databases or sources of health information, including plans for breach mitigation, reporting, and consumer notification to maintain public trust. Failure to do so could not only result in a security breach, but could also lead to significant administrative agency sanctions (e.g., from the Department of Health and Human Services Office for Civil Rights). Entities engaged in AI in health care may want to consider participation in Information Sharing and Analysis Organizations (ISAOs) as a risk mitigation strategy in order to benefit from legal protections for sharing of threat information.
3. *Unclear Regulatory Oversight of AI in Health Care.* – The FDA is still determining what types of software will require premarket approval and whether there will be alternative approaches for safety oversight for AI. There are still questions about how the FDA will define "decision support" tools and AI for software as a medical device. It is important for innovators to consider providing proactive feedback to the FDA and following the rapid policy changes which may affect business models. Furthermore, the FTC has signaled that it will become more active in monitoring representations to consumers about AI in consumer-oriented health tools.
4. *Unknown Liability Structures.* – Hardware defects, software programming defects, or failure of an AI algorithm could result in safety incidents or harm, and determining liability is a complicated undertaking. Best practices are not yet established for the use of sophisticated AI by health care providers. The example of a failed NHS algorithm resulting in

hundreds of thousands of missed breast cancer diagnoses is evidence of the safety and liability risk of AI in health care. Health care providers that use AI systems must consider the liability risk of relying on the software for health care decisions. Innovators will have to consider liability risks, including software bugs, insufficient or biased data sources, and security vulnerabilities. Mitigating risk will require consideration of regulatory oversight requirements. However, because the technology is developing faster than the law, the best strategy is to set contractual limitations and indemnities, obtain insurance coverage, and develop best practices, clinician training, and clinician review or customization of the technology. Entities also must monitor and comply with emerging regulations, and modify contract terms when necessary.

It is critical to think about the business opportunities that AI technology affords and that customers demand, but it is just as critical to stay abreast of changing laws and implement a strategy for managing uncertainty. Crowell & Moring's Digital Health team continues to monitor U.S. and international policy regulating AI and can work collaboratively with your team's leadership, lawyers, product managers, engineers, and government affairs teams to provide strategic counseling on these issues.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jodi G. Daniel
Partner – Washington, D.C.
Phone: +1 202.624.2908
Email: jdaniel@crowell.com

Maya Uppaluru
Counsel – Washington, D.C.
Phone: +1 202.624.2518
Email: muppaluru@crowell.com