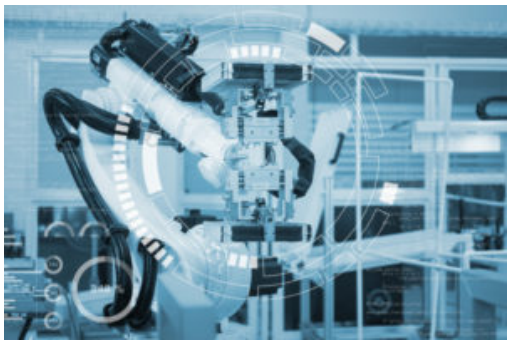
Five Emerging Concerns for the Health Care Industry as AI & Telehealth Converge



The use of telehealth continues to grow rapidly across the U.S. Given legislative **proposals** and the Centers for Medicare & Medicaid Services **efforts** to expand access to telehealth, we can only anticipate that remotely engaging with healthcare providers is here to stay. In fact, the National Center for Health Statistics and the Centers for Disease Control and Prevention **reported** that between April and July 2021, 24.5% of adults in the U.S. had a virtual care appointment with a healthcare professional over video or phone. Given the continued persistence of COVID-19 and the ease and convenience for both provider and patient, telehealth services will most likely remain popular even as the option of in-person appointments regains footing.

On a parallel front, artificial intelligence (AI) is also driving considerable advancements in patient care. Advances in AI offer a powerful way to create clinical and operational efficiency in today's healthcare system. According to a **study** by MIT, 72% of healthcare professional respondents showed interest in implementing AI in healthcare delivery. In the field of radiology, as just one of many examples, AI can already be used to find patterns in CT scans, mammography, and other imaging modes that help **radiologists more accurately diagnose** cancer and a whole spectrum of other sometimes hard-to-identify diseases.

Telehealth is one of the newest services to utilize AI widely, and there is great promise in its application. Telehealth typically involves a synchronous, real-time electronic communication from person-to-person. Subject to limitations in certain states, telehealth also can be furnished through asynchronous communication, whereby a physician reviews and makes medical assessments based on information that a patient has uploaded or stored in a database. Even though it is asynchronous, this remains a person-to-person communication. Recently, however, we see more and more opportunities for AI to augment the person-to-person nature of and enhance the capabilities of telehealth. For example:

- **Clinical Evaluation** – leveraging AI to take patient histories and make collecting patient information more efficient. This could include a series of AI-developed questions during telehealth intake designed to ask the right questions in the proper sequence to better assist a physician in determining the cause of a patient's symptoms.

- **Telemonitoring** – the potential for AI and telemonitoring extends beyond just collecting patient data and turning them into reports. Implementing AI into remote patient monitoring (RPM) devices can promote preventative care and equip the RPM with the ability to predict adverse events.

- **Quality Improvement** –further integration of AI technology in telehealth services can help

with quality improvement processes by enhancing clinical decision-making and disease diagnosis, ultimately optimizing patient care and significantly improving healthcare outcomes.

- **Virtual Health Assistants** – AI-enabled interfaces allow patients to have more power and control over their healthcare paths. AI applications in virtual health assistants can provide the patient with precise information about their healthcare condition and assist with better healthcare management.

With the promising future of the continued convergence of AI and telehealth and the increased use of digital and consumer technologies to deliver virtual care, there are several legal and regulatory considerations for telehealth providers. These include:

- **Protecting Patient Health Information.** One of the biggest issues related to data privacy and security with the application of AI in healthcare is the need to either use de-identified information or obtain patient authorization to use identifiable information. Absent patient authorization, it is difficult to use protected health information (PHI) for machine learning. But sometimes de-identified information is insufficient for machine learning. If the developer of the AI is using de-identified information, it must have the right to de-identify the PHI. Typically, a business associate (BA) is developing the AI. BA's must have the right to de-identify under the business associate agreement (BAA); otherwise, they can't de-identify PHI. Further, there is a separate risk that the AI can be used to re-identify de-identified information. Studies have **demonstrated** the potential to re-identify de-identified patient records by combining it with other data sources that AI collects such as facial recognition or iris scans. Because only a few states, like **California**, have banned re-identification of de-identified data, a Covered Entity may want to include provisions in a BAA with an entity developing AI to protect against that.

Another significant consideration with AI implementation in digital health is patient health information protection and verification. Healthcare providers are subject to state privacy and security regulations as well as the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations, which protect the privacy and security of health information and give individuals certain rights concerning their health information. According to a 2019 University of California Berkley **study**, due to the nature and functionality of AI, current laws and regulations appear inadequate to keep an individual's health status private. The findings demonstrate that using AI makes it possible to identify individuals by learning daily patterns collected by remote patient monitoring devices such as smartwatches and smartphones and correlating them to demographic data. If bad actors gain access to such information, they can piece together patients' identities. According to a 2020 cybersecurity **survey**, 70% of the healthcare providers that responded stated that they experienced significant security incidents between 2019 and 2020. Telehealth providers should be mindful of the potential gaps in data protections that could be created with the addition of AI. This includes continued vigilance when it comes to HIPAA compliance and reexamining their internal risk assessments, policies, and practices considering the additional risks raised by AI.

- **Corporate Practice of Medicine Considerations.** As telehealth platforms leverage AI to help physicians deliver care to patients, there is an increasing opportunity for providers to use AI, through machine learning, for example, to diagnose and/or identify the appropriate treatment regimen for patients. Potential corporate practice of medicine (CPOM) concerns could ensue. **Generally, CPOM laws** are designed to prohibit corporations from practicing medicine: only individual practitioners can diagnose and treat patients, and CPOM prohibitions prevent corporate interference with a healthcare professional's independent professional judgment. Without the right level of physician supervision, it is conceivable that

an advanced AI-enabled telehealth platform could potentially diagnose or recommend patient treatment options or otherwise blur the lines demarcating where the machine's judgment ends, and the physician's judgment begins. A company offering AI-enabled telehealth services should be mindful of and create clear supervision requirements and boundaries to avoid running afoul of these longstanding laws. These boundaries should identify important guardrails, including whether and how a physician can overrule AI-driven diagnoses, and when must a physician sign off on an AI-generated treatment regimen. Since telehealth is often practiced in multiple states, and because CPOM laws vary from state-to-state, providers utilizing telehealth services must structure their operations to account for the variability of the CPOM prohibitions in various states.

- **Health Disparities.** The implementation of AI-enabled telehealth services also raises important ethical questions about the availability of innovative care. There is a potential that adding AI to telehealth services might shrink the gap between those accessing advanced care technologies and those that are not. For example, **studies** have shown that those with limited English language skills have lower rates of telehealth use. Adding AI virtual assistants to telehealth technology could, for example, help to ensure that language barriers do not get in the way of appropriate care. Rather than finding a provider that speaks a particular language, an AI-enabled telehealth platform could assist by providing translation services in real time in multiple languages. This could allow an AI virtual assistant, for example, to collect more comprehensive medical history during a telehealth visit, thereby providing a greater opportunity for better care and treatment. Incorporating AI into telehealth visits might also allow for better questions that account for how different cultures view disease and treatment, or for diseases that might only affect a narrow sub-population.

But, there is also the possibility that AI-enabled telehealth services might exacerbate the gap between those who have access to the latest innovative technology and those who do not. The growing expansion of telehealth services could risk widening disparities among marginalized populations who may have limited access to necessary **resources**: for example, those who lack access to a computer or smartphone or lack reliable broadband access. The deployment of AI by telehealth providers is likely to lower costs and should improve disparities in access to care. However, in the short term, access to AI-aided telehealth services may be uneven and contribute to a greater disparity in access to care. The addition of AI to telehealth will likely not solve the physical access or cost problems, and it could conceivably add more costs to telehealth technology. Further, many state Medicaid programs do **cover** telehealth visits for their beneficiaries, but the infusion of AI may require state regulators to further examine telehealth coverage policies.

- **Professional Liability & Malpractice.** As AI advances and its capabilities are better leveraged, how will the highly litigious American people respond? Who will be responsible when AI-enabled telehealth results in an unfortunate misdiagnosis? AI and machine learning are not immune to mistakes. For example, the visual nature of a skin examination lends itself well to the use of machine learning as a potentially valuable tool in teledermatology and the **diagnosis and management** of dermatologic diseases, especially in areas where a dermatologist may not be available. However, just like humans, AI might not always get it right. AI algorithms have some shortcomings, including inapplicability outside of their training domain or bias. We know that **blind spots** in machine learning machines can sometimes imitate the worst societal biases, with a risk of **unintended consequences** that have particular effects on **minority groups**, which can open up providers to increased liability if they depend on these algorithms to assist in diagnosing patients. Who can be held liable for malpractice if a patient undertakes a series of damaging treatments – or fails to seek

treatment based on an AI-enabled diagnosis the patient receives through a telehealth platform? The AI developer? The telehealth platform? The individual physician who signed off on the misdiagnosis? And which law applies, especially if the patient is in one state, the telehealth provider in another state, and the AI data platform in yet another state? Further, how much training must a telehealth platform provide its individual physicians regarding the use of AI-infused tools? If a healthcare provider uses AI to treat or diagnose a patient, both the AI developer and the healthcare provider may be exposed to tort liability related to an adverse event. The AI developer can be exposed to products liability claims and the provider may be exposed to malpractice claims. However, without clear legislative direction, it is conceivable that litigants will use the courts to lay out these rules.

- **FDA Implications.** The regulatory framework governing AI is complex. A threshold question for any AI developer is whether their AI-enabled product will be actively regulated by the U.S. Food and Drug Administration (FDA), a question that hinges not only on the product's functionalities, but also its proposed marketing claims. Further, the FDA continues to develop its framework for regulation of AI-enabled products that the agency actively regulates. On January 12, 2021, the FDA **released** the agency's first Artificial Intelligence/Machine Learning (AI/ML)-based Software as a Medical Device (SaMD) Action Plan. This action plan describes a multifaceted approach to advance the FDA's oversight of AI/ML-SaMD, and offers stakeholders several opportunities to engage with the FDA to discuss the agency's oversight approach. For example, upcoming opportunities include the FDA's planned virtual public **workshop** on October 14, 2021 on the role of transparency in enhancing the safety and effectiveness of AI/ML-based SaMD. Stakeholder feedback continues to inform the evolution of FDA's regulatory framework for oversight of AI/ML-based SaMD, including FDA's expectations for such products during premarket review. A thorough understanding of such expectations early in development can inform more efficient development strategies.

Advances in the use of AI in telehealth will no doubt continue. AI's application in telehealth platforms is not just limited to potentially diagnosing a wide range of diseases (like analyzing data from tele-dermatological visits to more accurately diagnose skin cancer); but it can also improve the patient experience (by asking more pinpointed intake questions, for instance), make telehealth visits more efficient (by, for example, more rapidly analyzing a patient's history for a physician in advance of a visit), and help ensure more effective treatment (with AI-generated follow-up adherence or refill calls). AI can reduce differences in clinical practice, improve efficiency, and prevent avoidable medical errors that can help with healthcare costs and improve health outcomes and the patient experience.

But a fundamental component to achieving a safe and effective deployment of AI in telehealth services is ensuring that AI developers, telehealth platforms, and the physicians that leverage these tools have the necessary legal and regulatory guardrails in place. This includes addressing the application of current privacy and data security regimes, how telehealth providers supervise the use of AI technology to ensure compliance with CPOM laws, and how telehealth providers address growing disparities in access to care.