

ARTIFICIAL INTELLIGENCE IN HEALTH CARE: Welcome to the Machine



By Scott Bennett, Coppersmith Brockelman LLC,
and Leeann Habte, Best Best & Krieger LLP

The phrase “artificial intelligence” might conjure up futuristic images of robots who become more advanced than their human creators and end up destroying civilization. But there is no need to look to a dystopian future to see how artificial intelligence (AI) could change the ways we live and work. AI is already here, and very much a part of daily life as well as health care. This article explains the basics of AI, discusses current and emerging uses of AI in health care, and examines some of the legal issues that health care lawyers and providers will encounter as they consider adopting AI.

The Basics of AI Technologies

Let’s start by demystifying some terms that are commonly used in discussions of AI. Dartmouth professor John McCarthy first used the phrase “artificial intelligence” in 1955.¹ AI refers to computer systems that can perform tasks that normally require human intelligence. There are multiple types of AI technology. One is machine learning, which refers to a “machine’s ability to keep improving its performance without humans having to explain exactly how to accomplish all the tasks it’s given.”² Another is *deep learning* through *neural networks*, which are “massively distributed computational systems that mimic the multilayered connections of neurons in the brain.”³

Industry experts predict that the use of AI in health care will grow exponentially in the coming years.

Since the mid-2000s, the biggest advances in AI have been in specific types of machine learning: perception (including language and image recognition), and cognition/problem solving.⁴ These types of AI are now embedded in devices that are very familiar to consumers. Think of the language recognition that powers virtual assistants like Apple’s Siri, Amazon’s Alexa, and Google Assistant; the image-recognition technology used by Facebook to recognize friends’ faces; and the AI programs that have defeated human champions in chess (IBM’s Deep Blue), the TV show *Jeopardy* (IBM’s Watson), and most recently the ancient strategy game called Go (Google’s AlphaGo).

Uses of AI in Health Care

Industry experts predict that the use of AI in health care will grow exponentially in the coming years. A 2015 study found that the health care industry spent \$630 million on AI technologies in 2014, and predicted that figure will balloon to more than \$6.6 billion annually by 2021.⁵ Here is a sampling of the many new AI technologies that show promise in health care:

» Hospitals are exploring a wide variety of uses for virtual assistants like Amazon’s Alexa, including speaking safety checklists for surgeons, providing patients with information about common illnesses and medication, allowing voice

dictation by physicians, and interacting with older adults in their homes.⁶

- » Virtual assistants also can provide health information and recommendations to consumers. One example is a mobile application available in the United Kingdom only, which makes health recommendations based on a user’s personal history, common medical knowledge, and reported symptoms.⁷
- » Image-recognition software can recognize skin cancer in photos, identify arrhythmias in EKGs, and determine whether a nodule in a CT scan is malignant.⁸
- » Clinical decision support software can assist human providers. One example is IBM’s WatsonPaths, which provides treatment recommendations for oncologists, based upon what the program has learned from large amounts of patient data, as well as information it pulls from reference materials, clinical guidelines, and medical journals.⁹
- » Health care entities can use AI to help guard against cyberattacks by “learning in real time what’s going on, and using AI to recommend actions to take, even if the attack’s never been seen before.”¹⁰ AI also can detect and help prevent data breaches by employees through behavior analysis, where “[a] pattern of user behavior is established and any actions that deviate from that behavior, such as logging in from a new location or accessing a part of the system the user normally doesn’t access are flagged.”¹¹
- » Predictive analytics can determine which patients are at risk of hospital readmissions, falls, and health conditions that require intervention.¹²
- » AI technologies can accelerate and assist the development of drugs, biologicals, genomics, and personalized medical treatment.

The Legal Issues Associated with AI in Health Care

The use of AI in health care raises a number of legal issues, including the following.

1. Patient Consent and Privacy

One high-profile example of how the use of AI can create privacy concerns is the controversial arrangement between Google’s DeepMind and the United Kingdom’s National Health Service (NHS). In 2015, an NHS hospital provided identifiable health records of 1.6 million patients to DeepMind, an AI company. DeepMind planned to use the information to develop an application that would help NHS clinicians identify and manage acute kidney disease. However, the hospital failed to obtain patients’ consent, or even notify them, before disclosing their health information. The disclosure created outrage among members of the public as well as privacy advocates. And it might have been illegal. Under British law, express patient consent is not required to disclose patient information for “direct care.” But the UK’s Data Guardian concluded that the actual purpose of the disclosure “was for the testing of the Streams application, and not for the provision of direct care to patients.”¹³

In the United States, the use or disclosure of patient information in connection with AI similarly might require patient consent. The Health Insurance Portability and Accountability Act (HIPAA), for example, allows the use or disclosure of

protected health information for “treatment” without patient authorization. But AI technologies sometimes strain traditional legal categories, such as HIPAA’s definition of treatment. Consider a clinical decision support program like WatsonPaths, which learns from the health information of some patients to make recommendations for *other* patients. It is unclear whether that use of patient information could meet the HIPAA definition of treatment.¹⁴

Because of the imperfect fit between new AI technologies and laws designed in previous eras, health care entities might decide to err on the side of caution and seek patient consent before using identifiable patient information with AI. That would reduce both legal risk, and the kind of negative publicity the DeepMind-NHS deal received.

Because of the imperfect fit between new AI technologies and laws designed in previous eras, health care entities might decide to err on the side of caution and seek patient consent before using identifiable patient information with AI.



When it is not possible or practical to obtain patient consent, health care entities should consider de-identifying patient information used with AI. Emerging AI technologies raise questions about the sufficiency of current methods of de-identification. Even without AI, sophisticated researchers have been able to re-identify health information using publicly available sources.¹⁵ The risk of re-identification will be greater with new AI technologies. As one tech lawyer wrote: “Existing deanonymization capabilities will be super-turbo charged once these AI applications are more accessible (which is only a matter of time).”¹⁶ Health care entities using de-identified patient information with AI should consider using stronger methods of de-identification (for example, using the “expert method” rather than the “safe harbor” method under HIPAA).¹⁷

2. FDA Regulation

The Food and Drug Administration (FDA) regulates software that meets the definition of a “device” under the Food, Drug, and Cosmetic Act.¹⁸ In 2016, Congress enacted the 21st Century Cures Act (Act), which clarified the FDA’s regulatory authority over digital health and medical devices. Digital health includes AI systems that use machine learning or adaptive algorithms to provide diagnostic information for patients.¹⁹

The Act excluded from regulation as a device certain low-risk medical software, such as programs that encourage a healthy lifestyle, serve as electronic patient records, assist in displaying or storing data, or provide limited clinical decision support.²⁰ In December 2017, the FDA issued draft guidance, which states that the FDA considers clinical decision support software a “device” if it makes a treatment recommendation that could not be reached independently by a physician or other user. That would be the case, for example, where software analyzes a patient’s laboratory results using a proprietary algorithm or relies on data inaccessible to the user (rather than clinical practice guidelines, for example).²¹

In 2017, the FDA launched a pilot program to “pre-certify” eligible digital health developers who demonstrate a culture of quality and organizational excellence. Pre-certified developers could then market certain of their devices either without additional FDA review, or with a more streamlined premarket review.²²

Health care entities that are considering adopting clinical decision support software or similar programs should determine whether the software requires and has received FDA approval. Many technology developers are not familiar with the unique legal landscape in health care, including the scope of FDA regulation. Indeed, after the public outcry about its receipt of millions of identifiable patient records, DeepMind noted in a public statement that one contributing factor was its lack of familiarity with the complex legal requirements in health care.²³

3. Fraud and Abuse

As companies develop and test new AI technologies, they commonly offer the technologies to health care providers for pilot testing, research, or analysis, often at a reduced cost. This can implicate the Stark Law (Stark), Anti-Kickback Statute (AKS), or related state fraud and abuse laws, in particular if the services that these technologies support are reimbursed by Medicaid or Medicare.²⁴ Such arrangements should be carefully structured to eliminate or minimize any such legal risks, such as by ensuring that any payment received is for *bona fide* services, and that the arrangement falls within a Stark exception or AKS safe harbor.

4. Liability Issues

Just as the widespread adoption of electronic health records (EHRs) has affected the standard of care for health care providers, the use of AI technologies such as WatsonPaths might become a required part of medical decision making. For example, in a recent case involving a patient whose doctor failed to diagnose his prostate cancer in time for it to be cured, the court held that the physician violated the standard of care by failing to review the patient’s past visit notes that were available in the patient’s EHR—and that would have elucidated the nature of his problem.²⁵ As another example, drug-drug and drug-allergy interaction checks have come into common use as EHR systems have become widespread.²⁶ As a result, physicians who fail to screen and monitor for those harmful interactions may now face potential exposure to liability for negligence. Similarly, when AI is fully integrated into the health care system, use of AI might be considered the duty of a reasonably prudent practitioner, and consequently, the failure to use AI in diagnosing and treating a patient could expose providers to

malpractice claims. To minimize this potential liability, health care organizations that implement AI should develop policies to guide and standardize its use within the organization.

Typically, software and digital technology are licensed to a health care organization by the vendor who manufactures the technology.²⁷ These license agreements commonly include disclaimers of warranties with regards to the software's performance and its defects, and, if they include indemnification, stringent limitations of liability.²⁸ Health care lawyers should require terms in the license agreements that allocate appropriate liability among the parties, particularly when use of the software could result in harm to patients. Contract provisions also should address other potential risks, such as cybersecurity and data breaches.

In addition to contractual protections, the courts may be more willing to impose liability on AI product manufacturers.²⁹ For example, a class action was recently filed against eClinical Works, an EHR vendor, for \$1 billion for breach of fiduciary duty and gross negligence following claims that an individual died of cancer due to faulty EHRs.³⁰ Health care lawyers should consider keeping up to date on these litigation trends.

Due diligence with AI vendors is another way to reduce potential liability. It is important to do adequate research regarding the specific AI technology, as well as the developer. Health care entities that are considering adopting an AI technology should ask the vendor for:

- » Evidence of FDA approval, if applicable;
- » Information about any actual or potential lawsuits or claims relating to either the specific technology at issue, or any other technology of the same vendor;
- » Information about recent security incidents or breaches;
- » The vendor's security risk analysis related to the AI technology;
- » Names and contact information for other customers of the same technology, and different technologies from the same vendor;
- » Evidence that the vendor has all rights and licenses necessary to provide the technology, as well as to provide any other necessary services.

Other key pieces of information are any industry or peer reviews of the technology; the algorithms used by the technology, if the vendor will share them; and the data sources on which the technology relies.

5. Insurance Coverage

It is important to confirm that the organization has insurance that would cover the risks associated with use of a potential new AI technologies and software, which might include personal injury and wrongful death.

6. Discrimination and Meaningful Access

This is a potential area of concern for AI technologies that interact with patients, such as virtual assistants or online chatbots. There have been a number of recent lawsuits against hospitals alleging that the methods they use to communicate with deaf patients were discriminatory.³¹ Organizations that use AI technologies to interact with patients might be required to provide alternatives for patients who are not proficient in English, have a disability that prevents them from using the



Health care lawyers should require terms in the license agreements that allocate appropriate liability among the parties, particularly when use of the software could result in harm to patients.

technology, or do not have ready access to a computer or other necessary technology. Health care lawyers should assess interactive AI technologies' compliance with the Americans with Disabilities Act,³² Section 504 of the federal Rehabilitation Act,³³ Section 1557 of the Affordable Care Act,³⁴ and similar state laws.

7. Security Risk Analysis

The HIPAA Security Rule requires covered entities and business associates to update their security risk analysis "in response to environmental or operational changes affecting the security of electronic protected health information[.]"³⁵ Health care entities that start using a new or different AI technology should consider the appropriate updates to their risk analysis.

Conclusion

AI is already a part of daily life, and has made its way into health care as well. The technologies have the potential for dramatic improvements in the delivery of health care. But they also present potential risks that attorneys will need to help manage. **C**



Scott Bennett is a partner at Coppersmith Brockelman LLC in Phoenix, AZ. Scott assists health care clients with health information technology, data privacy and security, and compliance issues. Scott is a Certified Information Privacy Professional/United States (CIPP/US), through the International Association of Privacy Professionals.



Leeann Habte is a partner at Best Best & Krieger, a California firm known for its public agency practice. With a focus on health care privacy and data security, regulatory compliance, and reimbursement, Leeann provides strategic counseling to emerging medical device and digital health companies, health plans, hospitals, health information exchanges, and other organizations. Leeann serves as membership vice-chair of the American Health Lawyers Association Digital Health Affinity Group and is a Certified Information Privacy Professional.

Thanks go out to the leaders of the Health Information and Technology Practice Group for sponsoring this feature: **Amy S. Leopard**, Bradley Arant Boult Cummings LLP, Nashville, TN (Chair); **Alisa Lieberman Chestler**, Baker Donelson Bearman Caldwell & Berkowitz PC, Nashville, TN (Vice Chair—Strategic Planning and Special Projects); **Kathleen Dillon Kenney**, Polsinelli PC, Chicago, IL (Vice Chair—Educational Programs); **Lisa Pierce Reisz**, Vorys Sater Seymour & Pease LLP, Columbus, OH (Vice Chair—Membership); **Gerard M. Nussbaum**, Zarach Associates LLC, Chicago, IL (Vice Chair—Publications); **Leonardo Tamburello**, Willis Towers Watson, New York, NY (Vice Chair—Research & Website); **Sean R. Baird**, Amazon, Seattle, WA (Social Media Coordinator). For more information about the Health Information and Technology Practice Group, visit www.healthlawyers.org/PGs. Follow them on Twitter [@AHLA_HITsters](https://twitter.com/AHLA_HITsters).

Endnotes

- ## Endnotes
- Erik Brynjolfsson and Andrew McAfee, *The Business of Artificial Intelligence*, HARV. BUS. REV. (Aug. 7, 2017), available at <https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence>.
 - Id.*
 - Jason Tanz, *Soon We Won't Program Computers. We'll Train Them Like Dogs*, WIRED (June 3, 2017), available at <https://www.wired.com/2016/05/the-end-of-code/>.
 - The Business of Artificial Intelligence*, *supra* note 1; Brian Fung, *Everything you think you know about AI is wrong*, WASH. POST (JUNE 2, 2016), available at https://www.washingtonpost.com/news/the-switch/wp/2016/06/02/everything-you-think-you-know-about-ai-is-wrong/?utm_term=.d683cefb6b15.
 - Frost & Sullivan, *Cognitive Computing and Artificial Intelligence Systems in Healthcare: Ramping Up a \$6 Billion Dollar Market Opportunity* (Dec. 9, 2015), available at <http://www.frost.com/sublib/display-report.do?d=NFFE-01-00-00-00&bdata=aHR0CM6Ly93dzluZnJvc3QuY-29tL25ld3MvcHJlc3MtcMVsZWZfZXMvNjAwLW0tNi1iaWxsaW9uLWFYdG-lmaW9pYWwtaW50ZWxsaWdlbmNlXN5c3RibXMtcG9pc2VklWRyYW1h-dGJlLW1hcmtdC1leHBhbnNpb24taGVhbnR0Y2FyZUB%2BQeJhY2tAfkAX-NTezMzAyNzlxNDM3>.
 - Christina Farr, *Hospitals are looking for a hit Amazon Alexa app*, CNBC (June 26, 2017), available at <https://www.cnbc.com/2017/06/18/hospitals-are-looking-for-the-killer-amazon-alexa-app.html>.
 - Novatio, *10 Common Applications of Artificial Intelligence in Healthcare* (Aug. 29, 2017), available at <http://novatiosolutions.com/10-common-applications-artificial-intelligence-healthcare/>.
 - Jonathan Kay, *How Do You Regulate a Self-Improving Algorithm?*, THE ATLANTIC (Oct. 25, 2017), available at <https://www.theatlantic.com/technology/archive/2017/10/algorithms-future-of-health-care/543825/>; Enlitic, <https://www.enlitic.com>.
 - IBM, *WatsonPaths*, available at http://www.research.ibm.com/cognitive-computing/watson/watsonpaths.shtml#fbid=G_vsXhYab7e.
 - Scott Rosenberg, *Firewalls Don't Stop Hackers. AI Might.*, WIRED (Sept. 29, 2017), available at <https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/>; Ben Dickson, *How predictive analytics discovers a data breach before it happens*, TECHCRUNCH (July 25, 2016), available at <https://techcrunch.com/2016/07/25/how-predictive-analytics-discovers-a-data-breach-before-it-happens/>.
 - Donald Voltz, *Why artificial intelligence is needed to prevent cyber attacks*, HEALTH DATA MANAGEMENT (Oct. 31, 2016), available at <https://www.healthdata-management.com/opinion/why-artificial-intelligence-is-needed-to-prevent-cyber-attacks>.
 - John Mannes, *CareSkore gets \$4.3M to bring machine learning to preventive care*, TECHCRUNCH (Aug. 10, 2016), available at <https://techcrunch.com/2016/08/10/careskore-gets-4-3m-to-bring-machine-learning-to-preventive-care/>; DeepMind, *Streams in NHS Hospitals*, available at
 - FDA, *Clinical and Patient Decision Support Software: Draft Guidance for Industry and Food and Drug Administration Staff* (Dec. 8, 2017), available at <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationand-Guidance/GuidanceDocuments/UCM587819.pdf>.
 - FDA, *Digital Health Innovation Plan* (2017), available at <https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf>.
 - Mustafa Suleyman and Dominic King, *The Information Commissioner, the Royal Free, and what we've learned*, DEEPMIND (July 3, 2017), <https://deeptmind.com/blog/ico-royal-free/>.
 - The most pertinent guidance relates to fraud and abuse in the pharmaceutical industry. See, e.g., 68 Fed. Reg. 23731, 23735-36 (May 5, 2003); PHARM. RESEARCH AND MFR. OF AM., *PhRMA Principles on Conduct of Clinical Trials* (Apr. 8, 2013), available at <http://www.phrma.org/principles-and-guidelines-clinical-trials>.
 - The Doctor's Company, *Electronic Health Record Malpractice Risks*, available at <https://www.thedoctors.com/articles/electronic-health-record-malpractice-risks/>; Neil Chesanow, *8 Malpractice Dangers in Your EHR*, MEDSCAPE (Aug. 26, 2014), available at <https://www.medscape.com/viewarticle/828403>.
 - CTRS. FOR MEDICARE & MEDICAID SERVS., *EHR Incentive Payment Program*, available at <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/EducationalMaterials.html>.
 - Amanda Swanson and Fazal Khan, *The Legal Challenge of Incorporating Artificial Intelligence into Medical Practice*, 6 J. HEALTH & LIFE SCI. L. 90 (2012).
 - Id.* at 120.
 - W. Nicholson Price II, *Artificial Intelligence in Health Care: Applications and Legal Issues*, 14 SCITECH LAWYER 10 (2017); McDermott Will & Emery, *Digital Health Year in Review: 2017 Trends and Looking Ahead to 2018* (Jan. 10, 2018), available at <https://www.mwe.com/en/thought-leadership/newsletters/2018/digital-health-year-in-review-2017>.
 - Jessica Davis, *eClinicalWorks Sued for Nearly \$1B Due to Faulty Patient EHRs*, HEALTHCARE IT NEWS (Nov. 2017), available at <http://www.healthcareit-news.com/news/eclinicalworks-sued-nearly-1-billion-inaccurate-medical-records>.
 - See, e.g., BECKER'S HOSP. REVIEW, *Hospitals lack sign language interpreters in ER* (May 22, 2017), available at <https://www.beckershospitalreview.com/legal-regulatory-issues/hospitals-lack-sign-language-interpreters-in-er.html>; Paige Minemyer, *Offer in-person interpretation for deaf patients, not video sessions, feeds tell UVM Medical Center*, FIERCE HEALTHCARE (Nov. 30, 2017), available at <https://www.fiercehealthcare.com/healthcare/university-vermont-medical-center-deaf-patients-interpreters>.
 - 42 U.S.C. §§ 12101-12213.
 - 29 U.S.C. § 701.
 - 42 U.S.C. § 18116.
 - 45 C.F.R. § 164.308(a)(8).