Aashna Soni

Ms. Abdelaziz

Honors Lang P1

16 May 2022

Artificial Intelligence: The Future of Healthcare

Imagine a world in which patients do not have to go to the doctor's office for every new problem. If a patient's heart rate becomes abnormally high, her smartwatch could compare the heart rate to the patient's historical heart rate variation, factor in whether or not the patient was performing strenuous activities that could have prompted the change, and alert the doctor if the change is indicative of a serious condition. Imagine a world in which individuals diagnosed with cancer would have less uncertainty as to which treatment is best for them—instead of using trial and error, artificial intelligence (AI) models would be able to analyze the patient's genetic data and determine the best treatment plan. Patients of all races would benefit from this personalized health care approach because predictive models would use large, diverse sets of data. All of these benefits would come to fruition with the expansion of a single tool: artificial intelligence. Despite the privacy concerns posed by the adoption of AI in the healthcare industry, the expansion of this technology will significantly improve the diagnosis and treatment of diseases as well as bring equity to medical care.

The field of AI was first conceptualized in 1950 by Alan Turing, an English mathematician and computer scientist ("Turing test"). He developed the Turing test, which "determine[s] whether a computer can 'think,'" ("Turing test") or have complex thoughts like humans do. This test involves a human interrogator, who asks various questions to a computer and to another human. If the computer is repeatedly "misidentified as the human subject,"

("Turing test") it is regarded as having thinking capabilities. This simple idea fueled the AI revolution as engineers began to design computer programs that imitated human thought. With the advent of AI came the concept of machine learning, a subset of AI technology that employs models which are able to continuously improve their own analysis algorithms, making them significantly independent from humans ("What is Machine Learning?"). In the context of medicine, a machine learning model is first presented with large volumes of patient data including factors such as genetics, environment, lifestyle, and nutrition (Johnson et al.). This process trains the model, allowing it to then make predictions for new patients in a manner free from the bias and human error that accompany predictions made by medical caregivers (Khan et al.).

One area for leveraging AI data analysis techniques to improve patient health is the Internet of Medical Things (IoMT), "an amalgamation of medical devices and applications that can connect to health care information technology systems using networking technologies" ("Internet of Medical Things"). The different parts of the IoMT are designed to work together to make transferring health data to medical providers swift and easy, reducing "unnecessary hospital visits" ("Internet of Medical Things"). AI models are able to determine which data points from the large stream of data collected are actually relevant, allowing doctors to receive this important information in a "timely manner" (Venkatesh) and take necessary action. In addition to filtering data, AI models have the ability to "make inferences and predict medical diagnostics based on complex analysis algorithms" ("AI and IoMT"). This process involves examining a patient's health data in a broader context and looking for trends and patterns that could indicate important changes. For example, if a patient's blood pressure readings have been consistently high for several weeks, AI models would be able to identify this trend and interpret

it to mean that a patient might have hypertension, a condition that could put the patient at higher risk for heart disease ("High blood pressure"). By combining IoMT, which can detect day-to-day changes in vitals, with AI, for deep analysis, healthcare institutions can make the process of medical care hassle-free and more responsive to patients' changing needs ("AI and IoMT").

In addition to maintaining an individual's health using medical data collected on a daily basis, AI can be leveraged to diagnose more serious diseases using data obtained in a clinical setting, such as through radiology reports. Different individuals may be at varying risk levels for certain diseases, and AI analysis can be useful in predicting the likelihood of a particular individual developing a disease based on medical imaging data and patient records. Based on this information, AI models can then make a diagnosis for a patient. For example, an AI algorithm was designed to predict the likelihood of women developing breast cancer (Johnson et al.). This algorithm was "trained on 38,444 mammogram images from 9,611 women" and was able to "differentiate between normal and abnormal screening results," making interpreting medical images less prone to error and reducing "missed diagnoses of breast cancer" (Johnson et al.). This type of machine learning strategy could significantly help radiation oncologists, whose job relies heavily on "digital data processing and computer software" (Huynh et al.) to make diagnoses. With the expansion of AI, radiation oncologists can focus more on providing the specific care their patients need, leaving the highly technical data analysis process to a trained AI model. This system would also reduce the amount of time spent making a diagnosis, improving the chances that a suitable treatment will be implemented sooner.

The benefits of AI extend beyond predicting the risk levels for disease; AI can also design personalized treatment plans for patients. The need for such personalized analysis is illustrated by the current difficulty in treating cancer. Though oncologists are often able to

identify a few known mutations and treatments that have been proven to work for those specific mutations, there are still many other mutations whose effects are unknown (Degasperi et al.). As a result, individuals who are given the same official diagnosis may respond very differently to the same treatment. In an effort to elucidate the lesser-known mutations found in tumor screening reports, scientists conducted a study in Cambridge, UK, in which they performed a large-scale analysis of "12,222 whole-genome-sequenced cancers" (Degasperi et al.). The researchers were able to find many new mutational signatures, or patterns formed by specific combinations of mutations, that significantly impact the progression of cancer in an individual (Degasperi et al.). After discovering these new signatures, the researchers designed an algorithm called "Signature Fit Multi-Step," (Degasperi et al.) whose goal is to find new mutational signatures in future patients in light of the recent findings. The mutational signatures that this algorithm finds in a particular individual could help oncologists identify a treatment plan that has the highest chance of working. Further supporting the effectiveness of an AI-driven personalized approach to medicine is a study conducted by McDonald and others. In this study, researchers fed genetic data into a supervised learning AI model to predict how patients would respond to chemotherapy treatment. Using this approach, the researchers were able to identify multiple drugs that showed promise for the individuals in the study (Johnson et al.). Computer algorithms such as the ones previously mentioned have the potential to make precision medicine, "an innovative approach that takes into account individual differences in people's genes, environments, and lifestyles," ("Precision Medicine Initiative") the norm, improving health outcomes for everyone.

Not only can AI deliver individual benefits through a personalized healthcare approach, but it can also make healthcare more equitable overall. Currently, AI models contain significant levels of bias because the datasets they use are very limited. Thus, they cannot be used to help a

wide range of people (Khan et al.). For instance, postpartum hemorrhage is “a serious but rare condition when a woman has heavy bleeding after giving birth” (“Postpartum Hemorrhage”). Studies have shown that a great racial disparity exists in the outcomes of women who develop hemorrhage. While white patients have better access to prenatal care and thus experience better outcomes, black patients do not have the same access and are at higher risk for comorbidities (Khan et al.). An AI model trained mostly on data from white patients may, when applied to helping black patients, “fail to identify comorbidities” (Khan et al.) or wrongly identify an individual as having a low risk for developing the disease. This issue can be fixed through introducing large, diverse sets of data in the process of designing AI models, ensuring that underrepresented groups also contribute to the model’s calculations (Khan et al.). As these models are “studied and validated across many populations,” (“The potential of artificial intelligence”) health care outcomes will significantly improve for people of all groups. In addition to making the AI models themselves more accurate by introducing larger, more diverse data sets, increasing the usage of these predictive models will allow resources to be distributed quickly and efficiently to those who have the greatest need for them (Khan et al.). In a study conducted by Khan and others, “55 candidate risk factors for hemorrhage” (Khan et al.) were assessed by machine learning models. One of the models designed, the “Extreme Gradient Boosting machine-learning model,” (Khan et al.) showed high accuracy in predicting risk for hemorrhage. Through early risk detection using models such as the “Extreme Gradient Boosting machine-learning model,” (Khan et al.) the inequities between rural and urban health centers will be reduced by allowing resources to be allocated quickly to help patients who have high risk, regardless of where they live.

Despite all of the individual and systemic benefits offered by the expansion of AI data analysis in medicine, some argue that AI platforms cannot be trusted to store large amounts of data ranging from "genomics, medical history, behaviors, and social data that covers peoples' daily lives" (Johnson et al.) because the data are prone to attacks. In the past, companies have used data in ways that were not part of their original purpose. For instance, "in 2017, 23andMe received regulatory approval to analyze their customers' genetic information for risk of ten diseases" (McKeon). Such expansions of the ability of corporations to use customer data could pose a serious threat to people's privacy, and this data could potentially get into the wrong hands. Insurance companies, in particular, might use "predictive genetic testing to bias selection processes and charge higher premiums" (McKeon). Most of the arguments pointing out privacy concerns hinge on the assumption that data will be susceptible to outside threats. However, these concerns can be mitigated because techniques are currently being developed to protect against such attacks on data. Network security is one such method that has been widely adopted by large corporations. Network security is a "set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies" ("What is Network Security?"). Due to the growing amount of data being generated, network security techniques are becoming increasingly important to address potential data breaches. Network security protects data from "unauthorized personnel," ensures that data is safely transferred across networks, and controls "user behavior" ("What is Network Security?"). However, network security by itself is not a sufficient deterrent to attacks on data. To address this gap, a new technique, called endpoint security, is being designed. Endpoint security is "the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors" ("What is

Endpoint Security?"). Endpoint security differs from network security in that it is a more transparent process and can account for the multitude of possible endpoints that a network reaches ("Why Endpoint Security is Critical"). As healthcare organizations adopt a combination of network and endpoint security, patients' medical data will be significantly protected from outsider attacks, alleviating concerns that arise over the improper use of medical data.

In a world in which AI and technology are becoming ubiquitous, society must look at AI as a tool, which in and of itself is neither beneficial nor detrimental. When used properly, AI has the potential to greatly help individuals by predicting the likelihood of diseases and determining the best treatment plan based on an individual's specific circumstances. As new data analysis techniques are being developed, new methods to protect data are being created as well. Individuals should have faith in the ability of AI models to safely and securely use their data to greatly improve their quality of life. The main goal now is to move AI from research to application, from bench to bedside. Many studies have proven just how valuable of a tool AI is in medicine. Now, how can we leverage this tool to be widely used and seamlessly integrate it into the healthcare process? How can we make sure that all hospitals receive this benefit and not just a select few? Recognizing that AI is a powerful tool is the first step, and implementing it is the next. If we can successfully bring AI into a clinical setting, we would be able to ensure more equitable healthcare for all.

Works Cited

"AI and IoMT spur healthcare industry growth." *Tectales*, 23 Sept. 2018, tectales.com/ai/ai-iomt-spur-healthcare-industry-growth.html.

Degasperi, Andrea, et al. "Substitution mutational signatures in whole-genome-sequenced cancers in the UK population." *Science*, vol. 376, no. 6591, 2022, doi.org/10.1126/science.abl9283.

"High blood pressure (hypertension)." *Mayo Clinic*, 1 July 2021, www.mayoclinic.org/diseases-conditions/high-blood-pressure/symptoms-causes/syc-20373410#:~:text=High%20blood%20pressure%20(hypertension)%20is,problems%2C%20such%20as%20heart%20disease.

Huynh, Elizabeth, et al. "Artificial intelligence in radiation oncology." *Nature Reviews Clinical Oncology*, vol. 17, no. 12, 2020, pp. 771–781, doi.org/10.1038/s41571-020-0417-8.

"Internet of Medical Things Revolutionizing Healthcare." *Alliance of Advanced BioMedical Engineering*, aabme.asme.org/posts/internet-of-medical-things-revolutionizing-healthcare#:~:text=The%20Internet%20of%20Medical%20Things,technology%20systems%20using%20networking%20technologies.

Johnson, Kevin B., et al. "Precision Medicine, AI, and the Future of Personalized Health Care." *Clinical and Translational Science*, vol. 14, no. 1, 2020, pp. 86–93, doi.org/10.1111/cts.12884.

Khan, Mohammad S., et al. "The Quest for Equitable Health Care: The Potential for Artificial Intelligence." *NEJM Catalyst Innovations in Care Delivery*, 22 Dec. 2021, catalyst.nejm.org/doi/full/10.1056/CAT.21.0293.

McKeon, Jill. “CSA Guidance Addresses Security, Privacy Risks of AI in Healthcare.” *HealthITSecurity*, 7 Jan. 2022, healthitsecurity.com/news/csa-guidance-addresses-security-privacy-risks-of-ai-in-healthcare.

“Postpartum Hemorrhage.” *March of Dimes*, www.marchofdimes.org/pregnancy/postpartum-hemorrhage.aspx.

“Precision Medicine Initiative.” *Obama White House Archives*, obamawhitehouse.archives.gov/precision-medicine.

“The potential of artificial intelligence to bring equity in health care.” *MIT News | Massachusetts Institute of Technology*, 1 June 2021, news.mit.edu/2021/potential-artificial-intelligence-bring-equity-health-care-0601.

“Turing test | Definition & Facts.” *Encyclopedia Britannica*, 14 Dec. 2021, www.britannica.com/technology/Turing-test.

Venkatesh, A. Narasima, “Reimagining the Future of Healthcare Industry through Internet of Medical Things (IoMT), Artificial Intelligence (AI), Machine Learning (ML), Big Data, Mobile Apps and Advanced Sensors.” *SSRN Electronic Journal*, 2019, doi.org/10.2139/ssrn.3522960.

“What Is Endpoint Security? How It Works & Its Importance.” *Trellix*, www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html#:~:text=Endpoint%20security%20is%20the%20practice,the%20cloud%20from%20cybersecurity%20threats.

“What is Machine Learning?” *IBM*, 15 July 2020, www.ibm.com/cloud/learn/machine-learning.

“What is Network Security? Defined, Explained, and Explored.” *Forcepoint*,

www.forcepoint.com/cyber-edu/network-security#:~:text=Network%20security%20is%20a%20broad,both%20software%20and%20hardware%20technologies.

"Why Endpoint Security is Critical For Healthcare Cybersecurity." *HealthITSecurity*, 10 Dec. 2021, healthitsecurity.com/features/why-endpoint-security-in-healthcare-is-critical-for-cybersecurity.