YIGAL ARNON & CO.
LAW FIRM

Digital Health – Developments and Challenges

This article explores uses of telemedicine services and AI applications in the health sector, and addresses challenges that are endemic in these technologies.

MORNING, SEPTEMBER 2030

You wake up, it's a regular day. "Mom, I'm not feeling well" yawns the toddler. Hand on forehead. Hmmm... Maybe he's sick. You log into your local telehealth provider, which recommends performing a home swab test. If you don't do it, the provider will automatically inform the toddler's nursery school and he won't be allowed in. Swab the child's throat and process as instructed – the data is on its way to the lab. An alert from the telehealth portal - an artificial intelligence software has analyzed the data and determined that the child is well. Perfect! Off to preschool. In the afternoon the child's temperature rises. The physician's office, automatically alerted by the toddler's wearable bracelet, has already sent an alert that a prescription is on the way. The child's medical insurance has also been notified automatically and sends you a notification that the doctor's prescription will be 85% covered.

While this morning of the future differs significantly from the typical morning in 2020, artificial intelligence (AI), telemedicine and wearables are already integral parts of today's health landscape. By one expert estimate, within ten years the vast majority of surgical procedures will be performed by robots using artificial intelligence and the majority of hospitalizations will be replaced by monitoring and treatment via telemedicine. This article explores uses of telemedicine services, AI applications and wearables in the health sector, and addresses challenges that are endemic in these technologies.

ARTIFICIAL INTELLIGENCE

Artificial intelligence means the performance by a computerized system of tasks that would be considered intelligent were they to be performed by humans.

AI has been implemented in healthcare in patient diagnostic and screening applications, medical data analyses, medical treatment recommendations, pharmaceutical development, and in robots, used to perform surgical procedures. For example, Microbiologists at Beth Israel Deaconess Medical Center demonstrated that AI-enhanced microscopes can be used to identify bacteria quickly and accurately. John Hopkins Hospital partnered with GE Healthcare Partners to implement AI-based systems and predictive analyses in order to better manage patient safety, experience, volume, and movement.

AI-enabled wearables and connectivity devices are bringing diagnostic tools to patients, empowering them to manage their health condition AI fertility software and trackers promote women's health, and AI software and bots are used to treat mental health conditions – a field where there is

TAMAR TAVORY, ADV.
SPECIAL COUNSEL

NETANELLA TREISTMAN, ADV.
PARTNER

YOHEVED NOVOGRODER-SHOSHAN, ADV.
PARTNER

often a scarcity of treatment options.

However, AI's special characteristics raise novel challenges. AI can in certain instances lead to output that is at least partially tainted by prejudice, racism, or sexism. AI's algorithms are trained on certain data sets. Where the data set does not represent the totality of the patient population but only a subset thereof, the AI may make false recommendations or predictions when treating a patient from unrepresented group. According to a study published in Nature, widespread racism was revealed in decision making software used by US hospitals.[1] Therefore, careful attention must be paid to the data set input before adopting recommendations based on artificial intelligence, to ensure that discrimination or faulty presumptions do not lead to poor decisions.

In cases where AI serves as a physician decision support tool, questions are raised as to the delineations of the physicians' responsibility and how much weight will be accorded the software's "judgement," at the expense of the physician's own judgement. This is a challenge that will need to be overcome as the field develops.

Special attention is required in a "black-box" situation, where AI tools are employed but one cannot explain the causality between the input and the output – i.e., we are unable to explain how certain input (medical data on a disease for example) leads to a specific output (such as a recommended treatment). Physicians rely on their experience and on medical literature to explain the linkage between the disease and potential treatments. AI may generate insights and achieve better results than any individual health professional, however, the black-box output does not communicate why a specific course of treatment is recommended. This may leave a health professional lacking the ability to "understand" the AI's recommendation and to explain it to patients.

In addition, a "learning algorithm" improves its performance over time. Therefore, at a later point in time an AI algorithm may reach different conclusions regarding the same case, yielding inconsistent recommendations.[2]

HOW CAN THE CHALLENGES OUTLINED ABOVE BE ADDRESSED OR MITIGATED?

Algorithmic transparency can assist in identifying bias before it affects patients at a large scale. Algorithmic transparency demands that developers should consider explaining the reasoning for and document the following: where did the data come from? How was the data processed? How was the algorithm developed and validated and how does it reach its results? Increased transparency with regard to AI's training data set and algorithms will enable monitoring of both input and output of AI systems to ensure that decisions are unbiased, fair and equitable. This of course may involve a risk of disclosing trade secrets, but there are solutions which can be employed to mitigate this risk.

Another possible solution to the challenges outlined above is explainability. Explainability means use of methods and techniques in applying AI such that the results of the solution can be understood by humans. Explainability is aimed at making AI systems transparent and understandable so that regulators and experts can examine and analyze them. Developers are asked to provide both process-based explanations and outcome-based explanations for that purpose. Explainability can help identify potential bias.

The COVID-19 pandemic has caused a large uptick in proliferation of telehealth services

Currently there's no binding legislation that addresses AI's special characteristics and challenges in medicine (other than the general medical device's regulation).

When AI is embedded in a medical device, or when an AI tool functions as "software as medical device" under United States Food and Drug Administration (FDA) regulations and the European Union Medical Device Regulation (EMDR), it is subject to regulations that apply to medical devices. In Israel, the regulator has historically embraced the FDA and EUMDR approach to medical device regulation, and we can expect the same to be true with respect to regulation of AI products and applications.

The FDA recently published a proposed framework for regulating AI. A particularly noteworthy aspect of it is a pre-certification pilot program in which the FDA first looks at the company rather than primarily at the product, relying on certain companies' robust culture of quality and organizational excellence, as well as their commitment to monitoring real-world performance of their products.

In addition, several EU and US federal bodies have issued practical, mostly non-binding, guidance concerning the use of AI generally, discussing, among other possible solutions, transparency and explainability as reviewed above.[3] While this guidance is not specifically directed to use of AI in the healthcare context, we can expect that future regulatory schemes that target use of AI in the health environment may use this general guidance.

TELEHEALTH

Although use of telehealth technologies has been on the rise in recent years, the COVID-19 pandemic has caused a large uptick in proliferation of telehealth services. Distancing and isolation guidelines in various countries have made in-person visits to healthcare professionals more difficult; the ability to provide healthcare services at a distance has become a valuable tool in providing access to healthcare. A recent survey in the US revealed that 93% of patients were either satisfied or very satisfied with their telemedicine experience, and 92% would use telemedicine in the future.[4]

Telehealth is used to build ground-breaking healthcare tools and together with AI is expected to increase the quality of patient care immensely;

Tele-ultrasound is used to track a pregnancy condition from afar, accompanied by live guidance and an explanation from a telehealth ob/gyn;

Hospitals remotely monitor patients' conditions with mobile medical devices in order to minimize the medical team's exposure. In critical care units, telehealth is used to monitor patients' condition with AI based platform that can predict possible deterioration;

It has been reported that in China, an internet hospital is being established – a centralized 24/7 medical command, staffed by physicians and nurses, that delivers telemedicine services for patients at home or at local medical centers, backed by digital pharmacy services.

Regulatory regimes have responded to the rise of telehealth services by issuing targeted guidance. The US's Coronavirus Aid, Relief, and Economic

Security Act ("CARES Act") aimed at offering economic aid to the American people, included numerous measures intended to encourage the use of telehealth systems. As part of the CARES Act, the Federal Communications Commission provides $200 million in funding to the COVID-19 Telehealth Program.

Even prior to the Covid-19 pandemic, Israel's Ministry of Health issued guidance on how to apply general medical regulations in the telehealth setting. This guidance addressed the following, among other issues: when patients should be referred to face to face treatment, medical confidentiality, patient identification, informed consent, privacy and information security. However, many practical and legal issues are still unresolved.

On the regulatory end, ensuring that telehealth providers are properly accredited- even where a healthcare provider in one country treats a patient in a different country – is important to ensure quality of care and compliance with legal and safety requirements. Perhaps a global licensing framework should be considered which would recognize healthcare providers' licenses outside their home countries.

In addition, legally, it is not clear yet how the "old" liability legal regime will address the new technology. Who is responsible when something goes wrong in a clinical care unit supported by telehealth providers or in a tele-ultrasound guided by a remote physician? How quickly is the physician required to review results of the medical examination and would patient involvement in monitoring herself detract from the physician's responsibility if the monitoring was done in the wrong way? (Probably not).

On the technological end, standardization, connectivity and interoperability between different apps and telehealth platforms are required. Without these, it is and will continue to be very difficult to incorporate and use emerging technologies in healthcare.

These challenges are yet to be met.

WEARABLES AND OTHER PERSONAL HEALTH TECHNOLOGIES

Smart health devices, such as mobile apps, wearable devices, and digital assistants can provide tracking and monitoring, personalized recommendations to users, and even diagnostic services. Wearable devices can track activities and other indicators such as heart rate, temperature, and oxygen levels. Wearable devices can also use AI technology to make health assessments such as early detection of risk factors, and to provide recommendations such as exercise and fitness recommendations. Smart devices can also help patients managing chronic diseases, for example by performing continuous blood sugar tracking for individuals managing diabetes. Telehealth can also benefit from use of smart devices as they may allow healthcare providers to assess patients at a distance by means of such devices. The WHO has rolled out an AI digital health assistant to help individuals quit smoking.

> **A key challenge in the commercialization of digital health technologies such as AI and telehealth is privacy compliance**

However, wireless and wearable medical devices are potentially subject to cyber-attacks that can affect their efficacy and threaten patients' privacy.

In April 2018, the European Commission published a Communication on enabling the digital transformation of health and care in the Digital Single Market which highlights the importance of technology and lays out the context, needs, and recommendations for using digital solutions to improve health and healthcare. Among other issues the Communication encourages collaboration among different EU actors, promotes exchange of information, investment in digital solutions, increased use of data, and use of person-centered digital tools.

The World Health Organization (WHO) has announced the creation of a Department of Digital Health intended to "...maximize opportunities for digital health". In 2019, the WHO has released guidelines entitled "Recommendations on Digital Interventions for Health System Strengthening", which provides an “assessment of the benefits, harms, acceptability, feasibility, resource use and equity considerations” and is intended to provide health policy makers with recommendations and considerations for implementation of digital health solutions.

In September 2019, the US Food and Drug Administration (FDA) issued guidance regarding use of software and hardware in “mobile medical applications”, including wearables. Many wearables are not regulated as medical devices subject to FDA regulation; of those that are subject, the FDA has stated that it only intends to apply regulatory oversight in cases where there may be a risk to patient safety in the case of malfunction.

Wearables are often used together with artificial intelligence, which accelerates their performance, and are often used as platforms for telehealth, both in hospitals and in patients houses. Wearables are expected to change the face of healthcare provision, personalizing it and increasing accessibility of care within patients’ home.

The extent to which offshore providers of digital health technologies that involve the handling of data of Israeli data subjects are subject to Israeli privacy law is unclear

The use of wearables raises additional questions relating to patient involvement and its effect on healthcare providers’ responsibility. When is the healthcare provider required to intervene? What is the patient’s role in handling electronic health records and what are the patient’s rights in these records? What special training should be mandated for medical staff? However, a primary issue concerning wearables are the risks of infringement of privacy; these risks are discussed below.

PRIVACY

A key challenge in the commercialization of digital health technologies such as AI, telehealth and wearables is privacy compliance. AI, telehealth applications and wearables all involve the collection, processing and transfer of large amounts of personal data. Where a digital health solution is deployed in a cloud environment across country borders, solution providers must consider the privacy requirements of the country in which the data subject is located as well as each country in which data are collected, processed, and stored.

The GDPR governs processing of personal data in the EU, as well as processing of data of EU individuals (“data subjects”) regardless of the location of the processing, or the location of the data controller or data processor. Since health data is considered particularly sensitive data, it is subject to certain additional restrictions compared to non-sensitive personal data.

Data controllers and data processors are subject to different requirements under the GDPR. A “data controller” determines the purposes and means of processing. A “data processor” processes data solely on behalf of a controller and not for its own purposes. Data controllers must ensure that they have a legal basis for processing data; the GDPR provides a list of legal bases for processing, one of which must be met in order for the processing to be lawful. Since the uses of personal data must be identified and legitimized prior to processing, secondary use of personal health data – such as for medical research – requires an independent legal basis. For example, personal data may be collected on the legal basis of explicit and informed consent between a doctor in a private clinic and a patient for the purpose of medical diagnosis. Where the doctor or the private clinic may then want to engage in secondary use of the data for research purposes – for example to analyze trends across all patients – this secondary use of data will often require separate explicit data subject consent. The GDPR also requires adequate data security measures and regulates transfers of personal data of EU data subjects to recipients outside of the EU.

In Israel, privacy and data protection is governed by the Protection of Privacy Law-1981 (Privacy Law), various regulations, sector-specific laws that target health information and regulator-issued directives.

Unlike the GDPR and certain other national data protection laws, the Privacy Law and attendant regulations are silent on the law's territorial scope, and to date, the Israeli regulator has not issued guidance on how the Privacy Law and attendant regulations are to be applied to cloud-based technologies. The extent to which offshore providers of digital health technologies that involve the collection, export and processing of data of Israeli data subjects are subject to Israeli privacy laws is unclear. Unlike the GDPR, the Israeli Privacy Law does not dictate legal bases for processing. Instead, the 'purpose limitation' governs data use – ie – personal data may be used only for the purpose for which it is provided by the data subject, though defenses are available that justify processing on public interest and other grounds. Processing for other purposes including secondary use of identified medical data generally requires data subject consent. Like the GDPR, the Israeli regime adopts principles such as notice requirements and data security requirements (which are far more granular than the GDPR general guidance and data export restrictions). The regulation of secondary use of health data is in flux, and legislative proposals in this area have been proposed.

One advantage enjoyed by Israeli cloud services providers is the EU adequacy ruling, which since 2011 has designated Israel's domestic law as guaranteeing an adequate level of protection for the processing of personal data. This inclusion on the EU 'white list' of adequate countries enables the transfer of personal data from the EU to Israel without special arrangements; for purposes of GDPR, data transfers from the EU to Israel are treated as substantially equivalent to transfers from one EU country to another. This designation is particularly helpful to the deployment of Israeli digital health solutions in the EU, and holds particular significance in the wake of the decision of the European Court of Justice in July 2020 which invalidated the European Union (EU) -United States (US) Privacy Shield Framework.

There is no question that AI, telemedicine and wearables have the potential to increase the quality of patient care and patient well-being. As AI and telemedicine tools gain acceptance, regulators, healthcare institutions and patients will continue to grapple with the issues discussed above. ■

NOTES

[1] See Heidi Ledford "Millions affected by racial bias in health care algorithm." Nature 31, Oct. 2019

[2] For a detailed analysis of AI in medicine, see Keidar Roy & Tavory Tamar, "Legal and Regulatory Aspects of AI in Medicine" in *Emerging Technologies: The Israeli Perspective* (Lior Zemer, Dov Greenbaum and Aviv Gaon, eds, Nevo 2021) (Heb) to be published.

[3] Examples of AI's guidance include:
The FTC Guidance on Using Artificial Intelligence and Algorithms April, 2020 - https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms;

The White House's Draft Guidance for Regulation of Artificial Intelligence Applications July, 2019 - https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf;

Ethics Guidelines for Trustworthy AI, High-Level Expert Group on Artificial Intelligence Apr. 2019 (non binding) - https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai;

White Paper on Artificial Intelligence – A European approach to excellence and trust, The European Commission February, 2020 - https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf;

The Information Commissioner Officer in the UK and The Alan Turing Institute, Practical Guidance for Organizations on Explaining AI, June 2020 - https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/

[4] https://metova.com/survey-high-demand-telemedicine/

ABOUT THE AUTHORS

Yoheved Novogroder Shohan, Adv.
Partner, High Tech and Life Sciences Practice Group
Email: yohevedn@arnon.co.il

Netanella Treistman, Adv.
Partner, High Tech and Privacy Practice Group
Email: netanellat@arnon.co.il

Tamar Tavory, Adv.
Special Counsel, Life Sciences and Digital Health Practice Group
Email: tamart@arnon.co.il

Yigal Arnon & Co. Law Firm
22 Rivlin Street, Jerusalem 94240, Israel
Tel: +972 3 608-7777
Fax: +972 3 608-7724
www.arnon.co.il