Addressing Access with Artificial Intelligence: Overcoming the Limitations of Deep Learning to Broaden Remote Care Today

DR. BARRY SOLAIMAN*

I. INTRODUCTION

A shift is underway in the delivery of care to individuals. The traditional method of patients meeting with their doctor in a clinic or hospital is evolving—digital health technologies encompassing artificial intelligence ("AI") are enabling greater access for patients, with monitoring and prevention being seen as the future norm for care.[1] In this manner, there is a greater emphasis on providing constant care to individuals while they are on the move using technologies that enable patients to proactively manage their health throughout the day and take care of their wellbeing.[2] There is a greater emphasis on home care premised on independent and healthy living that utilizes technology to monitor patients at home and deliver care there, rather than in a hospital.[3] The role of primary and community care providers is also evolving to encourage the use of health technologies for care on the move or at home. The aim is to lessen the burden on residential and hospital care providers, lower costs, and emphasize prevention through broadening access to mobile care. This is all possible because AI can analyze patient data anywhere in the world, as long as there is an internet connection available to transmit patient data from a device to the cloud and servers for processing. Prior to the COVID-19 pandemic in 2020, there was already greater uptake of such technologies in various jurisdictions. For example, National Health Service ("NHS") trusts in the United Kingdom had signed long-term contracts for the broad use of wearable devices utilizing AI to provide remote care to patients.[4] Telemedicine has long been established as a means of delivering care in

---

1.   *See* Eur. Health Telematics Ass'n, *Exploring Digital Therapeutics, Artificial Intelligence, and Virtual Coaches*, EHTEL (June 3, 2020), https://www.ehtel.eu/18-articles/67-digital-therapeutics-artificial-intelligence-and-virtual-coaches.html.

2.   *See id.*

3.   *See id.*

4.   *See* Laura Donnelly, *NHS Experiment in AI Will See Whole City Offered Virtual Hospital Appointments and Diagnosis by Chatbot*, TELEGRAPH (Jan. 23, 2020), https://www.telegraph.co.uk/news/2020/01/23/nhs-experiment-ai-will-see-whole-city-offered-virtual-hospital/.

the United States and Canada.[5] Digital therapeutics are spouting. The boom in wearable fitness trackers monitoring vital signs such as a person's heart rate has precipitated for years. Virtual assistants can now monitor and advise patients from their homes. Recent developments indicate a greater move towards the use of such health technologies. The pandemic has resulted in health bodies, hospitals, and doctors not only leaning on health devices, but relying on them, for delivering basic care.[6] The potential implications expand to both clinical practice and health research.

This Article considers how health technologies using AI can be used to expand access to care today within existing regulatory confines in the United States. Embedded within that discussion are legal and ethical considerations that are important to the facilitation of such technologies for providing care. There will be regulatory changes in the years to come, and it is beneficial to highlight where the law currently stands. In this regard, this Article provides a modest overview of remote care solutions and a guide to three central legal considerations that arise in using AI for remote care. These considerations should form part of the criteria used to evaluate any exploratory discussions for new health devices.

---

5.   Telemedicine can be traced back to 1879 in the United States. *See* Thomas S. Nesbitt*, The Evolution of Telehealth: Where Have We Been and Where Are We Going?*, *in* The Role of Telehealth in an Evolving Health Care Environment: Workshop Summary 11, 11 (Tracy A. Lustig ed., 2012), https://www.ncbi.nlm.nih.gov/books/NBK207145/pdf/Bookshelf_NBK207145.pdf. For Canada, remote consultations have been utilized since the 1970s. *See* Canadian Med. Ass'n, CMA Health Summit, Virtual Care in Canada: Discussion Paper 3 (2019), https://www.cma.ca/sites/default/files/pdf/News/Virtual_Care_discussion-paper_v2EN.pdf; *see also* Jocylene Picot, *Telemedicine and Telehealth in Canada: Forty Years of Change in the Use of Information and Communications Technologies in a Publicly Administered Health Care System*, 4 Telemedicine J. 199, 199–205 (1998), https://doi.org/10.1089/tmj.1.1998.4.199.

6*.   See generally* Niels Peek et al., *Digital Health and Care in Pandemic Times: Impact of COVID-19*, BMJ Health & Care Informatics (June 21, 2020), https://informatics.bmj.com/content/bmjhci/27/1/e100166.full.pdf (discussing digital health technologies following the pandemic). *See, e.g.*, Ahmad A. Aalam et al., *Remote Patient Monitoring for ED Discharges in the COVID-19 Pandemic*, 38 Emergency Med. J. 1, 1–3 (Jan. 20, 2021), https://emj.bmj.com/content/emermed/38/3/229.full.pdf (discussing the utilization of remote care solutions in emergency departments during the pandemic).

To anchor this discussion, I would like to contextualize the premise around which the analysis rotates. It is not uncommon to hear that AI, like stem cell research before it, is merely hype, with its potential applications being "exaggerated."[7] Indeed, the potential for AI is exciting, but one must not get overexcited. Taking a step back, it can be seen that AI is predominantly in the "Innovation Trigger" or, in some circumstances, the "Peak of Inflated Expectations" in the Gartner Hype Cycle.[8] It is also true that hyperbolic attention can detract from the important ethical and legal discussions that are necessary. AI is not a panacea, and the public ought not to be misled about its benefits. Caution ought to be exercised in encouraging "premature or unwarranted clinical use."[9] I should bring your attention to a particularly potent statement by the Director of the U.S. Defense Department's Advanced Research Projects Agency who said of AI: "They can be tricked easily. There are lots of folks looking at how you would trick an AI system, we're starting to look at that, and from the initial things I've seen, it doesn't take a lot to trick an AI system."[10] It should also be emphasized that, so far at least, regardless of the AI system used (which are explored below), much human involvement is needed in the healthcare context.[11]

Nevertheless, despite all those important disclaimers, the "hype" surrounding AI is different to other areas such as stem cell

---

7.   *See* I. Glenn Cohen, *Informed Consent and Medical Artificial Intelligence: What to Tell the Patient?*, 108 GEO. L.J. 1425, 1468–69 (2020) (citing Timothy Caulfield et al., *Confronting Stem Cell Hype*, 352 SCI. MAG. 776, 776 (2016), https://iscrm.uw.edu/wp-content/uploads/2018/06/ScienceMay16.pdf), https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3631992_code358116.pdf?abstractid=3529576&mirid=1.

8.   Laurence Goasduff, *Top Trends on the Gartner Hype Cycle for Artificial Intelligence, 2019*, GARTNER (Sept. 12, 2019), https://www.gartner.com/smarterwithgartner/top-trends-on-the-gartner-hype-cycle-for-artificial-intelligence-2019/.

9.   *See* Caulfield et al., *supra* note 7, at 777.

10.   Jory Heckman, *DARPA: Next Generation Artificial Intelligence in the Works*, FED. NEWS NETWORK (Mar. 1, 2018, 6:54 PM), https://federalnewsnetwork.com/technology-main/2018/03/darpa-next-generation-artificial-intelligence-in-development/.

11.   Barry Solaiman & Mark Bloom, *AI, Explainability, and Safeguarding Patient Safety in Europe: Towards a Science-Focused Regulatory Model*, *in* THE FUTURE OF MEDICAL DEVICE REGULATION: INNOVATION AND PROTECTION (Christopher Robertson & Carmel Shachar eds., 2021).

research. While much human involvement is needed at present, that paradigm is changing. It used to be the case that an AI system required human data, domain knowledge, and known rules to operate or make a prediction.[12] These requirements could be seen with Google Deep-Mind's AlphaGo, which initially required all three to play Go.[13] However, DeepMind's latest iteration, called "MuZero," has achieved mastery in Go, Chess, Shogi, and Atari video games—without any human data, any domain knowledge, nor any rules.[14] We are already at the stage where AI systems "learn" rules without human interaction.[15] As Professor Wendy Hall has stated, these developments are "quite astounding."[16] While such advances will take time to proliferate into the sphere of health, it is unlikely that we will see a retreat from the AI technologies already in use in healthcare, which are analyzed below. That is the premise of this Article: Yes, AI should not be overhyped, but its applications in healthcare are not significantly overhyped. The analysis below demonstrates that AI appears to be a real, growing, and important factor in healthcare—all the more reason why legal and ethical analyses are needed.

In examining the potential issues surrounding AI and remote care, this Article is divided into three parts. Following this Introduction, Part II is a discussion of what AI is. Part III is an analysis of existing remote care technologies. Part IV outlines three existing regulatory issues concerning the use of AI for the provision of remote care. Namely, I have focused on data protection, informed consent, and medical liability.[17] Overall, the aim is for this Article to highlight how AI technologies can provide remote care to patients. The pandemic will inevitably lead to discussions about how AI can be leveraged to deliver remote care in circumstances where in-person care raises risks of infections spreading. Healthcare leaders are more willing than ever to extend access to care by remote means both in the short and long term,

---

12. Leo Kelion, *DeepMind's AI Agent MuZero Could Turbocharge YouTube*, BBC News (Dec. 23, 2020), https://www.bbc.com/news/technology-55403473.

13. *Id.*

14. *Id.*

15. *Id.*

16. *Id.*

17. There are other issues that I point to in this Article, but the focus is narrowed to these three areas because of the important considerations they raise for remote care technologies using AI.

and the factors analyzed here are intended to frame some key legal considerations surrounding those efforts.[18] Finally, Part V concludes by arguing that while AI can be used to broaden remote care within the existing regulatory framework, relevant stakeholders ought to implement more robust practices concerning data protection, informed consent, and medical liability, in anticipation of regulatory changes in the future.

II. A Brief Explanation of AI

The seeds of AI were sewn in the 1940s.[19] Like all technologies, AI could initially only perform rudimentary tasks. Since then, the technology has advanced to not only play games like Chess, but to beat human players at games like Chess. The first foray into the use of AI in the health context was in the 1970s when a system called DENDRAL was used to assist in identifying molecules (that system formed the basis for a later development called MYCIN which was used for diagnosing blood infections).[20] Despite the decades long history, it is only recently that mainstream attention has been given to the use of AI in healthcare. Today, AI is used in and alongside electronic health records, diagnostic systems, robotics, telemedicine, wearables, and more.[21]

To understand how AI works (while avoiding delving too deeply into the technical abyss), it is helpful to analogize a human

---

18.   I should note that this Article is limited to the remote applications of health technologies and not in-person care, such as AI being used in surgical procedures. Further, in-person interventions, such as surgical procedures, raise separate doctrinal considerations which are beyond the scope of this Article. For example, informed consent case law in the United States is predominantly focused on surgical interventions rather than diagnoses or other aspects of care. *See* Cohen, *supra* note 7, at 1444.

19.   For a history, see STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 16–28 (3d ed. 2010).

20*.   See id.* at 23; *see also* Robert K. Lindsay et al., *DENDRAL: A Case Study of the First Expert System for Scientific Hypothesis Formation*, 61 A.I. 209 (1993).

21.   For electronic health records, see generally Sebastian Vollmer et al., *Machine Learning and Artificial Intelligence Research for Patient Benefit: 20 Critical Questions on Transparency, Replicability, Ethics, and Effectiveness,* BMJ (Mar. 20, 2020), bmj.com/content/368/bmj.l6927 (the other items highlighted will be exampled under Part III of this Article below).

brain.[22] The brain receives inputs through the senses such as sight, sound, smell, touch, and taste. It processes these inputs and produces an output. For example, someone throws a ball at you which you see with your eyes. Your brain processes this action and activates your nerves and muscles which lead to you jumping out of the way. At a very basic level, AI operates in a similar way. However, before moving forward, some terminological calibration is necessary. The terms "machine learning" and "deep learning" are often discussed alongside AI. Machine learning is a form of AI.[23] Some (but not all) forms of machine learning systems are "supervised" and "unsupervised" networks. The former requires more human input than the latter. "Deep learning" is another term which often arises. It is a subset of machine learning that can be used with supervised or unsupervised systems.[24] It is more sophisticated and is, therefore, useful for complex healthcare applications. The networks used in deep learning systems are called artificial neural networks ("ANN").[25]

Returning to the brain analogy—AI utilizes artificial neural networks which can be thought of as the brain of AI. Consider the example of an ANN containing three layers—an input layer, a middle "hidden" layer, and an output layer. Those layers are connected by electronic neurons (i.e., nodes) that send "signals" to one another using mathematical equations (such as sigmoid functions). Like a human brain, an ANN also receives inputs and produces outputs. One straightforward use of AI is in diagnostics. Networks have been trained to detect the early stages of lung cancer.[26] The network is provided with thousands of CT scans of healthy and diseased lungs. Those images are provided to the "input layer" (or the first layer of the network)

---

22.   For a slightly more technical explanation, see Solaiman & Bloom, *supra* note 11; I emphasize that this is merely a simplistic analogy. Biological neurons rarely correspond to "nodes" used in computing. *See* Ron Sun, *Connectionism and Neural Networks*, *in* THE CAMBRIDGE HANDBOOK OF ARTIFICIAL INTELLIGENCE 108–09 (Keith Frankish & William M. Ramsey eds., 2014).

23.   As such, the terminology "AI/ML" is often adopted. However, this Article will simply refer to "AI" which also captures "AI/ML".

24*.   See* RUSSELL & NORVIG, *supra* note 19, at 830.

25.   For an analysis of ANNs, see Anders Krogh, *What Are Artificial Neural Networks?*, 26 NATURE BIOTECH., 195–97 (2008), https://doi.org/10.1038/nbt1386.

26.   Elizabeth Svoboda, *Artificial Intelligence Is Improving Detection of Lung Cancer: Machine Learning Systems for Early Detection Could Save Lives*, NATURE (Nov. 18, 2020), https://www.nature.com/articles/d41586-020-03157-9.

which then propagates the image through numerous hidden layers performing mathematical equations. At the end of the network is the "output layer" (or the final layer of the network) which gives a prediction or recommendation.

Some networks are trained quite vigorously initially so that a human being will provide feedback, telling the network if it has erred. For example, the network might indicate that an image shows a healthy lung, but the image actually shows a confirmed cancer case. The human being training the network will provide feedback, indicating that the network chose the wrong output. At this point, the network "back-propagates" that feedback. Thus, moving from the output layer back through the middle layers to the input layer (recalibrating the mathematical decisions it initially made along the way). The network will propagate forward again with more accurate equations and, therefore, a greater likelihood of choosing the correct output next time. Through an analysis of thousands of images, the network's calibration becomes so fine-tuned and sophisticated, that it surpasses human analyses, detecting traits common to a positive cancer diagnosis that are undetectable to the human eye assessing the scan.[27] Through that process, AI networks have become more accurate than humans in diagnosing illnesses.[28] CT scans which might have been dismissed by doctors because they did not raise any concerns from a human visual analysis, would raise an alert when analyzed by AI.[29]

The consequences of approved medical devices encompassing AI are significant because care can be provided remotely, and disease may be diagnosed months or years earlier than a human check-up. Early detection of disease in these circumstances is associated with much better survival odds.[30] It should also be apparent that the success of AI networks depends on the quantity and quality of available data.

---

27.   *See* Sara Reardon, *Rise of Robot Radiologists*, 576 NATURE S55, S56 (Dec. 26, 2019), https://media.nature.com/original/magazine-assets/d41586-019-03847-z/d41586-019-03847-z.pdf.

28.   *See* Diego Ardila et al., *End-to-End Lung Cancer Screening with Three-Dimensional Deep Learning on Low-Dose Chest Computed Tomography*, 25 NATURE MED. 954 (May 20, 2019).

29*.   See* Svoboda, *supra* note 26.

30.   This can be seen with cancer diagnoses, for example. *See, e.g.*, Nigel Hawkes, *Cancer Survival Data Emphasize Importance of Early Diagnosis*, BMJ (Jan. 25, 2019).

A significant reason why AI has grown in health in recent years is owing to the boom in big data from a plethora of sources which can be used to train AI.[31] The uses of AI in health move far beyond the diagnosis of CT scans. Those technologies are highlighted below to set up a discussion concerning regulations.

III. HEALTH TECHNOLOGIES ENCOMPASSING AI

There is an ever-growing expansion of promising health technologies encompassing AI. These technologies are being used today to enhance the provision of remote care in multifaceted ways. This Part outlines the existing integration of technology within the health sector for preventing illnesses, managing health conditions, and monitoring patients. The technologies described here are not general health and wellness apps one would find on an app store. Instead, the focus is on technologies used by providers in the provision of health services to patients. The distinction is that the former involves the collection of user data to provide information or recommendations to an individual independent of the inputs of a qualified medical professional. The latter is a tool used by providers to deliver direct and continuing care to patients through an ongoing care or research experience. The technology described below is exciting, but it bears repeating here that AI is not a panacea for remote care; its limitations will be highlighted along with its potential.

A. Telemonitoring & Wearable Devices

The first relevant category concerns devices used for tele-monitoring. In other words, devices that are used for monitoring patients at a distance by transmitting sensor data back to the cloud.[32] For example, Omron has developed a blood pressure monitor called HeartGuide,

---

31. Indeed, big data is enabling a significant upscale in the capability of AI. *See* Randy Bean, *How Big Data is Empowering AI and Machine Learning at Scale*, MICH. INSTIT. OF TECH. SLOAN MGMT. REV. (May 8, 2017), https://sloanreview.mit.edu/article/how-big-data-is-empowering-ai-and-machine-learning-at-scale/.

32. There are various technical methods and approaches to the transmission, processing, and analysis of such data. For an overview of these approaches, see generally Erwin Adi et al., MACH. LEARNING & DATA ANALYTICS FOR THE IOT (June 30, 2020) (unpublished manuscript), https://arxiv.org/pdf/2007.04093.pdf.

which is worn on the wrist.[33] HeartGuide is approved by the U.S. Food and Drug Administration ("FDA") for users to wear and track their blood pressure at any time. The strap collects readings and uses AI to provide users with insight into their blood pressure levels which can also be shared with a doctor.[34] The device is a microcosm of the developments in wearable tech more generally. The miniaturization of hardware in this and similar devices has allowed oscillometric measurements to be undertaken in ways not possible in the past. Another example is Biosticker by BioIntelliSence.[35] It combines data from different sensors to detect symptoms such as coughing, sneezing, and vomiting.[36] There are a myriad of other wearable sensors that have been created or are currently in development, such as those predicting Alzheimer's disease, those which can detect cancer cells,[37] and those which can monitor abnormal gait patterns to predict a stroke before its onset.[38]

These uses are not hypothetical. In the United Kingdom, the NHS successfully piloted a program called "Current Health," which involved fitting discharged patients with a wearable device on their arm to monitor their vitals such as heart rate, oxygen levels, blood pressure,

---

33.   *The 100 Greatest Innovations of 2019*, POPULAR SCI. (Dec. 3, 2019), https://www.popsci.com/story/technology/best-of-whats-new-2019/.

34.   *Omron Healthcare and PhysIQ Partner to Transform Cardiovascular Patient Care*, OMRON (Feb. 6, 2019), https://omronhealthcare.com/2019/02/omron-healthcare-physiq-partner-transform-cardiovascular-patient-care/.

35.   Conor Hale, *Tracking Not Just Data, but Individual Symptoms, Like Vomiting: BioIntelliSense Exits Stealth with FDA-Cleared Wearable*, FIRECEBIOTECH (Jan. 28 2020), https://www.fiercebiotech.com/medtech/biointellisense-exits-stealth-fda-cleared-wearable-tracks-individual-symptomatic-episodes.

36.   *Id.*

37.   Jack Carfagno, *Five New and Emerging Wearable Medical Devices*, DOCWIRE (Dec. 2, 2019), https://www.docwirenews.com/docwire-pick/future-of-medicine-picks/top-5-wearable-medical-devices/; *see also* Nida Shahid et al., *Applications of Artificial Neural Networks in Health Care Organizational Decision-Making: A Scoping Review*, PLOS ONE (2019), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0212356.

38.   Fei Jiang et al., *Artificial Intelligence in Healthcare: Past, Present and Future*, STROKE & VASCULAR NEUROLOGY 230, 240 (2017) (citing Andrea Mannini et al., *A Machine Learning Framework for Gait Classification Using Inertial Sensors: Application to Elderly, Post-Stroke and Huntington's Disease Patients*, SENSORS (Jan. 21, 2016)), https://svn.bmj.com/content/svnbmj/2/4/230.full.pdf.

body temperature, and more.[39]   Through their device, the company claims that their "AI-powered algorithms stratify patients by risk and flag early signs of health deterioration to help prioritize treatment for the patients who need it most."[40] The pilot in the United Kingdom led to a 22% fall in home visits, saving significant costs.[41]   In 2019, the same device received "the first-ever FDA clearance for end-to-end, real-time, passive [remote patient monitoring] wearable and plat-form."[42] It was initially piloted in Mount Sinai Hospital in New York.[43] In late 2020, it was announced that the same system would be expanded at the same hospital to monitor cancer patients. [44]   Those undergoing chemotherapy are at a high risk of infection, meaning that their home is a safer environment than a hospital.[45] Wearable devices can facilitate the remote care of such high-risk groups, particularly during a pandemic when those risks are heightened. Despite these uses, it should be emphasized that the uptake of these technologies is in its infancy. Most of the programs discussed are pilot programs. The long-term efficacy and benefits are yet to be established. It is also unclear, in the long term, whether patients would be satisfied using wearable devices in lieu of direct care with their doctor. Nevertheless, the proliferation of wearables and the benefits yielded so far are promising indications of their future success.

B. Telemedicine Consultations & Home AI Diagnostics

Other applications for remote care involve online telemedicine consultations. The pandemic has resulted in a significant shift towards

---

39.   Moni Miyashita & Michael Brady, *The Health Care Benefits of Combining Wearables and AI*, HARV. BUS. REV. (May 28, 2019), https://hbr.org/2019/05/the-health-care-benefits-of-combining-wearables-and-ai.

40*.   See Transition Healthcare from the Hospital to the Home*, CURRENT HEALTH, https://currenthealth.com (last visited May 26, 2021).

41.   Miyashita & Brady, *supra* note 39.

42.   Dave Muoio, *FDA Clears Current Health's Remote Monitoring Platform for Home Use*, MOBIHEALTHNEWS (Apr. 24, 2019), https://www.mobihealth-news.com/content/fda-clears-current-healths-remote-monitoring-platform-home-use.

43.   Miyashita & Brady, *supra* note 39.

44.   Jasmine Pennic, *Mount Sinai to Deploy Current Health's RPM Solution to Enhance Oncology Patient Care*, HIT CONSULTANT (Dec. 15, 2020), https://hitcon-sultant.net/2020/12/15/mount-sinai-current-health-rpm/#.X-20aZ5R1PY.

45*.   See id.*

telemedicine, which is likely to persist.[46] Instead of meeting with a doctor face-to-face, many consultations have been arranged by phone or video chat to avoid the risk of COVID-19 spreading. Beyond the pandemic, the benefits are potentially significant. Consider an individual living remotely on a farm where access to care is limited or where there is a lack of experts in a specific sub-field of health residing in the patient's nearest town. There are also efficiency gains in terms of waiting lists, referrals, and so on.

For the most part, AI is not involved in telemedicine consultations involving a doctor and patient in a live discussion. However, the scope for AI is increasing in the areas of clinical assessment and evaluation, tele-diagnosis, virtual assistants, and remote patient monitoring.[47] For clinical assessments, certain questions could be integrated into the telemedicine platform which prompt a clinician to ask relevant questions for specific health complaints.[48] For diagnosis, tele-dermatology, in particular, has the potential to make inroads. The hope is that patients can use a smartphone app to take a photograph of a skin lesion which could be analyzed by the AI algorithm to determine whether it is cancerous.[49] That computational deep learning analysis could be immediately shared with the doctor who would then be able to make a rapid decision about the appropriate next steps. Thus far, a mobile phone alone is not enough, but patients have been equipped with portable dermatoscopes (that magnify, capture, and transfer the image remotely) for use with their cell phones.[50] While these uses are limited at present and cannot replace proper in-person consultations, consider the potential benefits for our friend residing on that farm.[51] An

---

46.   *See generally* Barry Solaiman, *COVID-19 and the Shift Towards Telemedicine: Developing a Regulatory Foundation in a Post-Pandemic World,* 2 QATAR BUS. L. REV. 7 (2020).

47.   Craig Kuziemsky et al., *Role of Artificial Intelligence Within the Telehealth Domain*, YEARBOOK OF MED. INFORMATICS 35, 36–38 (2019).

48.   *Id.* at 37.

49.   Mulin Xiong et al., *Artificial Intelligence, in* DERMATOLOGY 85–86 (2019).

50.   Monika Janda et al., *Lesion Selection by Melanoma High-Risk Consumers During Skin Self-Examination Using Mobile Teledermoscopy*, 150 J. OF AM. MED. ASS'N DERMATOLOGY 656, 656 (2014).

51.   For a recent overview of the diagnostic success rate of tele-dermatology, see Arthur Martin & Pascale Guitera, *Teledermatology for Skin Cancer: The Australian Experience*, 9 CURRENT DERMATOLOGY REP. 43 (Mar. 3, 2020); *see also* Xiong, *supra* note 49, at 88.

appointment and diagnoses in the face-to-face setting could have taken weeks or months when time is of the essence. While I have exampled tele-dermatology, there are other offshoots garnering much attention too, such as tele-psychiatry, tele-pathology, and tele-radiology, among others.[52]

This technology points towards a future in which AI can be combined with telemedicine consultations to enhance remote care. The shoots of that future are beginning to sprout, but the challenge, at present, is improving the technology so that clinicians have access to high quality scans or other diagnostic information. Currently, as noted above, there is good success with the use of AI for predicting or identifying illness when analyzing high quality scans obtained in a clinical setting.[53] For example, AI networks have been used to analyze ocular images to diagnose cataract disease, identify skin cancer from clinical images, and detect diabetic retinopathy through retinal fundus photographs.[54] In remembering to keep out excitement in check, it should be argued that it is highly unlikely that mobile devices will be able to produce ocular images, never mind without an expert present to ensure good images are produced. However, handheld devices which can be mounted onto mobile phones to take high-quality retinal pictures are being tested.[55] It is clear that devices will advance, offering more options for obtaining data at home which can be shared remotely for AI analysis. Those diagnostics may, in the future, be used more widely than before during remote telemedicine consultations.

---

52. Kuziemsky et al*., supra* note 47, at 35.

53*. See* Reardon, *supra* note 27.

54*. See* Jiang et al., *supra* note 38, at 238 (citing Erping Long et al., *An Artificial Intelligence Platform for the Multi-Hospital Collaborative Management of Congenital Cataracts*, Nature Biomed. Eng'g 1 (2017)); *see also* Andre Esteva et al., *Dermatologist-Level Classification of Skin Cancer with Deep Neural Networks*, 542 Nature 115 (2017); Varun Gulshan et al., *Development and Validation of a Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs*, 316 J. of Am. Med. Ass'n 2402 (2016).

55*. See* Shelley Zalewski, *Earlier Detection of Diabetic Retinopathy with Smartphone AI*, Mich. Health Lab (Apr. 29, 2019), https://labblog.uofmhealth.org/health-tech/earlier-detection-of-diabetic-retinopathy-smartphone-ai.

C. Virtual AI Assistants

Virtual assistants are another means of AI technology providing remote care. An interesting example of such a program in development is "Cardiac Coach" which is designed to support those recovering from cardiac health problems.[56] The software allows an individual to have a discussion with a human-like assistant on their computer.[57] The concept video of the software is ambitious, showing an AI assistant that can detect emotion in the tone of a person's voice, provide sympathy, ask targeted questions about medications, give recommendations, set reminders to meet with a doctor, and more.[58] While the program may or may not come to fruition as intended, it paints a picture of what the future may look like. More sophisticated conversational AI programs are able to draw upon a broad knowledge base of information, apply contextual acuity, recall previous interactions with the patient, and draw on their medical records.[59] A physical manifestation of this technology would be with robots providing home care in lieu of nurses.[60] The elder care function of such robots involves providing reminders, agenda posology, monitoring, telepresence, and social interaction to help with loneliness.[61] There are also simpler methods of delivering virtual assistance through chatbots which can respond to written or spoken queries and provide recommendations for the user.[62] These are relatively unsophisticated uses of AI, but they can be helpful solutions for basic remote assistance. The benefits are potentially significant for those who are cognitively impaired because, by offering alternative

---

56. *See Cardiac Coach*, UNEEQ, https://digitalhumans.com/casestudies/cardiac-coach/ (last visited May 26, 2021).

57. *See* UneeQ Digital Humans, *UneeQ's Digital Human Cardiac Coach Will See You Now*, YOUTUBE (Sept. 16, 2020), https://www.youtube.com/watch?v=lwnPxcHoK0E&feature=emb_imp_woyt.

58. *See id.*

59. *See* Kuziemsky et al., *supra* note 47, at 38.

60. *See* Nancy Robert, *How Artificial Intelligence Is Changing Nursing*, 9 NURSING MGMT. 30 (2019).

61. *See e.g.*, *Buddy the First Emotional Companion Robot*, BUDDY THE EMOTIONAL ROBOT, https://buddytherobot.com/en/buddy-the-emotional-robot/ (last visited May 26, 2021).

62. Kuziemsky, *supra* note 47, at 38.

means of communication that the user can take their time to prepare, it is improving accessibility for them.[63]

The use of virtual assistants to provide remote care is quite dependent on the investments made by providers and the willingness of patients to use them. People generally seem to prefer to speak to a human being rather than a robot, but these assistants are becoming rather nuanced and advanced, equipped with the ability to carry out sophisticated conversations. Google Duplex demonstrated these conversational advancements, with its assistant able to call and book restaurant appointments, dealing with complex conversations in a realistic manner.[64] Cardiac Coach demonstrates similar natural language understanding which may be able to overcome the hesitancy of some to use it. For now, there are virtual assistants which can help with providing remote care, but they are limited.

IV. REGULATORY LIMITATIONS FOR REMOTE ACCESS?

This Part outlines the existing regulatory architecture governing the use of AI and other health technologies. In places, this Part refers to a helpful legal and ethical framework provided by Sara Gerke, Timo Minssen, and Glenn Cohen to examine whether and how that architecture applies to existing technologies.[65] In terms of the overarching approach to the governance of AI in the United States, there have been several important developments since 2018. Gerke, Minssen, and Cohen summarize those well, but an even shorter summary is provided here.[66]

While the United States does not presently have a general AI strategy,[67] the White House Summit on Artificial Intelligence for

---

63. *Id.*

64. *See* Yaniv Leviathan & Yossi Matias, *Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone*, GOOGLE AI BLOG (May 8, 2018), https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html.

65. *See* Sara Gerke et al., *Ethical and Legal Challenges of Artificial Intelligence-Driven Healthcare*, *in* ARTIFICIAL INTELLIGENCE IN HEALTHCARE 295, 296 (Adam Bohr & Kaveh Memarzadeh eds., 2020).

66. *See id.* at 296–99.

67. *See* Tim Dutton, *An Overview of National AI Strategies*, MEDIUM (June 28, 2018),   https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd.

American Industry in 2018 emphasized that the United States' leadership in AI will be characterized by its "free market approach to scientific discovery."[68] An overarching goal will be to remove barriers to AI innovation and to enable high-impact applications of AI within specific sectors.[69] Indeed, the healthcare sector was represented at the Summit, and examples were given of machine learning being used in cancer detection and health analytics for improving outcomes for veterans.[70] Since then, former President Trump issued an Executive Order on Maintaining American Leadership in Artificial Intelligence.[71] This led to the American AI Initiative which, among other things, aims to set AI governance standards.[72] In 2020, draft guidance was produced by the White House on regulating AI applications, underpinned by several principles that are not necessary to examine for our purposes.[73] Finally, in 2021, the FDA issued an "Action Plan" outlining the next steps for the oversight of AI/machine learning-based software as a medical device ("SaMD").[74] The plan is premised on developing regulations for software that evolves over time, establishing good practices

---

68.   WHITE HOUSE OFF. OF SCI. & TECH. POL'Y, SUMMARY OF THE 2018 WHITE HOUSE SUMMIT ON ARTIFICIAL INTELLIGENCE FOR AMERICAN INDUSTRY (May 10, 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf?latest.

69.   *Id.* at 2.

70.   *Id.* at 10.

71.   Exec. Order No. 13,859, 84 Fed. Reg. 2967 (Feb. 11, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/; *see also* Gerke et al., *supra* note 65, at 297.

72.   *See* Exec. Order No. 13,859, *supra* note 71; *see also* Gerke et al., *supra* note 65, at 297.

73.   *See* Memorandum from Russell T. Vought, Acting Dir., to the Heads of Exec. Dep'ts & Agencies on Guidance for Regul. of A.I. Applications (2020), https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf; Gerke et al., *supra* note 65, at 297. Although no policy has been announced at the time of writing, the emphasis on developing AI will likely continue under the Biden Administration. *See* Karen Hao, *The Biden Administration's AI Plans: What we Might Expect*, MICH. INSTIT. OF TECH. TECH. REV. (Jan. 22, 2021), https://www.technologyreview.com/2021/01/22/1016652/biden-administration-ai-plans-what-to-expect/.

74.   Press Release, Fed. Dep't of Ag., FDA Releases Artificial Intelligence/Machine Learning Action Plan (Jan. 12, 2021), https://www.fda.gov/news-events/press-announcements/fda-releases-artificial-intelligencemachine-learning-action-plan.

to evaluate and improve algorithms, fostering a patient-centered approach, and advancing real-world performance monitoring pilots.

As the constituent facets of the Action Plan come to fruition, we will be better able to decipher their impacts on the use of AI for remote care. As it stands, the existing arrangements underscore the somewhat open approach towards AI technologies in the United States. It has been argued that the U.S. legal system is more facilitative towards companies than the European Union for bringing devices to the market. For this reason, companies in Europe have sought to take their products to the U.S. market instead of the United Kingdom and Europe where there have been significant technological developments.[75] As such, in terms of addressing access to healthcare "now" the United States appears best placed to take advantage owing to rapid technological developments alongside a permissive regulatory system. At the same time, the lack of regulatory guidance can also be a limiting factor because device creators will be unclear about the permissible limits of their technology in the healthcare setting and, therefore, their exposure to liability.[76]

Medical devices must gain FDA approval. Timo Minssen and his co-authors have examined that pathway in detail, so we need only briefly mention it here.[77] The Federal Food, Drug, and Cosmetic Act ("FD&C") is the relevant law in this area. Many apps are not regulated by the FDA because the software does not meet the definition of a "medical device."[78] While certain software functions may technically fall within the regulations, the FDA has noted that it will not enforce the requirements of the FD&C Act owing to the low risk posed by a device.[79] In practice, the FDA will only implement regulatory

---

75. *See* MARCO DE MORPURGO, DIGITAL THERAPEUTICS 8 (Sept. 18, 2020), https://www.dlapiper.com/en/us/insights/publications/2020/09/digital-therapeutics/.

76. *Id.*

77. *See* Timo Minssen et al., *Regulatory Responses to Medical Machine Learning*, J.L. & BIOSCIS. (Apr. 11, 2020), https://doi.org/10.1093/jlb/lsaa002; *see also* Stan Benjamens et al., *The State of Artificial Intelligence-Based FDA-Approved Medical Devices and Algorithms: An Online Database*, 118 NATURE PARTNER J. DIGIT. MED. 1 (Sept. 11, 2020), https://www.nature.com/articles/s41746-020-00324-0.

78. *See* Food, Drug, and Cosmetic Act of 1938, 21 U.S.C. § 201(h).

79. *See* U.S. FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 2 (2019), https://www.fda.gov/media/80958/download (issued following an amendment to section 520 of the Food,

oversight over medical devices "whose functionality could pose a risk to a patient's safety if the device were to not function as intended."[80] Thus, clinical grade devices will be the target of regulations rather than general wellness apps.

There are certain risk profile classifications for each medical device (Class I, II, and III devices (from low to high risk)). The classification system is not a perfect fit for medical devices using AI, and reforms are being proposed.[81] Those proposals are for a different article to consider. However, it is worth noting that the FDA has sought to offer new pathways to approval through its De Novo process. The De Novo pathway enables the FDA to evaluate novel devices anew for low or moderate risk devices. [82] After submitting a De Novo request, the FDA is required to make a classification determination for the device within 120 days.[83] The device will be granted Class I or Class II classification where the requisite criteria for classification are satisfied.[84] Once granted, the device may be immediately marketed, and a classification regulation for that device type is created.[85] The new device may also serve as a predicate device moving forward.[86] Medical devices used for remote care will need to go through this process, and it would be unsurprising if regulations are simplified in the future. For our purposes here, we shall pivot our boat away from these FDA reeds and

---

Drug, and Cosmetic Act by § 3060(a) of the 21st Century Cures Act, "removing [some] software functions from the definition of [a medical] device.").

80. *See id.*

81. *See* Gerke et al., *supra* note 65, at 5.

82. U.S. FOOD & DRUG ADMIN., DE NOVO CLASSIFICATION PROCESS (EVALUATION OF AUTOMATIC CLASS III DESIGNATION) GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (2017), https://www.fda.gov/media/72674/download; *see also* Press Release, U.S. Food & Drug Admin., FDA News Release: FDA Permits Marketing of First Game-Based Digital Therapeutic to Improve Attention Function in Children with ADHD (June 15, 2020), https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-first-game-based-digital-therapeutic-improve-attention-function-children-adhd.

83. *See* 21 U.S.C. § 513(f)(2)(A)(iii); *see also* U.S. FOOD & DRUG ADMIN., DE NOVO CLASSIFICATION PROCESS, *supra* note 82, at 5.

84. *See* 21 U.S.C. § 513(a)(1)(A), (B); *see also* U.S. FOOD & DRUG ADMIN., DE NOVO CLASSIFICATION PROCESS, *supra* note 82, at 5.

85. *See* U.S. FOOD & DRUG ADMIN., DE NOVO CLASSIFICATION PROCESS, *supra* note 82, at 5.

86. *See id.* at 12.

move towards legal questions regarding the permissible limits of technologies post-approval.

To unpack the question of regulatory permissibility of such approved devices, Gerke, Minssen, and Cohen's framework is helpful to follow. That framework focuses on the relevant legal and ethical matters. [87] The former concerns safety and effectiveness, liability, data protection and privacy, cybersecurity, and intellectual property. The ethical considerations involve informed consent, safety and transparency, algorithmic fairness, bias, and data privacy.[88] This Article does not visit every issue but rather samples the core issues that might accelerate or limit the propagation of AI for remote care. Particularly, this Article highlights the issues of data protection and privacy, informed consent, and medical liability. Doctors, health institutions, and developers should think of these issues as criteria to consider when seeking to use AI enabled medical devices to broaden remote care.

A. Data Protection & Privacy in the United States

The health devices analyzed point to the evolving nature of health data.[89] Traditional notions of what constitutes health data such as medical records, diagnostic images, or test results are being expanded to include big data arising from medical research, environmental research, socioeconomic analyses, and data from fitness apps and wearable devices.[90] A device may collect patient data and transmit it to their doctor, researchers, insurers, and the company who owns the device (for information such as usage statistics and more).[91] Such data is crucial and, indeed, beneficial to the patient's care. However, there are also risks, such as deeply sensitive data being misplaced, data being susceptible to reidentification, and risks that consent for the use of that

---

87.   *See* Gerke et al., *supra* note 65, at 296.

88*.   See id.* at 295.

89.   *See* Effy Vayena & Alessandro Blasimme, *Biomedical Big Data: New Models of Control Over Access, Use and Governance*, 14 J. BIOETHICAL INQUIRY 501, 505 (2017).

90.   *See* Effy Vayena et al., *Evolving Health Data Ecosystem*, WORLD HEALTH ORG. (2016), https://www.who.int/ehealth/resources/ecosystem.pdf?ua=1 (this broad collation of data is referred to as the "digital phenotype" by some); *see also* Sachin H. Jain et al., *The Digital Phenotype*, 33 NATURE BIOLOGY 462, 469 (2015).

91.   *See* Veyrat, *supra* note 75, at 14.

data not being obtained properly.[92] In this regard, the Health Insurance Portability and Accountability Act ("HIPAA") seeks to protect individuals from the unauthorized disclosure of their health data.[93] The law was amended by the Health Information Technology for Economic and Clinical Health Act 2009 ("HITECH").[94] Within HIPAA is the Privacy Rule, which creates protections for patients and their health information.[95] Those protections include limits and conditions regarding what information can be disclosed without a patient's authorization, and the right of patients to obtain, examine, and seek corrections for their health information.[96]

Glenn Cohen and Michelle Mello have analyzed the adequacy of HIPAA and the amendments brought about by HITECH in protecting health data in light of rapidly advancing technology.[97] They argue that HIPAA has proved "surprisingly functional" following the amendments.[98] It has ensured "reasonable information flows" of patient health information while giving patients confidence in sharing their health data with their doctors.[99] At the same time, there are significant limitations. HIPAA misses much of the health data ecosystem such as data recorded by life insurance companies, user-generated information arising from health devices used by individuals, and non-health information on which inferences about health are based.[100]

---

92.   This is opposed to obtaining electronic informed consent for the care given using AI, as discussed above.

93.   I. Glenn Cohen & Michelle M. Mello, *HIPAA and Protecting Health Information in the 21st Century*, 320 J. OF AM. MED. ASS'N 231, 231 (2018).

94.   For a useful overview of the changes to HIPAA by HITECH, see *What is the HITECH Act?*, HIPAA J., https://www.hipaajournal.com/what-is-the-hitech-act/#:~:text=HITECH%20changed%20the%20HIPAA%20right,health%20data%20 with%20other%20organizations (last visited May 26, 2021).

95.   *See* 45 C.F.R. §§ 160, 164 (2021); *see also The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Dec. 10, 2020), https://www.hhs.gov/hipaa/for-professionals/privacy/in-
dex.html#:~:text=The%20HIPAA%20Privacy%20Rule%20establishes,certain%20h ealth%20care%20transactions%20electronically.

96.   *See* 45 C.F.R. §§ 160, 164 (2021).

97.   *See* Cohen & Mello, *supra* note 93, at 231.

98.   *See id.*

99.   *See id.*

100.   *See* W. Nicholson Price II & I. Glenn Cohen, *Privacy in the Age of Big Medical Data*, 25 NATURE MED. 37, 41 (2019); *see also* Alex Pearlman, *HIPAA Is the*

Not only is the scope of the law limited, but there are three additional challenges concerning how data is handled. First, the usual structures of medical research are changing. While universities and health systems may have rigorous oversight (through Institutional Review Boards) of research, more private entities are now using data in research that has less rigorous, or non-existent, oversight.[101] Second, data that is determined to be "individually identifiable health information" is protected under the HIPAA Privacy Rule.[102] Under section 164.514 of HIPAA, methods are provided for in the law for ensuring that such data is not identifiable such as names, some address information, medical record number, and several others. Such deidentified data will no longer be subject to HIPAA, but it will also have less value for research as a consequence.[103]

Third, at the same time, it is wrong to assume that data can always be deidentified. A common argument is that data can simply be deidentified or anonymized so that the information cannot be linked to a specific individual if the data is misplaced.[104] In reality, that argument is somewhat tenuous. It has been noted that several data points, such as a patient's geolocation from their smartphone, dates and times of clinic visits, purchase data online, and more points can be combined to identify an individual.[105] Indeed, the National Committee on Vital Health Statistics ("NCVHS") has noted how the challenges of deidentifying data are far more complex today than they were when HIPAA was enacted: "Even data properly de-identified under the Privacy Rule may carry with it some private information, and, therefore, poses some

---

Tip of the Iceberg When It Comes to Data Privacy and Your Medical Data, BILL OF HEALTH (Jan. 7, 2019), https://blog.petrieflom.law.harvard.edu/2019/01/07/hipaa-is-the-tip-of-the-iceberg-when-it-comes-to-privacy-and-your-medical-data/.

101.   *See* Cohen & Mello, *supra* note 93, at 231.

102.   *See* 45 C.F.R. § 160.203 (2021); *see also* 45 C.F.R. § 160.103 (2021) (defining "individually identifiable health information.").

103.   *See* 45 C.F.R. § 164.514 (2021); *see also* Letter from William W. Stead, Chair, Nat'l Comm. on Vital & Health Stats., to Hon. Thomas E. Price, Sec'y, Dep't of Health & Hum. Servs. (Feb. 23, 2017), https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf.

104.   *See* Veyrat, *supra* note 75, at 15.

105.   *See* I. Glenn Cohen & Michelle M. Mello, *Big Data, Big Tech, and Protecting Patient Privacy*, 322 J. OF AM. MED. ASS'N 1141, 1143 (2019).

risk of re-identification, a risk that grows into the future as new datasets are released and as datasets are combined."[106]

In this regard, the requirement to deidentify data under HIPAA could pose the most significant hurdle to the utilization of technologies premised on broadening access to care today. For example, if a company pools user data from a medical device to use in research designed to enhance its product, then it may be limited by the Privacy Rule under HIPAA. Health devices depend on broad user data for their useful propagation, and the Privacy Rule could make the collection of such broad data difficult. Nevertheless, that hurdle is not insurmountable.

Returning to the limitations briefly noted above, HIPAA targets specific entities rather than specific types of data.[107] In practice, non-health data can be accessed from a variety of sources which can lead to inferences about an individual. Examples noted include phone numbers, incomes, presence of children, education, credit card, geography, age, gender, marital status, occupation, and whether an individual is a homeowner.[108] A company may not violate the law where an algorithm processes non-health data about a person's purchase of food items and over-the-counter health products to predict that individual's likelihood of diabetes.[109] This is possible due to the convoluted way in which entities are covered by the law.

The NCVHS provides several illustrative examples of this by highlighting how some entities are covered by separate regulations.[110] A child's information provided to a school by their parent is protected by a Privacy Rule under the Federal Educational Rights and Privacy Act ("FERPA").[111] A pharmacy filing a prescription, giving informal advice, and other information is protected information. Pediatricians are covered entities, and an employer may also be subject to restrictions

---

106.   *See* Letter from William W. Stead, *supra* note 103, at 2; *see also* Cohen & Mello, *supra* note 93, at 231.

107.   *See* Cohen & Mello, *supra* note 93, at 232.

108.   *See* Robert Gellman, Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges 27 (2017), https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf.

109.   *See id.* at 49.

110.   *See id* at 9–12.

111.   *See* 20 U.S.C. § 1232(g).

on sharing the health information of an employee.[112] Beyond such entities, matters become more complex. Where an individual purchases over-the-counter medicine at a supermarket, a protected health information record is not created.[113] If the individual is using a reward club card associated with the supermarket, an identifiable data record is created.[114] That record can (and is often) sold to third parties such as marketing companies.[115] Drug manufacturers can even acquire that data which contains details about the name of the individual, their insurance coverage for the purchase of the drug, where and when they purchased the drug, and what they purchased.[116] That data is not covered by HIPAA despite it being health information.[117]

These considerations extend to social media. Information shared on Facebook or Twitter could be re-shared by "friends" of the person disseminating it. The social media company can also use that information when creating the individual's profile and developing targeted advertising.[118] A private medical information website could collect user data about searches where a person creates a profile. Even where a profile is not created, the individual could be identified using their IP address, cookies on their browser, or other trackers. Such a website is not covered by privacy laws, nor are other types of internet tracking companies and search engines.[119] The "tremendous" growth of such "non-health" data that can be used to derive inferences about a person's health has led some to argue that the notion of health data should be broadened to include "past and future health data and indirect, inferred, and invisible health data."[120]

Therefore, despite HIPAA, the data environment suggests that companies are able to take advantage of a broad range of data. The law is sufficiently porous for technologies to be developed and for them to

---

112.   *See* GELLMAN, *supra* note 108, at 9–10.

113.   *See id.* at 10.

114.   *See id.*

115.   *See id.*

116.   *See id.*

117.   *See id.* at 11.

118.   *See id.* at 9.

119.   *See id.* at 11.

120.   Christophe Schneble et al., *All Our Data Will Be Health Data One Day: The Need for Universal Data Protection and Comprehensive Consent*, 22 J. MED. INT. RSCH. 124, 124 (2020).

obtain data that might help in improving their efficacy. Nevertheless, while reidentification of data seems possible through advances not covered by HIPAA, companies ought to exercise caution in embedding such practices because calls for the penalization of data misuse are increasing.[121] With this in mind, I would like to switch gears to consider the European Union, because developments there may point towards a potential regulatory path for the United States in the future.

1. Data Protection & Privacy: Could the United States Follow the European Union?

Entities could have already been subject to more onerous data protection provisions under the California Consumer Privacy Act ("CCPA"), but exceptions have ultimately been carved out for HIPAA.[122] Despite that, it is worth positing what might happen should medical devices be subject to more robust oversight. The CCPA was influenced by the General Data Protection Regulation ("GDPR") in the European Union, and it is worth considering what would happen if the United States ultimately opted to replicate those provisions generally––such a replication could align with Cohen and Mello's call for a separate regime for data.[123] In the European Union, the GDPR creates special categories of data which includes health data and other types of data which may lead to inferences about a person's health.[124] Health data "means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[125] This is a broad category that includes the following:

> Information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for

---

121.   *See* Cohen & Mello, *supra* note 93, at 232.

122.   *See* Meghan C. O'Connor et al., *With CCPA in Effect, What Do Health and Life Sciences Entities Need to Know? And How Does the New Amendment Affect You?*, LEXOLOGY   (Jan.   28,   2020),   https://www.lexology.com/library/detail.aspx?g=931a3a85-bf4d-470b-838a-e1b8c181f7ca.

123.   *See* Cohen and Mello, *supra* note 93, at 232.

124.   General Data Protection Regulation, 2016 O.J. (L 119) (EU).

125.   *Id.*

> example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.[126]

Beyond specific health data, the GDPR also covers personal data which can be used to infer information about a person's health.[127] That data includes genetic data, racial and ethnic origin, sex life, and others.[128] The Information Commissioner's Office ("ICO") in the United Kingdom explains that such health data categories extend to data from medical devices or data from fitness trackers.[129]

It is worth considering how such data protection standards might be applied in practice. Eric Wierda and his co-authors highlight three areas that raise important considerations for the application of the GDPR to health technologies.[130] First, whether data processing actually falls within the scope of the GDPR.[131] Second, the legal identity of an entity as being either a data processor or a data controller. Third, the use of cloud services and their legal status.[132]

The first matter on the scope of the GDPR elucidates anonymization considerations regarding user data arising from health technologies which can be used for commercial or research purposes.[133] Anonymous data is "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[134] Even where data has undergone pseudonymization, it will not

---

126.   General Data Protection Regulation, 2016 O.J. (L 119) (EU).

127.   *See What Is Special Category Data?*, INFO. COMM'R OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd1 (last visited May 26, 2021).

128.   General Data Protection Regulation, 2016 O.J. (L 119) (EU).

129.   *See What Is Special Category Data?*, *supra* note 127.

130.   *See* Eric Wierda et al., *Protecting Patient Privacy in Digital Health Technology: The Dutch m-Health Infrastructure of Hartwacht as a Learning Case*, 6 BMJ INNOV. 170, 174–75 (2020).

131.   *See id.*

132.   *See id.*

133.   *See id.* at 174.

134.   *See* General Data Protection Regulation, 2016 O.J. (L 119) (EU).

be permissible to use that data for broader purposes where it can be "attributed to a natural person" through the use of additional information.[135] The GDPR, therefore, contemplates the concerns regarding the limitations of deidentification. To account for those risks, the GDPR requires that account is taken of all the means reasonably likely to be used by any entity to identify the person.[136] It states that:

> To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.[137]

Thus, where data is rendered anonymous such that the data subject is not or no longer identifiable, the GDPR will not apply.[138] And his co-authors note that while the GDPR creates a high bar, it can be challenging to delineate between anonymous and identifiable data in practice.[139] They argue that entities should act cautiously and determine that information is personal identifiable data where there is any doubt.[140]

Second, it is critical to design technology that distinguishes between the obligations of the data controller and data processor because the GDPR has separate expectations for both.[141] The healthcare provider will typically be the data controlling entity, while the data processor will be the company delivering the medical device.[142] The data controller has primary responsibility for determining the purpose and extent of the data processing.[143] The data processor has narrower obligations as set out in a contract such as those concerning the security of the data.[144] This includes taking responsibility for the obligation under

---

135.   *See id.*
136.   *See id.*
137.   *See id.*
138.   *See id.*
139.   *See* Wierda, *supra* note 130.
140.   *See id.*
141.   *See id.* at 175.
142.   *See id.*
143.   *See id.*
144.   *See id.*

the GDPR concerning data processing which requires that "appropriate technical and organizational measures" are implemented to "ensure a level of security appropriate to the risk."[145] Matters become more complicated where a data processor uses data in broader ways. In such circumstances, the data processor may also become an additional data controller, which raises the level of responsibility under the GDPR.

It is helpful to consider how such responsibilities may arise where a health device is used to provide remote access to care. One study analyzes the compliance with the GDPR of an mHealth device used to monitor patients in the Netherlands with heart disease.[146] The hardware device connected to software (on mobile apps, tablets, or personal computers). Data collected through the device was transmitted to a cardiology center through partner servers before being integrated into electronic patient health records.[147] A healthcare professional would then interpret that data and contact the patient if necessary.[148] This example is useful because it operates in a similar manner to other health devices being used to provide remote care.

In this example, eight critical stages were followed to ensure compliance with data protection rules. First, "onboarding of the patient" requires that informed consent is obtained from the patient for the processing of their health data in the mHealth program.[149] Second, "data collection" requires validated and certified data collectors and the disclosure of data that is stored and processed.[150] Third, "data transmission" requires a data processing agreement between the data controller and the data processor about the activities and duties of the data processor (this includes requirements regarding encryption).[151] Fourth, "data storage on external servers" emphasizes that data is stored within the protected European Union regulatory environment (this includes data minimization standards).[152] Fifth, "sharing of personal data" requires that personal data is only shared for the purposes stated in the data processing agreement (unless the data is aggregated and no longer

---

145.   General Data Protection Regulation, 2016 O.J. (L 119) 1, 51 (EU).

146.   *See* Wierda, *supra* note 130, at 171.

147.   *See id.*

148.   *Id.*

149.   *Id.* at 172.

150.   *Id.* at 172–73.

151.   *Id.* at 173.

152.   *Id.* at 174.

considered personal data in light of the GDPR).[153] Sixth, "sharing of aggregated data" emphasizes that data can only be used for research purposes where it is not considered "personal data."[154] Seventh, "data storage by healthcare provider" requires that hospital information systems adhere to security standards, that a Data Privacy Impact Assessment is performed, and that any breaches are promptly notified.[155] Eighth, "data interpretation by healthcare provider" requires that data collection is limited only to the parameters relevant for delivering care specific to the patient (privacy by design and default).[156]

On the third matter raised by Wierda and his co-authors, data controllers and processors may use cloud services to send and retrieve data quickly and efficiently. In such circumstances, the company providing the cloud service will be considered a "data processor" for the purposes of the GDPR.[157] They note that there are increased risks surrounding confidentiality and data privacy with the use of cloud services in countries with strict national security and anti-terrorism legislation such as the United States.[158] As such, they recommend that only cloud services based in the European Union be used.[159]

At present, the United States and European Union take different approaches to data protection. Rather than possessing an overarching data protection law that is relevant specifically to health data, the U.S. regulatory landscape generally comprises sector-specific data protection laws.[160] The European Union has a more overarching approach through the GDPR. By highlighting both approaches, we can see the factors pertaining to data that must be considered in the U.S. landscape. This section uses the GDPR as an example because that regulatory approach could plausibly indicate the future in the United States. The United States would not necessarily replicate the GDPR, but some elements might be transposed (in one form or another) into U.S. law. Any elements that are transposed may create greater hurdles for the dissemination of the health technologies described in this Aricle. To ensure

---

153.   *Id.*
154.   *Id.*
155.   *Id.*
156.   *Id.*
157.   *Id.* at 175.
158.   *Id.*
159.   *Id.*
160.   *See* Vayena & Blasimme, *supra* note 90, at 507.

the best possible chance of using technologies for remote care not only now (by following the U.S. legal architecture), but also in the future, it would be wise for developers to consider the GDPR architecture as a checklist or guidelines for best practices in this area.

2.   A Note on Consent & Data

In this discussion on the use of data, we must briefly consider the issue of consent. This is a different issue to obtaining electronic informed consent for care given using AI, which is covered below. As discussed by Effy Vayena, the right to notice and consent concerning a person's access to their data is protected under HIPAA.[161] One approach has been to require general consent of the patient as well as secondary consent that determines whether a patient is happy with their data being used in subsequent medical research.[162] Another crucial matter concerns the transmission of patient data to insurers who require such information to reimburse the use of a device. The question is whether patients can consent to such data being transmitted if it were needed for insurers to determine adherence and efficacy of the device. It may be the case that opt-out models of consent will become prevalent, whereby patients are deemed to consent to the use of their data obtained through digital therapeutics unless they revoke it.[163]

A sensible solution to these dilemmas has been proposed by the European Data Protection Supervisor ("DPS") which issued an opinion stating that app developers, app stores, device manufacturers, and advertisers are subject to the same data protection rules despite their incongruent business models.[164] The DPS recommended that a single policy be created to ensure the accountability of designers, manufacturers, and others involved in the design, supply, and functioning of apps.[165] This policy would require mobile health devices be created with transparency in mind so that users would be clear about what data

---

161.   *See id.*

162.   *See* Veyrat, *supra* note 75, at 16.

163.   *See id*.

164.   *See* GIOVANNI BUTTARELLI, EUR. DATA PROT. SUPERVISOR, MOBILE HEALTH: RECONCILING TECHNOLOGICAL INNOVATION WITH DATA PROTECTION 2 (May   21,   2015),   https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf.

165.   *See id.*

was being collected and that such data was only being collected to perform the "expected function" of the device.[166] The DPS also recommended that data should only be used in mobile health to benefit individuals and should not be used where the consequences would be harmful or discriminatory.[167]

Following the publication of the Opinion, a draft Privacy Code of Conduct on mobile health apps was created.[168] The draft Code is premised on the principles of obtaining user consent for the use of their data, using data for specific and legitimate purposes, ensuring privacy by design, ensuring certain data rights for users, that data is retained only for as long as is necessary, implementing security measures, rules on advertising, third-party disclosure protections, protections for data transferred outside the European Union, protocols for data breaches, and restrictive approaches to gathering data about children.[169]

These principles may illuminate a more specific regulatory model in the future, but they are yet to be implemented. Indeed, following the assessment of the draft Code, the Data Protection Working Party noted that the code was not drafted in line with the GDPR and would have to be revised.[170] Nevertheless, these principles illuminate best practices. Developers can roll out AI to provide remote care today, but those efforts should also be future proofed, ready to anticipate potential regulatory developments.

B.   Informed Consent

We must consider the issue of consent not just in terms of obtaining data, but also in terms of AI's use of data to deliver care. Indeed, there are ethical, legal, and technical considerations regarding obtaining informed consent for the use of remote care solutions employing AI. For legal and ethical considerations, Cohen has produced

---

166.   *See id.*

167.   *See id.*

168.   *See Privacy Code of Conduct on Mobile Health Apps*, EUR. COMM'N (Oct. 29, 2020), https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

169.   *See id.*

170.   Letter from Audrea Jelinek, Chairperson, Art. 29 Working Party, to Hans Graux, Timelex Att'y 1–3 (Apr. 11, 2018), https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=52056.

a wonderfully detailed article on the law of informed consent involving AI in the United States.[171] Key questions include whether a doctor relying on an AI recommendation for their patient's care has legally secured informed consent.[172] Further, whether a doctor who decides to overrule the AI recommendation and fails to tell their patient that they have done so, has failed the patient's legal and ethical right to informed consent.[173] Ethical questions consider whether doctors must inform patients that they are using AI, the extent to which doctors must educate patients about AI systems providing a recommendation for their care, including the types of data used, biases in the data, and so on.[174]

Cohen argues that the preponderance of jurisprudence in the United States leads to the conclusion that doctors will generally not be liable for failing to inform patients about the use of AI to provide recommendations for their care.[175] In the United States, there are generally two standards of informed consent—the physician standard and the patient standard.[176] The former standard entails what a reasonable physician ought to disclose to a patient.[177] The latter standard requires that information is disclosed which is material to the patient's decision (such as information regarding the diagnosis and treatment).[178] The scope of these informed consent standards, however, is limited in the AI context. Cohen notes that some U.S. states only require consent for surgical or other invasive procedures.[179] There are possible areas where informed consent may raise important considerations for health technologies. For example, it might be arguable that there ought to be disclosure where a physician relies on AI to make a decision, enabling them to perform at the level of a specialist.[180] Additionally, jurisprudence demonstrates that there will be liability where a person other than

---

171.   *See* Cohen, *supra* note 7, at 1426.
172.   *See id.*
173.   *See id.* at 1425.
174.   *See* Gerke et al., *supra* note 65, at 301.
175.   *See* Cohen, *supra* note 7, at 1429.
176.   *See id.* at 1432.
177.   *See id.* at 1433.
178.   *See id.* at 1433–34.
179.   *See id.* at 1434.
180.   *See id.* at 1435–36.

the agreed physician performs a critical part of a surgical procedure.[181] A similar analogy may be drawn with the use of AI. A surgeon may perform a specific surgical technique based on an AI recommendation, but the patient may be unaware that the AI recommendation played a role in that particular part of their treatment.[182] Therefore, liability may follow because informed consent is lacking. Despite these various "fact patterns," Cohen notes that grounding such obligations is "far from easy."[183] The extent to which these considerations might actually apply in practice is an open question. At present, they are yet to be tested or answered.

There are also technical aspects for ensuring informed consent for care which happen to utilize AI technology. In some circumstances, obtaining consent would simply replicate traditional means. A doctor giving their patient a device for their care would be able to obtain the patient's consent for that method of care directly. For remote care, two broader considerations arise which may require a deviation from the traditional approach. First, the doctor may not be able to meet with a patient physically, so informed consent will need to be obtained electronically. Second, remote health devices involve several interactions between different entities sharing a range of data. Informed consent must cover those interactions, as well as evolving recommendations of a device that may require further consent as the course of care evolves.

In this regard, electronic informed consent ("eIC") is an important method for remote AI care. eIC does not simply mean obtaining an electronic signature. The Electronic Signatures in Global and National Commerce Act was enacted more than two decades ago to allow for signatures in contracts electronically.[184] Since then, all fifty states have passed legislation on the use of such signatures.[185] The challenge with eIC is ensuring that proper disclosure is made to the patient about what they are consenting to. Consequently, while it is required that eIC replicates the same standard as hand-written signatures (such as having easily understandable language), there are

---

181.   *See* Cohen, *supra* note 7, at 1438 (referring to Perna v. Pirozzi, 457 A.2d 431 (N.J. 1983)).

182.   *See id.* at 1439.

183.   *See id.* at 1468.

184.   15 U.S.C. §§ 7001–31.

185.   John T. Wilbanks, *Electronic Informed Consent in Mobile Applications Research*, 48 J. OF L., MED., & ETHICS 147, 147 (2020).

additional recommendations that go beyond those requirements. However, those recommendations will not be applicable where FDA regulations apply. While most adopters of eIC undertake research that is regulated by the FDA or Health and Human Services, there remain many unregulated app developers who may simply state that they are not FDA regulated and will revert to standard consent and privacy policies for consumer technologies instead.[186]

As such, technologies may fall under different regulatory rubrics. Some apps will be governed by the Fair Information Practice Principles ("FIPP"), which simply require that "notice" is given for a person to consent. The terms are presented to a person on the screen, and they click that they agree.[187] A "daisy chain" of contracts involving privacy policies, terms of use, and terms of service usually arise for individuals participating in a study using mobile phones that connect to wearable devices.[188] As Wilbanks notes, these contracts complicate the informed consent process because they are dense, participants do not read them, and, in any case, they do not meaningfully protect privacy.[189] He notes that "the current state of practice seems little impacted by these efforts to improve understandability, directly countervailing the informing requirement of informed consent."[190]

Other apps will not fall under such consumer technology policies but will fall under FDA requirements instead. For those within the FDA's regulatory orbit, there is guidance concerning the appropriate processes for obtaining consent electronically in FDA regulated medical devices.[191] The FDA define eIC as: "the use of electronic systems and processes that may employ multiple electronic media, including text, graphics, audio, video, podcasts, passive and interactive Web sites, biological recognition devices, and card readers, to convey

---

186.   *See id.* at 149.

187.   *See id.*

188.   *See id.* at 150.

189.   *See id.*

190.   *See id.*

191.   Food & Drug Admin., Use of Electronic Informed Consent Questions and Answers: Guidance for Institutional Review Boards, Investigators, and Sponsors 2 (2016), https://www.fda.gov/media/116850/download.

information related to the study and to obtain and document informed consent."[192]

For there to be adequate informed consent, there must be a process utilizing the above approaches to facilitate a person's understanding of the information before them, and the opportunity for the individual to ask questions.[193] This may be an ongoing process where an individual's participation continues, requiring the individual to provide additional information.[194] In this manner, eIC has certain benefits. It may have an interactive interface which assists with comprehending and retaining information more clearly than a paper, written consent form. A patient can be rapidly notified of any amendments through an eIC and provide consent to those changes. That consent can be integrated into databases instantaneously without the need for a manual update by a human being.[195]

An eIC form may be completed in various ways, and there are a range of factors in how the eIC is completed that might affect its validity. The FDA guidance considers several relevant factors which are beyond the scope of this Article to analyze in detail. For example, how the eIC might be presented to the subject, how and where the eIC process may be conducted, how and when questions from subjects should be answered, the steps that may be taken to facilitate the subject's understanding of the information, and the steps that may be taken to convey additional information such as new findings during the course of the research, among others.[196]

The impact of the COVID-19 pandemic also highlights the FDA's greater emphasis on obtaining eIC for clinical trials of medical products.[197] For example, for hospitalized patients or those in isolation

---

192.   *Id.*

193.   *See* 45 C.F.R. § 46.116 (2021) (setting out the general requirements for informed consent, noting that there must be a concise and focused presentation of the key information in assisting an individual's decision to participate or not); *see also* 21 C.F.R. § 50.20 (2021) (requiring that an investigator cannot involve a human subject in research without obtaining their informed consent, and that consent must be obtained free of coercion and undue influence).

194.   *See* FOOD & DRUG ADMIN., *supra* note 191, at 3.

195.   *See id.*

196.   *See id.* at 4–13.

197.   FOOD & DRUG ADMIN., CONDUCT OF CLINICAL TRIALS OF MEDICAL PRODUCTS DURING THE COVID-19 PUBLIC HEALTH EMERGENCY: GUIDANCE FOR

due to the pandemic, the FDA recommended that eIC be obtained instead of written consent.[198] The FDA provided the example of the COVID My-Studies app, which is a platform that enables investigators to obtain informed consent where face-to-face meetings are not possible.[199] To use the app, the investigator may send the informed consent documents electronically to the patient who can then sign the documents which are accessible to the doctor.[200] While that guidance was issued only for the duration of the public health emergency, the door may very well have been opened to even more permissible methods of obtaining informed consent which may benefit technologies ensuring broader access to care in the future.

It should be noted that the guidance is non-binding. [201] Companies do not have to implement such consent requirements in their devices.[202] They could create AI devices that provide remote care without such necessities. Yet, the guidelines smooth the path for technologies providing remote access to care. A simple and efficient eIC mechanism ultimately allows a company to argue that they are following best practices. These observations lead to the conclusion that informed consent will not be a barrier to the proliferation of AI technologies in healthcare at present. There are no clear answers regarding the legal and ethical informed consent issues pertaining to the use of AI from the jurisprudence. The conclusion is thus that liability will likely not follow for the issues outlined at the start of this passage. For the technical aspects of informed consent, the requirements depend on which pigeon-hole developers decide to place their product. The FDA's guidance does not seem particularly onerous at a technical level and following it would arguably be best practice.

INDUSTRY, INVESTIGATORS, AND INSTITUTIONAL REVIEW BOARDS (2020), https://www.fda.gov/media/136238/download.

198.   *See id.* at 15.

199.   *See id.*

200.   *See COVID MyStudies Application (App)*, U.S. FOOD & DRUG ADMIN. (May 29, 2020), https://www.fda.gov/drugs/science-and-research-drugs/covid-mystudies-application-app.

201.   *See* FOOD & DRUG ADMIN., *supra* note 192, at 1.

202.   *See id.*

C. *Medical Liability*

The final matter to focus on is the potential liability that may flow from the use of AI. The technology is available and growing, but does the law create an impediment to providing remote care by creating undue burdens surrounding liability? There are all sorts of scenarios one could envisage. Who is liable if a wearable device does not correctly detect an illness, or if a doctor relies on a recommendation that is incorrect, or if a virtual assistant gives advice which harms the patient? Can these scenarios impede the rollout of AI devices for use in remote care?

Medical malpractice falls under negligence in tort law. A medical professional generally owes a duty of care to their patient, and they will be deemed to be in breach of that duty of care where they fall below the required standard. The standard of care applied is that of a reasonably competent physician exercising a reasonable degree of care and skill.[203] In the context of the remote care devices we considered above, negligence claims might arise where the doctor either improperly uses the technology or fails to use it. In those circumstances, it may be found that they have not used practices and procedures that are in accordance with those followed by the average competent physician in the same field.[204] Michael Froomkin, Ian Kerr, and Joelle Pineau highlight how technology can cause the standard of care to change quickly.[205] Other breakthrough technologies, such as automated external defibrillators and x-rays, very quickly became the standard diagnostic after their introduction and doctors were held to be so clearly negligent where they did not use them.[206] Ultimately, there have been criticisms that technologies have been "anointed" too quickly with little proof that they are helping patients.[207]

---

203.   For a good overview of the law, see A. Michael Froomkin et al., *When AIs Outperform Doctors: Confronting the Challenges of a Tort-Induced Over-Reliance on Machine Learning*, 61 ARIZ. L. REV. 33, 51 (2019). *See also* W. Nicholson Price II, *Medical Malpractice and Black-Box Medicine*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS (I. Glenn Cohen, Holly Fernandez Lynch, Effy Vayena, & Urs Gasser eds., 2018).

204.   *See id.* at 53.

205.   *See id.* at 58.

206.   *See id.* at 56–57.

207.   *See id.* at 57.

At present, there is no case law concerning negligence and the use of AI.[208] Nevertheless, Nicholson Price, Sara Gerke, and Glenn Cohen have mapped eight different liability scenarios and how the current law might deal with them.[209] Liability can only arise if some harm is ultimately caused. Thus, we can discard scenarios where a decision by a physician relying on AI technology falls below the standard of care, if that decision does not result in harm. We can therefore eliminate four scenarios mapped out by the authors where no injury arises, meaning there can be no liability.

The remaining scenarios emphasize the importance of following or deviating from the standard of care. Consider an AI recommendation which follows the expected standard of care. For example, AI accurately recommends a specific dosage of medicine. Where the doctor rejects that recommendation (and harm results), he or she will be liable.[210] This is unsurprising because the doctor has fallen below the expected standard of care irrespective of whether the AI system was involved or not (the AI system has not recommended anything particularly novel in this scenario). If the doctor had followed the recommendation, then he or she would be acting in accordance with the standard of care. Where AI provides a recommendation that follows the standard of care, but which turns out to harm the patient, the doctor will not be liable for following the recommendation because it nevertheless accords with the standard of care.[211]

Now consider AI making a nonstandard care recommendation. If a doctor rejects a nonstandard care recommendation of AI, and the patient is harmed, then the doctor will not be liable because they did not deviate from the standard of care.[212] In other words, even though the AI recommendation was right, that recommendation did not fall within the standard of care at that time. The patient cannot sue because the AI recommended a novel approach that is not encapsulated by current standards. On balance, this appears to be fair because a doctor cannot be held to some unknown and novel recommendation.

---

208.   *See* W. Nicholson Price II et al., *Potential Liability for Physicians Using Artificial Intelligence*, 322 J. OF AM. MED ASS'N 1765, 1765 (2019).

209.   *See id.* at 1765–66.

210.   *See id.*

211.   *See id.*

212.   *See id.* at 1766.

Having said all that, over time, the standard of care is likely to shift as it has done before. Froomkin and his co-authors argue that once AI is demonstrably superior to clinicians, the law will require that AI recommendations be the standard of care.[213] We might enter a future in which the standard of care is determined by algorithms. Before that happens, Price and his co-authors suggest that doctors relying on a novel AI recommendation may be able to use that reliance as a defense where harm results to the patient.[214] For now, they conclude the following:

> [The] analysis suggests an important implication for physicians using medical AI to aid their clinical decisions: because current law shields physicians from liability as long as they follow the standard of care, the "safest" way to use medical AI from a liability perspective is as a confirmatory tool to support existing decision-making processes rather than as a source of ways to improve care.[215]

Consequently, of the medical devices encompassing AI described in this article, it is best that they are used as a tool by doctors for monitoring and confirming disease. The onus will remain on medical professionals to not solely rely on the AI system for providing remote care. To analogize, an on-board parking camera in a car always warns users not to solely rely on the camera when parking, the driver should still physically look around them to identify dangers (such as a child running from the side) that the camera would not see. The same is true with remote care devices. They are an incredibly helpful tool for providing remote care, but they should not be used in isolation.

V. CONCLUSION

The overarching picture is of a rather sporadic, incoherent, and loophole-filled legal landscape. Yes, there are specific FDA requirements that must be adhered to for devices to go to market, but once there, the impediments to their rollout are not onerous. In many instances, both legislation and case law are simply lacking for their

---

213.　*See* Froomkin et al., *supra* note 203, at 61–62.
214.　*See* Price II et al., *supra* note 208, at 1766.
215*.*　*See id.* at 1765.

application to new AI-based technologies. There is an opportunity to expand within the market more easily while this environment persists. As such, enhancing remote care and thus, the accessibility of care overall, through the use of AI-technologies is possible. These technologies are growing and have demonstrable benefits for patients. Wearables, telemedicine consultations using AI, virtual assistants, and other AI devices can extend the hand of healthcare to those who need it. They can assist in lowering costs, lower waiting times, assist doctors in diagnosing illness, and lead to overall efficiency gains.

However, the use of these devices is only just sprouting. It is inevitable that the regulatory schism will not persist for long. By the time it is remedied, remote care solutions might become more of a mainstream option for care. Therefore, this Article attempts to emphasize a focus on best practices to future-proof the use of new remote AI-technologies sprouting today for the mature environment of tomorrow. While there are other issues to consider, this short Article focuses on the areas of data privacy and protection, informed consent, and medical liability. In some cases, such as the European Union's GDPR, we can imagine where future regulations might go. Indeed, the CCPA was inspired by the GDPR. In other cases, there are currently guidelines and non-binding recommendations. Finally, as we saw with Wierdah medical liability, one must deduce the potential regulatory developments that might appear down the line. By applying additional best practices in the currently scant legal environment, more robust mechanisms can be employed for remote care that will improve the odds of longevity for those devices while ultimately benefitting patients.

***