Welcome to the next installment of Arnold & Porter's Virtual and Digital Health Digest. This edition primarily covers March 2023 highlights across the virtual and digital health space. This digest focuses on key virtual and digital health and telehealth-related developments in the United States, United Kingdom, and European Union in the healthcare, policy, regulatory, and privacy spaces.

In this issue, you will find the following:

US News

EU and UK News

US News

FDA REGULATORY UPDATES

FDA Issues Draft Guidance on Marketing Submission Recommendations for a Predetermined Change Control Plan (PCCP) for AI/ML-enabled Device Software Functions. On April 3, 2023, FDA issued draft guidance titled "Marketing Submission Recommendations for a Predetermined Change Control Plan for AI/ML-enabled Device Software Functions" (PCCP Draft Guidance). The guidance, which applies to devices that are or include machine learning-enabled device software functions (ML-DSF), proposes what FDA describes as a least burdensome approach to support iterative improvement through modifications to such devices while continuing to provide a reasonable assurance of device safety and effectiveness. As further detailed in a 2019 discussion paper and 2021 work plan, one element of FDA's proposed approach to regulation of AI/ML-enabled devices is inclusion of predetermined change control plans (PCCPs) in premarket submissions. Although there are a few examples of AI/ML devices that FDA has cleared with PCCPs, the agency when issuing the work plan indicated that it may need additional statutory authorities to fully implement its proposed approach to AI/ML devices. The new PCCP Draft Guidance aligns with recent legislative changes providing FDA statutory authority relating to authorizing devices with PCCPs. As further detailed in the January 2023 issue of our Digital & Virtual Health Digest, as part of the recently enacted Food and Drug Omnibus Reform Act (FDORA), Congress gave FDA authority to approve a PCCP submitted in a premarket approval application (PMA) or 510(k) premarket notification (510K), provided the device remains safe and effective without the change and, in the case of a 510(k) device, remains substantially equivalent to the predicate. FDORA also expressly provides that a PMA supplement or new 510(k) premarket notification shall not be required for a change to an approved or cleared device if the change is consistent with an approved or cleared predetermined change control plan.

The newly issued PCCP Draft Guidance provides recommendations on the information to include in such a PCCP in a marketing submission for a ML-DSF. For purposes of the guidance, the term "PCCP" refers to a plan that includes device modifications that would otherwise require a premarket approval supplement, *de novo* submission, or a new premarket notification. As proposed in the draft guidance, a PCCP describes the anticipated ML-DSF modifications and the associated methodology to implement those modifications, which would be reviewed in the marketing submission to ensure continued safety and effectiveness of the device without necessitating additional marketing submissions for each modification described in the PCCP. The draft guidance outlines the components of a PCCP, including a detailed description of modifications, a modification protocol, and an impact

assessment. Notably, the draft guidance explains that modifications to an authorized PCCP will generally constitute changes to the ML-DSF that require a new marketing submission for the device, which will include the modified PCCP. FDA encourages manufacturers to leverage the Q-Submission process for obtaining FDA feedback on a proposed PCCP prior to submitting a marketing submission.

Comments on the PCCP Draft Guidance are due by July 3, 2023.

FDA Issues Guidance on Timeline for Implementation of FDORA Medical Device Cybersecurity Information Submission Requirements. On March 30, 2023, FDA issued guidance entitled "Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act" (Cybersecurity RTA Guidance). This guidance relates to the new cybersecurity requirements established by FDORA, as codified in new section 524B of the Federal Food, Drug, and Cosmetic Act (FDCA). Section 524B requires the inclusion of cybersecurity information in premarket applications for "cyber devices" and makes failure to comply with the new cybersecurity requirements a prohibited act under the FDCA. The term "cyber device" is defined to mean a device that (1) includes software validated, installed, or authorized by the sponsor as a device or in a device; (2) has the ability to connect to the internet; and (3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats. In summary, under section 524B, sponsors of cyber devices must provide a plan to monitor, identify, and address any post-market cybersecurity vulnerabilities; establish and maintain procedures to ensure the device and related systems are cybersecure; provide a software bill of materials; and fulfill any other requirements FDA may develop to ensure the device and related systems are cybersecure. FDA may exempt certain devices or categories of devices from these cybersecurity requirements.

Although FDORA had an effective date of March 29, 2023, the Cybersecurity RTA Guidance explains that for premarket submissions for cyber devices submitted *before* October 1, 2023, FDA generally does not intend to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B. Rather, FDA "intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process." For cyber device premarket submissions submitted beginning October 1, 2023, however, FDA may refuse to accept the submission if the cybersecurity information required under section 524B is not included. FDA expects that by October 1, sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain the information required by section 524B.

Additional information about other FDA reforms included in FDORA can be found in the Arnold & Porter FDORA Advisory.

FDA Releases Framework for the Use of Digital Health Technologies (DHTs) In Drug and Biological Product Development. On March 23, 2023, FDA released a document outlining its "Framework for the Use of DHTs in Drug and Biological Product Development" (DHT Framework), meant to guide the use of DHT-derived data in regulatory decision-making for drugs. FDA developed the DHT Framework to advance a Prescription Drug User Fee Act VII (PDUFA VII) commitment. The DHT Framework defines DHTs as "systems that use computing platforms, connectivity, software, and/or sensors for health care and related uses." DHTs include technologies intended for use as a medical product, in a medical product, or as an adjunct to other medical products (devices, drugs, and biologics), and may also be used to develop or study medical products. As noted in the DHT Framework, there is a large spectrum of DHTs available for potential use to support drug development and review, some of which meet the definition of a device under the FDCA and others that do not. DHTs, as described in the DHT Framework, often consist of sensor hardware

that allows for continuous or intermittent recording of physiological and/or behavioral data (e.g., blood pressure, physical activity, glucose levels) and can also be software applications that are run on general-purpose computing platforms (e.g., mobile phone, tablet, or smart watch). DHTs may, for example, be used to administer electronic clinical outcome assessments, including electronic patient reported outcome and electronic performance outcome instruments.

The DHT Framework outlines a multifaceted approach to collaboratively address potential challenges with DHTs. Elements of the DHT Framework include: (1) creating a steering committee to ensure consistent policy across FDA regarding the use of DHT-derived data in regulatory decision-making for drugs; (2) holding public meetings or workshops with key stakeholders to gather input into issues related to the use of DHTs in regulatory decision-making; (3) identifying demonstration projects to inform methodologies for efficient DHT evaluation; (4) issuing guidance documents on the use of DHTs in drug clinical trials; (5) publishing guidance on regulatory considerations for prescription drug use-related software; (6) enhancing consistency across FDA centers with regards to the development, use, and review of DHTs and associated endpoints; and (7) enhancing IP capabilities to support the review of DHT-generated data.

FDA Issues Updated Draft Guidance on Electronic Systems, Records, and Signatures in Clinical Investigations. On March 16, 2023, FDA issued an updated draft guidance entitled "Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations" (Part 11 Draft Guidance). The Part 11 Draft Guidance provides information for sponsors, clinical investigators, IRBs, clinical research organizations, and others on the use of electronic systems, records, and signatures in clinical investigations of foods, medical products, tobacco products, and new animal drugs. As described by FDA, the goals of the draft guidance are to: (1) update recommendations for applying and implementing data integrity and data security controls, including the use of audit trails and the protection of records in the current environment of electronic systems used in clinical investigations; (2) provide additional recommendations on the risk-based approach to validation of electronic systems described in the August 2003 Part 11 guidance; and (3) facilitate the use of electronic systems, electronic records, and electronic signatures to improve the quality and efficiency of clinical investigations. The new draft guidance focuses on recommendations regarding the Part 11 requirements under which FDA considers electronic systems, records, and signatures to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

As it relates to digital health technologies specifically, the new Part 11 Draft Guidance includes recommendations on the use of DHTs to remotely acquire data in clinical investigations. The recommendations include how to identify

the data originator when using DHTs to capture data from participants, how data attribution should be ensured, considerations for the initial transfer of data from a DHT to a durable electronic data repository, and DHT-collected data FDA intends to inspect during an inspection. The new Part 11 Draft Guidance revises the 2017 draft guidance entitled "Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 — Questions and Answers" and, when finalized, will supersede the 2007 guidance entitled "Computerized Systems Used in Clinical Investigations."

Comments on the Part 11 Draft Guidance are due by May 15, 2023.

HEALTHCARE FRAUD AND ABUSE UPDATES

Continued Crackdown on Genetic Testing.

The crackdown on medically unnecessary testing by DOJ and U.S. attorneys continues. On March 13, 2023, Dr. Kathy Cornelius, a Delaware physician, agreed to pay $500,000 following allegations that she violated the False Claims Act (FCA) by ordering medically unnecessary genetic testing for more than 250 Medicare beneficiaries for over a year and a half. Dr. Cornelius allegedly based these referrals for tests that cost thousands of dollars per patient from brief telemedicine consultations that produced no legitimate medical justification for the tests. Medicare coverage rules require that tests be ordered by a provider who will use the results of the testing in the treatment of the patient. DOJ alleged that Dr. Cornelius did not have a medical relationship with the patients outside of these tests.

In another case of allegedly fraudulent testing, on March 28, 2023, a Utah resident pleaded guilty in a healthcare fraud and kickback scheme involving genetic cancer tests (CGX Tests). Jordan Bunnell and other co-conspirators operated, owned, and had a financial interest in a marketing call center, a clinical laboratory, and telemedicine company that either conducted or arranged for a variety of medical tests. DOJ alleged that between October 2018 and July 2019, Bunnell and others paid kickbacks and bribes to numerous parties in exchange for referrals and orders for CGX Tests for Medicare beneficiaries and those of other healthcare benefit programs. DOJ alleged that Bunnell and his co-conspirators caused US$89 million in losses to Medicare and other federal and private health care benefit programs.

Fraudulent orders of genetic testing tend to raise red flags given their significant costs to federal healthcare programs. Further, these cases reflect HHS's continued focus on fraud and abuse in ordering medically unnecessary testing through telemedicine platforms highlighted in the July 20, 2022 Special Fraud Alert and emphasized in DOJ's FCA FY 2022 year in review discussed in the March Digest.

Former Florida Resident Charged in US$101 Million Healthcare Kickback Scheme. On March 23, 2023, a former Florida resident was charged for his role in a durable medical equipment kickback scheme. Raheel Naviwala and his co-conspirators operated and owned multiple call centers that they used to acquire doctors' orders for durable medical equipment (DME), including orthotic braces, for Medicare beneficiaries that were not medically necessary. These DME orders were obtained through a network of marketing call centers and telemedicine companies and were provided in exchange for kickbacks from certain companies that provided the braces to Medicare beneficiaries. In total, Naviwala and his co-conspirators allegedly caused US$101 million in losses to Medicare.

Florida Man Sentenced to Nine Years in Federal Prison for His Role in International Health Care Fraud Scheme. On March 30, 2023, an individual was sentenced on conspiracy and kickback charges for his role in selling fraudulent doctors' orders to co-conspirators who used these orders to submit more than US$48 million in fraudulent Medicare payments. Nagaindra Srivastav owned B2B Apps Solutions (B2B) that Srivastav and his co-conspirators used to establish and operate an internet-based platform used by individuals and businesses in the healthcare industry to purchase and sell physician orders for DME. Srivastav allegedly purchased the medically unnecessary doctor's orders he sold to his customers from telemedicine companies based in the Philippines and Pakistan and was notified on several instances that the purported authorizing physician had not actually spoken with the patient, signed the order, or prescribed the DME. Further, Srivastav created RepsHub, a website where DME companies and others could upload potential DME-patient information called "leads," that were generally obtained through telemarketing campaigns targeting beneficiaries for whom DME products could be billed. Srivastav offered and sold leads that he obtained through the call centers controlled by himself and his co-conspirators. Srivastav was sentenced to nine years in prison, followed by three years of supervised release, and was ordered to pay US$48 million in restitution.

CORPORATE TRANSACTION UPDATES

Collapse of Silicon Valley Bank Signals End of Golden Era for Digital Health Venture Capital Funding. The Silicon Valley Bank's (SVB) collapse on March 10, 2023 marked the end of digital health venture funding's peak. Venture funding for the digital health market boomed from 2020-2022, with the pandemic acting as a catalyst for digital health and telehealth innovations. While other banks turned away from digital health and telehealth startups because of their perceived risk, SVB was often the bank of choice for these digital health startups. For example, 44% of U.S. venture-backed technology and healthcare companies that went public in 2022 were SVB's clients, and 76% of all venture capital-backed public health offerings since 2020 used SVB. As of December 2022, SVB said it had US$78.8 billion in healthcare deposits and investments. Last November, SVB provided Oak Street Health with a US$300 million credit facility and DispatchHealth, an at-home healthcare company founded in 2013, with a US$330 million round of venture capital funding.

The FDIC takeover of SVB raises questions about how the failure will impact both more established digital health companies as well as startups seeking capital. It is likely that the fall of SVB will cause digital health startups and more established digital health companies to flock to larger, more traditional banks or seek other sources of funding, albeit at higher rates, given the perceived risk of funding startups. It is also possible that some digital health innovations that would have received funding in a more permissive environment will not easily find a replacement investor, thus stifling digital health innovations and creating a digital health setback in the coming years.

Transcarent to Acquire Majority of AI-healthcare Company 98point6 for US$100 Million. While many digital health companies are recalibrating after the recent banking failures, Transcarent and 98point6 have made headlines with a strategic acquisition. Transcarent, a consumer-directed digital healthcare platform for employees of self-insured employers, announced last month it will acquire the majority of on-demand healthcare startup 98point6 for US$100 million. The acquisition includes 98point6's nearly 100-member clinician-physician group, self-insured employer business, and software license to its artificial intelligence-enabled chatbot. In the release announcing the deal, Transcarent CEO Glen Tullman praised the acquisition: "By combining the 98point6 AI-powered virtual care technology and an affiliated group of world class physicians with Transcarent's comprehensive care platform, we will deliver consumers and employers what they really want and need."

While Transcarent already offers 24/7 access within 60 seconds to doctors through its app, Transcarent relies on third-party contractors to offer this care. The acquisition of 98point6 will allow Transcarent to forgo such use of third-party contractors and instead offer 24/7 care in-house at a near-instantaneous rate. Notably, the acquisition includes 98point6's artificial intelligence-enabled chatbot that collects patient information and summarizes it for a physician, who can then continue the conversation and provide proper treatment. The acquisition will expand Transcarent's platform to "a full spectrum of virtual and in-person care, providing a more personalized Member health and care experience that integrates across solutions."

The acquisition closed on March 31, 2023. 98point6 will use its remaining assets after the acquisition to rebrand as 98point6 Technologies, shifting its focus on licensing its software to third-party providers and becoming a "pure play technology company."

Best Buy Health Will Set Up Virtual Hospital Care Through Deal With Atrium Health. Best Buy's Geek Squad is setting up virtual hospital rooms in homes. Best Buy Health announced on March 6 that it struck a three-year deal with Atrium Health, the nation's largest hospital at-home provider, to set up technology in patients' homes that remotely monitors their vitals. Atrium Health launched its at-home healthcare program in 2020 as a response to COVID-19, and the partnership with Best Buy Health seeks to enhance the already established program. The partnership leverages Atrium Health's strength as a leader in telemedicine while also tapping into Best Buy Health's unique ability to set up technology seamlessly through its Geek Squad, which has been entering consumers' homes and setting up complicated technology for decades.

With this new partnership, Geek Squad will set up and install in patient's homes technology that tracks patients' heart rates, blood oxygen levels, and other vital signs. Geek Squad shares the data with doctors and nurses through a telemedicine hub. In addition to post-operative care, Atrium Health's hospital at-home program provides care for conditions, such as heart failure, COPD,

pneumonia, asthma, and various infections, using wearable technology, telehealth visits, and home visits. Geek Squad members specially trained in health began setting up the virtual-care systems in February. While the two companies have not yet disclosed the deal's financial terms, it has been announced that Atrium will buy devices from Best Buy, use the Geek Squad for installation, and patients will pay Atrium through their insurance.

This is not Best Buy's first venture into the digital health sphere. Over the past five years, Best Buy acquired three different healthcare companies specializing in telehealth, remote patient monitoring, and emergency services. While Best Buy has indicated it will not venture into the direct provision of healthcare, its focus on the health sector continues to grow with partnerships and acquisitions of digital and telehealth companies.

PRIVACY UPDATES

White House Unveils National Cybersecurity Strategy. On March 2, 2023, the White House announced a national cybersecurity strategy designed to make the U.S. digital ecosystem more resilient and "values-aligned." The full strategy guide describes how companies and organizations that control personal consumer data should be held accountable when they fail to act as "responsible stewards" for the data they possess. Notably, the strategy guide provides that the Biden Administration endorse legislative efforts to impose federal limits on the ability to collect, use, transfer, and maintain personal data and provide protections for sensitive data, including health information and geolocation. President Biden summarized his commitment on this issue during the State of the Union address, calling for robust privacy protections and transparency regarding the collection, use, and sharing of personal data.

President Biden Releases Budget Proposal for Fiscal Year (FY) 2024. On March 9, 2023, President Joe Biden released his proposed FY 2024 budget, which amounts to US$6.9 trillion for the upcoming fiscal year, including US$688 billion in non-defense discretionary spending and US$886 billion in defense spending. The budget proposal includes an 11% increase in the Department of Health and Human Services (HHS) budget as described in the FY 2024 HHS Budget Brief, including a proposed increase of US$88 million above 2023 enacted levels for cybersecurity initiatives in the Office of the Chief Information Officer, for a total of US$188 million for FY 2024. The budget includes US$20 million to increase HHS' cybersecurity workforce to improve the Office of Inspector General's (OIG) cybersecurity efforts and support an "artificial intelligence-ready" workforce. The budget notes that both HHS and the U.S. healthcare industry face significant cybersecurity risks that HHS OIG oversight and other federal enforcement agencies plan to help mitigate in the future. While the president's budget request officially kicks off the FY 2024 appropriations cycle and is the starting point for the annual budget and appropriations process, the president's budget is often viewed as more of a messaging statement than a budgetary blueprint. With Republicans in control of the House, much of President Biden's proposals are unlikely to be enacted as presented, as many ultra conservatives are calling for significant cuts to federal spending across the board. House Republicans are planning to counter with a budget proposal of their own. In an interview on March 30, Speaker McCarthy shared that the House Republican Conference is close to releasing legislation outlining the GOP's spending priorities.

Congressional Cybersecurity and Privacy-Related Activity. In January, Sen. Mark Warner (D-VA) told reporters he plans to introduce legislation in 2023 to help strengthen healthcare organizations' cybersecurity defenses. Sen. Warner, who is co-founder of the Senate Cybersecurity Caucus, issued a report in November that urged Congress to consider federal legislation related to cybersecurity in the healthcare sector, including by assigning a "senior leader" at HHS to lead an office on cybersecurity. This year, we also expect House

Energy & Commerce Chair Cathy McMorris Rodgers (R-WA) and Ranking Member Frank Pallone (D-NJ) to reintroduce an updated version of the American Data Privacy and Protection Act (H.R. 8152), a broad privacy bill which would set new federal privacy standards for companies, non-profits, and other entities. While the bill would not apply to health data already covered by the Health Insurance Portability and Accountability Act (HIPAA), it would cover health data held by non-HIPAA-covered entities, such as tech companies acting in the digital health space who are not providing services to those covered entities. HIPAA-covered entities would still be required to comply with the act when it comes to protecting other types of data. On March 1, the Innovation, Data, and Commerce Subcommittee of the House Committee on Energy and Commerce held a hearing on the bill.

On March 2, Sens. Amy Klobuchar (D-MN), Elizabeth Warren (D-MA), and Mazie Hirono (D-HI) introduced the UPHOLD Privacy Act of 2023 (S. 631), which would prevent companies from profiting off of patients' data for advertising purposes by banning the use of personally identifiable health data for commercial advertising and prohibiting the sale of precise location data to and by data brokers. House Republicans also outlined some of their cyber-related policy priorities last year through the Healthy Future Task Force (Task Force), a 17-member panel led by Reps. Brett Guthrie (R-KY) and Vern Buchanan (R-FL). The Task Force's modernization subcommittee expressed additional support for improving patient data-sharing standards that prioritize privacy and security and promote the interoperability of electronic health records. However, the narrow House GOP majority may face hurdles due to the potential costs of such proposals, particularly until the larger debt ceiling debate is resolved, making the possibility of passing comprehensive legislation difficult to enact even where there may be policy agreement with the Democrat-controlled Senate and the Biden Administration.

EU and UK News

REGULATORY UPDATES

Transition Periods for the EU MDR Finalized. Regulation (EU) 2023/607, which extends the transitional provisions applicable under the EU Medical Devices Regulation (MDR) for certain medical devices, entered into force on March 20, 2023. The Regulation provides that certificates issued by Notified Bodies from May 25, 2017 under the old regime, valid on May 26, 2021, and not withdrawn since, shall remain valid after the period indicated on the certificate until the following dates and provided certain conditions are met:

- December 31, 2027: Class III and Class IIb implantable (with exceptions)
- December 31, 2028: Class IIb (with exceptions), Class IIa, and Class I sterile or measuring
- December 31, 2028: devices that did not require Notified Body involvement to obtain a CE certificate under the old regime, for which the declaration of conformity was drawn up prior to May 26, 2021, and do require Notified Body involvement under the MDR

Certificates that expired before March 23, 2023 shall be considered valid until the above dates if certain conditions are met. In addition, the Regulation removes the "sell-off" deadline, which previously enabled devices already placed on the EU market to remain in the supply chain and be made available in the EU without having to be taken off the market. Read our blog and the February Digest for more details.

Increased Funding for Medical Technologies in the UK. On March 3, 2023, the UK government's Department of Health and Social Care (DHSC) announced awards of nearly £16 million to nine artificial intelligence (AI) technologies that detect cancers, diagnose rare diseases, and identify at-risk patients more quickly. The funding will be used to accelerate the testing, evaluation, and use of the technologies in the NHS. In the Spring Budget 2023 and announced on March 15, 2023, the Medicines and Healthcare products Regulatory Agency (MHRA) will also receive £10 million from the UK government to speed up the approval process and ultimately provide access to innovative medicines and medical technologies in the UK.

UK Proposals on Medical Devices Regulatory Reform. On March 7, 2023, an advisory group on behalf of the UK government's Life Sciences Council published proposals to accelerate access to innovative technologies. The proposals are based on three priority areas:

- International recognition — the group proposes that a recognition route for approvals of medical devices be developed to include other trusted jurisdictions, such as the U.S., and explore greater flexibility over requirements for markings and labels on devices.
- Routes for innovation — it is proposed that pre-market regulatory advice be expanded and performance metrics for uptake of HealthTech Innovation be developed.
- System capacity — delivery of a HealthTech Regulatory skills program and a specialist network of innovation centers are suggested.

While not specific or focused on virtual and digital health technologies, such products will also be able to benefit from these reforms if accepted and adopted by the UK government.

Update on the UK's Pro-innovation Regulation of Technologies Review. On March 8, 2023, the UK government's Chief Scientific Adviser (CSA) wrote a letter to the Chancellor of the Exchequer with interim recommendations regarding the mutual recognition of technologies approved internationally.

The CSA is currently undertaking a "Pro-innovation Regulation of Technologies Review: life sciences" due to be completed by early May 2023, but wanted to highlight the recommendations prior to the Spring Budget 2023 announcement (see above). The CSA recommended that the MHRA and the National Institute for Health and Care Excellence (NICE) adopt a broader approach to mutual recognition, particularly for well-established technologies, and that this should be paired with a rigorous surveillance process. The CSA also suggested that a new risk-based recognition route to market should be introduced for MedTech and In-Vitro Diagnostics. Part of the funding announced for the MHRA in the Spring Budget 2023 will also be used to establish the international recognition framework. Regulators in the U.S. and Japan are expected to be the MHRA's first regulatory partners in this respect.

Recommendations regarding better data-sharing between regulators and the use of AI applications are expected in the May report.

Launch of UK Artificial Intelligence and Digital Regulations Service. On March 7, 2023, the UK's Health Research Authority (HRA) announced the launch of the Artificial Intelligence and Digital Regulations Service website. Previously, this service was not open to the public. This service is aimed at innovators and users, offering information and advice on regulations governing the development and adoption of AI and digital technologies in health and social care in England. Guidance for developers is split into regulations for medical devices, non-medical devices, and a data compliance checklist.

Guidance From the MHRA on Software as a Medical Device. On March 22, 2023, the MHRA published guidance on how to draft an intended purpose statement for Software as a Medical Device (SaMD) to assist manufacturers in meeting their statutory obligations. Intended purpose is defined as "the use for which the device is intended according to the data supplied by the manufacturer on the labelling, in the instructions and/or in promotional materials." This guidance supplements the MHRA's guidance on "Medical device stand-alone software including apps," which provides criteria for software meeting the definition of a medical device under the UK legislation. While this guidance is UK-focused, it is also helpful in assisting with interpretation of the EU provisions, as the definitions are similar.

The new guidance presents four key elements of an intended purpose: (1) structure and function of the device; (2) intended populations; (3) intended user; and (4) intended use environment. These elements should be set out in sufficient detail to reflect the state-of-the-art and wider literature. The guidance covers common issues with the intended purpose for SaMD that have been

identified by MHRA based on previous examples, such as vague intended uses, and provides example cases to demonstrate such issues. The guidance provides a flow chart to help manufacturers define their intended purpose for SaMD. The guidance advises that the process is followed both at an early stage, but also at key phases during development and post-marketing to ensure the criteria are still met. It also emphasizes that a clear intended purpose will aid manufacturers in their agreements and partnerships with healthcare providers and engagement with NICE.

UK ABHI Report on Using Digital Health Technologies to Help the NHS. In March 2023, the UK Association of British HealthTech Industries (ABHI), the industry body for medical technology in the UK, published a report on how digital health technologies can address key challenges faced by the NHS. ABHI recommends that the MHRA be provided with resources to support and process SaMDs, NHS data be made accessible in a safe and secure manner to innovators, an assessment program for digital health solutions be designed, and specific funding pathways for digital technologies be developed. The report includes case studies demonstrating the benefits of health technologies and identifies barriers to accessing health technologies.

Publication of UK CSA Report on Digital Health Technologies. On March 15, 2023, the CSA published a report on digital technologies. The CSA makes various recommendations with respect to AI, including creating a regulatory sandbox as a safe live testing environment for applications and publishing a clear policy on relationships between intellectual property law and generative AI. The sandbox is intended to allow innovators to experiment with new products or services with enhanced regulatory supervision and without risk of fines or liability. The recommendations mirror the UK government's approach to regulating AI, as discussed in our blog post, whereby regulatory authorities have discretion over how the principles apply in their respective sectors. In its response, the government accepted both recommendations.

Publication of UK Government's White Paper on AI. On March 29, 2023, the UK government launched a white paper on AI, outlining its approach to regulating AI across the economy and its intention to build public trust and encourage safe innovation. Recognizing the speed with which AI is developing, the government states it will take an adaptable approach to regulating AI and will empower existing sector regulators to develop tailored approaches to regulation. This was one of the options assessed in the report on the framework options for AI governance from the Department for Science, Innovation and Technology and the Office for Artificial Intelligence.

The white paper states that regulators should consider five key principles: (1) safety, security, and robustness; (2) transparency and explainability; (3) fairness; (4) accountability and governance; and (5) contestability and redress. Regulators will issue practical guidance, tools, and resources over the next 12 months to set out how to implement these principles.

The government will help regulators develop consistent guidance in conjunction with the Digital Regulation Cooperation Forum (DRCF). DRCF's role will involve facilitating cross-regulator engagement on the principles, horizon scanning, and establishing the cross-sectoral sandbox. The white paper notes the MHRA's approach to AI as a medical device, as discussed in our blog, stating that the MHRA will develop guidance on the transparency and interpretability of AI as a medical device, as well as how to meet product safety requirements.

Stakeholders may provide feedback on the white paper until June 21, 2023. We are preparing a more detailed update on these proposals and will share it in a later digest.

PRIVACY UPDATES

Support for the EHDS from MedTech Europe. On March 2, 2023, MedTech Europe announced its support for the proposed European Health Data Space (commonly referred to as the EHDS), which it believes will help harness the benefits for health data sharing. MedTech Europe recommends that the framework be consistent and coherent with existing and upcoming EU regimes to avoid administrative burden, have clearly defined key terms, build upon the existing trade secret and IP rights framework, clarify the competencies of newly established Health Data Access Bodies, and involve stakeholder input. MedTech Europe's position paper provides more detail.

Updated Guidance on AI From the UK ICO. On March 15, 2023, in response to industry feedback, the UK's Information Commissioner's Office (ICO) updated its guidance on AI and data protection. The updates include: a new chapter on ensuring compliance with transparency obligations in AI; a new section on what details should be covered by a Data Protection Impact Assessment when using AI to process data; new content on using AI to make inferences, affinity groups, and special category data; and a discussion of how fairness applies to AI. Annex A considers fairness throughout the AI life cycle and how fundamental aspects of designing AI may impact fairness.

DHSC Publishes UK's Cyber Security Strategy. On March 22, 2023, the UK's DHSC published its strategy to achieve cyber resilience and further protect sensitive information across the health and social care sector by 2030. The approach consists of identifying the most critical areas of the sector where disruption would cause the greatest harm to patients, uniting the sector to pool resources and enable faster responses, train the workforce, ensure security is implemented into emerging technologies, and support organizations in response and recovery. An implementation plan setting out planned activity for the next two to three years is expected in the summer of 2023.

REIMBURSEMENT UPDATES

Report on Digital Transformation in Healthcare. In March 2023, the European Institute of Innovation and Technology Health Think Tank published a report on the impact of digital transformation in healthcare across Europe. Key stakeholders discussed the German fast-track assessment and reimbursement model for digital medical devices (DiGA), which was introduced in 2019. While DiGA has facilitated access to evidence-based digital healthcare, implementation has been slower than expected with only 15 digital health applications obtaining a permanent listing in the last three years. Challenges for manufacturers have been the competent authority's, Bundesinstitut für Arzneimittel und Medizinprodukte's (known as BfArM), strict study design and evidence standards and the associated investment to meet these, as well as defining and proving the positive healthcare effect. There has also been a slow uptake by medical professionals with only low numbers of prescriptions registered; this has been attributed to insufficient communication and engagement about availability and benefits.

DiGA has inspired similar models in other EU countries, as reported in our previous Digest, but this is leading to disparities in access to digital health apps across the EU and, therefore, there is a call for harmonization across the EU. The report concludes by setting out several recommendations for governments, regulatory bodies, policymakers, and healthcare stakeholders to improve access to citizens and convergence between EU member states.

PRODUCT LIABILITY UPDATES

Position Paper From the European Consumer Organisation on the proposed Product Liability Directive. On March 1, 2023, the European Consumer Organisation (BEUC) published a position paper on the European Commission's proposal to revise the Product Liability Directive (PLD). While supporting many elements of the proposal (for example, bringing software within the scope of the PLD), the BEUC put forward several possible improvements. One such improvement was that the definition of product should explicitly state that software, including AI, is covered as a component of a product, as a standalone product, and as a service. Currently, the proposal only contains this language in the recital. There will also be a need to ensure that the inclusion of AI does not conflict with the draft AI Liability Directive, as discussed in our previous Digest.

Questions/Comments?

Contact a member of our Editorial Committee

Allison Shuren
Partner
Washington, DC

Chris Anderson
Partner
Chicago

Abeba Habtemariam
Partner
Washington, DC

Jackie Mulryne
Partner
London

Nancy L. Perkins
Counsel
Washington, DC

Monique Nolan
Counsel
Washington, DC

Amanda Cassidy
Sr. Health Policy Advisor
Washington, DC

Eugenia Pierson
Sr. Health Policy Advisor
Washington, DC

Mickayla Stogsdill
Sr. Health Policy Advisor
Washington, DC

Emma Elliston
Associate
London

Rachel Mower
Associate
Chicago

Alison Peters
Associate
Washington, DC