Welcome to the third installment of Arnold & Porter's Virtual and Digital Health Digest. This edition primarily covers December 2022 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, regulatory, privacy, and corporate transactions space.

In this issue, you will find the following:

EU and UK News

US News

FDA REGULATORY UPDATES

Digital Health Provisions Included in Consolidated Appropriations Act.
As part of the Consolidated Appropriations Act of 2023, signed into law on December 29, 2022, Congress included a package of FDA "riders"—deemed the Food and Drug Omnibus Reform Act (FDORA). While there are numerous medical device provisions in FDORA, particularly relevant to the digital health space are ones relating to cybersecurity requirements and predetermined change control plans for devices that employ artificial intelligence (AI) or machine learning (ML).

- **Cybersecurity:** Section 3305 of FDORA 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, 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.
- **Predetermined Change Control Plans:** 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 pre-determined change control plans in premarket submissions. Although there are examples of AI/ML devices that FDA has cleared with predetermined change control plans, the agency has indicated that it may need additional statutory authorities to fully implement its proposed approach to AI/ML devices. To that end, Section 3308 of FDORA expressly permits FDA to approve a predetermined change control plan submitted in a premarket approval application (PMA) or 510(k) premarket notification, 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. Section 3308 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. Notably, for 510(k) devices, the provision appears to prohibit the use of changed versions of a device

implemented in accordance with a predetermined change control plan as a predicate device, specifying that only the version of the device originally cleared or approved prior to any predetermined change control plan changes can be used as a predicate device. As further detailed in the November issue of our digest, FDA has indicated that draft guidance on predetermined change control plans will be issued in 2023.

For more information about other FDA reforms included in FDORA, please see our FDORA Advisory.

FDA Issues Report on Risks and Benefits of Non-Device Software Functions. In December 2022, acting on a requirement of the 21st Century Cures Act (Cures Act), FDA issued a publication entitled "Report on Risks and Benefits to Health of Non-Device Software Functions." Enacted in December 2016, the Cures Act amended the FDCA statutory definition of a "device" to exclude certain software functions, including, for example, certain general wellness, administrative, and clinical decision support functions. The Cures Act requires FDA to publish a report every two years that examines the risks and benefits to health associated with such exempt software functions. This report is the third such report issued by FDA since enactment of the Cures Act.

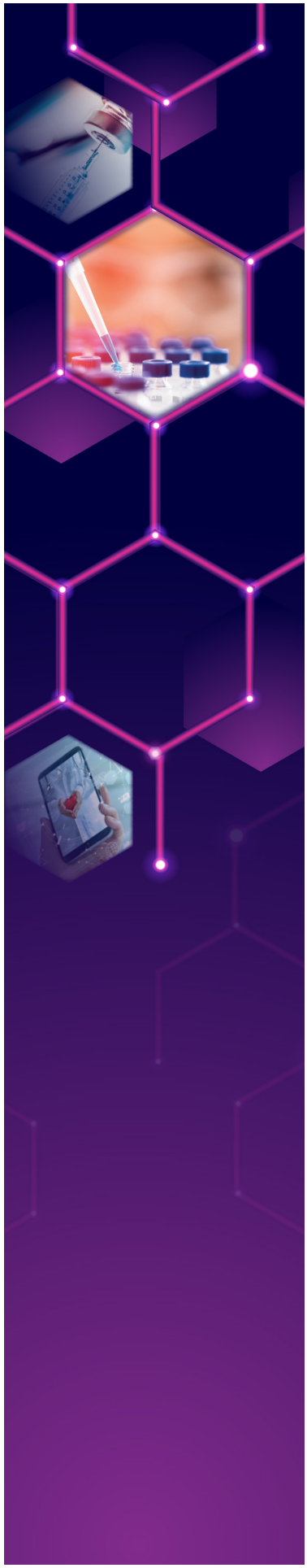
As further detailed in the report, in general, FDA's analysis found more benefits than risks to patient safety and health related to the Cures Act software functions. While the report "identifies only a few reported negative impacts on patients safety and health," FDA acknowledges that adverse events may be underrepresented in the report given that there is no requirement to report adverse events from a non-device software. Select examples of changes and updates from the last version of the report (2020) include: (i) discussion of the positive impact of e-prescribing software on health care costs, (ii) new evidence on the impact of certain CDS software on medication use, unnecessary treatments, and adherence to treatment guidelines, (iii) new information on adverse events related to laboratory workflows, (iv) information on the impact of mobile phone apps and wearables on mental health, smoking cessation, and disease education, and (v) information on adverse events and issues with EHR data entry and systems security.

FDA Updates Digital Health Policy Navigator. On December 14, 2022, FDA updated the Digital Health Policy Navigator (Policy Navigator). First released in September 2022 in conjunction with updates to various FDA digital health guidances, the Policy Navigator provides an interactive overview of the FDA digital health policies that might apply to a proposed software function. The Policy Navigator includes seven steps, with the answers to each question guiding users through the most relevant FDA medical device regulatory considerations. FDA updated the Policy Navigator in response to feedback from stakeholders. Updates include improvement in access to the tool through the webpage and the addition of examples to the clinical decision support software policy considerations in Step 6.

FDA Finalizes Several Digital Health-Related Device Classifications. In recent weeks, FDA has finalized several software-related device classifications for product types that were reviewed through the agencies *de novo* classification process. The *de novo* process can be used by sponsors to request that FDA classify novel devices that lack a predicate device, including novel digital health devices, into Class II (moderate risk) or Class I (low risk). After issuance of a *de novo* classification order, FDA will follow up with a final order codifying the classification in regulations. The recently codified device classifications include the ones listed below. All of these devices were classified into Class II (special controls).

- Pediatric Autism Spectrum Disorder Diagnosis Aid
- Virtual Reality Behavioral Therapy Device for Pain Relief

- Gastrointestinal Lesion Software Detection System
- Hardware and Software for Optical Camera-Based Measurement of Pulse Rate, Heart Rate, Breathing Rate, and/or Respiratory Rate
- Adjunctive Hemodynamic Indicator With Decision Point
- Brain Stimulation Programming Planning Software
- Digital Therapy Device to Reduce Sleep Disturbance for Psychiatric Conditions



FDA Issues Warning Letter to Company Marketing Unapproved Software Products. In the enforcement space, FDA recently posted to its website a Warning Letter issued to a company marketing several products, including a mobile app and other software-based products, for device uses without compliance with FDA's device requirements. The Warning Letter relates to RoyalVibe Health Ltd.'s (RoyalVibe's) marketing of the CellQuicken Analyzer (Smart-Watch and Software), RoyalVibe Ultrasound Generator, Envirovibe Water Restructuring Pad, Brainvibe Neuroplasticity Visual Program, RoyalVibe Therapy Balls, and RoyalVibe Application. FDA alleges various FDCA violations, including that the products are adulterated and misbranded as they lack PMA approvals or 510(k) clearances, that RoyalVibe failed to register and list the products with FDA, and that RoyalVibe denied or limited an FDA inspection.

As is often the case with Warning Letters issued to companies marketing unapproved software products, FDA appears to have had prior communications with the company about the regulatory status concerns prior to escalation to issuance of a public Warning Letter. FDA alleges that despite RoyalVibe representing that it would cease selling the products in the US, the product websites remained active and the companion app continued to be available for download in the US. The Warning Letter instructs RoyalVibe to provide a plan for how it will handle the previously distributed adulterated products and the steps that it has taken to remove its products from the US market.

Owlet Announces Submission of De Novo Classification Request for Baby Heart Rate, Oxygen Monitor. Back in October 2021, Owlet Baby Care, Inc. (Owlet) received a Warning Letter from FDA alleging the company's Smart Sock products are devices. While an "FDA Response" section on Owlet's website explains that Owlet is "no longer selling the Smart Sock in the US," Owlet now appears to be working with FDA to obtain two marketing authorizations. Most recently, in a December 22 press release, Owlet announced that it submitted a *de novo* classification request for "an over-the-counter software-as-a-medical-device that offers heart rate and oxygen displays and notifications in conjunction with Owlet's existing Dream Sock sleep monitoring capabilities." The press release explains that the *de novo* request is Owlet's second FDA submission this year, with the company in October announcing that it submitted a 510(k) premarket notification for a prescription-only monitor designed to be used in-home for babies under the supervision of a physician.

HEALTHCARE FRAUD AND ABUSE UPDATES

Physician Charged in $9.5 Million Health Care Fraud Conspiracy. On December 14, 2022, a federal indictment was unsealed detailing charges against Dr. Benjamin T. Toh, who was charged for his role in a more than $9.5 million healthcare fraud conspiracy. Between March 2019 and September 2019, Toh submitted false and fraudulent claims to Medicare and Medicaid for cancer genetic testing in exchange for kickback payments. Specifically, Toh obtained access to Medicare and Medicaid patients through purported telemedicine companies and signed orders for cancer genetic testing (CGx) in exchange for the payment of kickbacks. The government alleged that Toh signed orders without regard to whether they were medically necessary, that he was not the treating physician of the patients, and he did not conduct an actual telemedicine visit, nor did he follow up with patients on the test results.

In a similar telemedicine fraud case, Alexandra Stchastlivtseva was charged with conspiracy to defraud the United States and to offer to pay healthcare kickbacks, five counts of offering and paying healthcare kickbacks, and conspiracy to commit money laundering. Allegedly, Stchastlivtseva offered to pay and ultimately paid kickbacks and bribes to several telemedicine companies and marketing companies in exchange for completed doctors' orders of orthotic braces and glucose monitors for Medicare beneficiaries that were medically unnecessary. Medicare paid more than $17.3 million on these fraudulent claims.

Lab Owner Convicted in $463 Million Genetic Testing Scheme to Defraud Medicare. On December 14, 2022, Minal Patel was convicted for his role in a Medicare fraud scheme for submitting medically unnecessary genetic tests. Patel, who owned LabSolutions LLC (LabSolutions), conspired with patient brokers, telemedicine companies, and call centers to fraudulently state that Medicare covered certain cancer genetic tests. After the Medicare beneficiaries agreed to take a test, Patel paid kickbacks and bribes to patient brokers to obtain signed doctors' orders authorizing the tests from telemedicine companies. To conceal the kickbacks, Patel required the patient brokers to sign agreements that stated the brokers were performing legitimate advertising services for LabSolutions. The government alleged that the telemedicine doctors approved the genetic testing even though they were not treating the beneficiaries and often did not even speak with them. From July 2016 through August 2019, LabSolutions caused more than $463 million in fraudulent and medically unnecessary claims to be submitted, leading to over $187 million being paid for fraudulent claims by Medicare. Patel personally received $21 million of these Medicare proceeds.

OIG Reports on Illinois' Compliance With Requirements for Claiming Medicaid Reimbursement for Telehealth Payments During COVID-19. On December 21, 2022, OIG published a report summarizing the audit results of the state Illinois Medicaid program telehealth payments during COVID-19. The

audit examined $584,492 Medicaid fee-for-service telehealth payments, totaling $21,052,452 ($13,980,157 federal share), that Illinois' State Agency that administers the state Medicaid program included on its federal financial participation (FFP) reports with dates of March 1, 2020 through March 1, 2021. The services were audited for compliance with federal and state telehealth coverage and payment requirements, including the relaxed distant and originating site rules, type of telecommunication system used for service, documentation of the telehealth service, and use of the appropriate HCPCS codes and modifiers. In addition, OIG conducted a qualitative review of the services billed as telehealth to determine whether the service could be delivered via a telecommunications system. OIG found that Illinois largely complied with payment requirements—only 532 payments of the total payments reviewed were not allowed. The key errors included: payment to the same provider for both a distant and originating site service, duplicate payments for the same service and incorrect use of the telehealth modifier with an in-person service, and payments for services that could not be performed via a telecommunication system. The results of this audit give suppliers and providers of telehealth services some insight into areas to direct compliance efforts and their own internal auditing programs.

PROVIDER REIMBURSEMENT UPDATES

Consolidated Appropriations Act, 2023. On December 29, 2022, President Biden signed into law the *Consolidated Appropriations Act, 2023*. The law provides $1.7 trillion to fund the federal government for one year and contains several provisions related to telehealth reimbursement. Most notably, Section 4113, titled "Advancing Telehealth Beyond COVID-19," extends certain Medicare flexibilities adopted during the public health emergency (PHE) for up to two years—until December 31, 2024—regardless of when the PHE ends. Previously, the Consolidated Appropriations Act, 2022 extended certain Medicare flexibilities up to 151 days after the end of the PHE. In addition, in its calendar year 2023 physician fee schedule final rule, the Centers for Medicare & Medicaid Services extended additional telehealth flexibilities in connection with the possible end of the PHE. (See Arnold & Porter's December edition of the Virtual and Digital Health Newsletter for a summary of those changes.)

In particular, Section 4113(a)-(f) extends several policies, including (1) allowing telehealth services to be furnished in any geographic location and any originating site; (2) expanding the list of practitioners eligible to furnish telehealth services; (3) extending coverage of telehealth services furnished by Federally Qualified Health Centers and Rural Health Clinics; (4) delaying the in-person visit requirements under Medicare for mental health services furnished through telehealth and telecommunications technology; (5) allowing the furnishing of audio-only telehealth services; and (6) allowing the use of telehealth to conduct face-to-face encounters prior to recertification of eligibility to hospice care.

In addition, Section 4113(g) requires the Secretary of the US Department of Health and Human Services to conduct a study on program integrity related to Medicare part B telehealth services using medical record review. In particular, the scope of the study must include a review and analysis of information related to the duration and type of the telehealth services furnished and, to the extent feasible, the impact on future utilization of health care services by Medicare beneficiaries, such as the utilization of additional telehealth services or in-person services, including hospitalizations and emergency department visits. Interim and final reports on this study are due to Congress no later than October 1, 2024 and April 1, 2026, respectively. To carry out these various provisions, Section 4113(g)(3) appropriates an additional $10 million to the amounts otherwise available to the agency.

PRIVACY UPDATES

Telehealth Websites Found to Be Sharing Sensitive User Data via Tracking Technologies. According to the findings of an investigation of the online practices of 50 direct-to-consumer telehealth companies by the medical reporting company STAT and the nonprofit newsroom The Markup, reported on December 13, 2022, many of these companies are using online tracking tools to collect—and in some cases to share—individually identifiable information on patients who may be unaware of the tools.

In the fall of 2022, STAT and The Markup completed registration and related forms on the websites of all 50 of the investigated telehealth companies (using fictional names and medical information together with dummy email and social media accounts). Using a Google Chrome tool (Chrome DevTools), they were able to identify what elements of the data they had provided was being shared by the telehealth companies with third parties.

As reported by The Markup, the investigation found that all but one of the investigated companies was sharing Internet Protocol (IP) addresses and webpage visit histories of site visitors with at least one "big tech" platform (such as TikTok, Meta, or Snap). Although this type of tracking is very common and the information shared is very limited, an IP address is "personal information" under almost all data privacy laws, including the privacy and security regulations implementing the Health Insurance Portability and Accountability Act (the HIPAA Privacy and Security Rules). Moreover, the investigation found that 25 of the investigated sites were using tracking tools that shared with the "big tech" platforms information on individuals' purchases of prescription medicines or subscriptions to particular plans of treatment through the sites. And on 13 of the 50 sites, the investigators found that tracking tools were used to collect and share the information site visitors provided for treatment intake purposes. For example, one site used a pixel that sent to Facebook the investigators' responses to questions about self-harm, drug, and alcohol use, together with each investigator's (fictional) first name, email address, and phone number.

The STAT-Markup findings were published just a few weeks after the Office for Civil Rights (OCR) at HHS issued its bulletin on the risks for entities regulated by the HIPAA Privacy and Security Rules of using online tracking technologies, such as Google Analytics and Meta Pixel, as discussed in our December 2022 Digital and Virtual Health Digest. For HIPAA-regulated companies, the collection of an IP address alone in association with a response to an intake screening question such as "Do you have diabetes?" or "Do you suffer from anxiety or depression?" triggers an obligation not to use or share that information, with limited exceptions, without the written authorization of the individual to whom the information pertains.

And for non-HIPAA-regulated entities, while not subject to HIPAA Privacy or Security Rule liability and associated penalties, other liability risks may loom for

using tracking technologies to collect and share personal health information. The Federal Trade Commission (FTC) has explicitly warned companies that use of tracking technologies to collect health and other sensitive personal information may constitute an unfair or deceptive practice under Section 5 of the FTC Act, if such practices are not properly disclosed and agreed to by the site users to whom the information pertains. And as highlighted in our Advisory on the enforcement action against Sephora brought by the Office of the California Attorney General, the use of online tracking tools to collect and share sensitive personal information may trigger liability under state laws such as the California Consumer Privacy Act (CCPA) as well.

After compiling their findings from the investigation, STAT and The Markup shared those findings with all of the 50 investigated companies. At least one company, Workit Health, reported that it had changed its use of trackers, and when the investigators tested Workit Health's site a second time, they found no evidence that tech platform trackers were being used to collect user data during the site's intake or checkout processes.

EU and UK News

REGULATORY UPDATES

Joint EU-US Roadmap on Managing AI. On December 1, 2022, the EU-US Trade and Technology Council published a joint roadmap on evaluation and measurement tools to manage the risks of AI and increase trust in the development, deployment, and use of AI systems. The roadmap sets out three activities aimed at aligning the EU and US risk-based approaches to AI:

1. Advancing shared terminologies and taxonomies;
2. Supporting leadership and cooperation on international technical standards and tools to measure and manage AI risks; and
3. Exchanging information on existing and emerging AI risks.

A number of short-term and long-term mechanisms are listed to meet these objectives. For example, these implementation mechanisms include establishing expert groups on each objective in the short term, and in the longer term, conducting workshops of the expert groups.

Council of the EU Publishes Its Position on the AI Act. On December 6, 2022, the Council of the EU (Council) adopted its general approach to the European Commission's (Commission) proposal for the EU's Artificial Intelligence Act (EU AI Act). The draft EU AI Act was presented by the Commission in April 2021 as a means of facilitating investment and innovation in AI, while enhancing governance and ensuring AI systems placed on the market are safe and respect fundamental rights. As part of its "compromise proposals", the Council has narrowed the definition of "AI system" to those developed through machine learning approaches and logic- and knowledge-based approaches, clarified many of the requirements for high-risk AI systems to make them more feasible and less burdensome for stakeholders, and has simplified the compliance framework. However, the medical devices that incorporate AI will have to meet both the provisions of the EU AI Act and the Medical Devices Regulation 2017/745 (MDR), which has been an area of concern noted by industry bodies (as discussed in our previous Digest). The proposal is also being discussed by the European Parliament (EP) and once the EP adopts its position (estimated to be in or around March 2023), the legislators will begin negotiations to reach a final agreement on the wording of the EU AI Act.

MedTech Europe Comments on the EU AI Act and the Council's Position. On December 7, 2022, MedTech Europe published two position papers: one on its view on the European Commission's proposed EU AI Act and the other on its reaction to the EU Council's general approach to the EU AI Act. In the former, MedTech Europe welcomes AI regulation that supports accessibility of AI in medical technologies, but is concerned that AI devices will be regulated by both the AI Act and the MDR. MedTech Europe states that regulatory alignment between sectors is essential to ensure that medical technology manufacturers can balance any new requirements against benefit-risk ratio requirements established in the MDR/IVDR. One particular area of concern is the diverging classification system between a high-risk AI system under the EU AI Act and the device risk classification under the MDR/IVDR.

In MedTech Europe's response to the Council's position, it repeats its concerns about the EU AI Act creating unnecessary regulatory burdens on providers of AI-enabled medical technologies. MedTech Europe welcomed reference to the MDR in the recitals to the EU AI Act, but requested further clarification on which legislation takes precedence and suggested that notified bodies carrying out the conformity assessments under the MDR could also carry out the relevant assessments under the EU AI Act. MedTech Europe also considered that the newly proposed definition for AI system remains unclear and does not meet its aim of distinguishing AI from traditional software.

Implementation of the EU MDR Likely to Be Delayed. On December 9, 2022, the European Commission announced its intention to set out proposals to extend the transitional period under the MDR. The Commissioner for Health and Food Safety noted that under the current timelines, "There is a real risk that most of medical devices will expire or not be available in the EU market." The full extent of the proposals were not published at that time. However, the information provided indicated that the new deadlines will be in 2027 or 2028 (depending on the risk classification of the device) and will be available to companies that comply with a number of conditions, for example that the manufacturer has already started the process to bring the device into compliance with the MDR. These changes will apply to all medical devices within the scope of the MDR, which will include digital health technologies. For more details, see our blog. The full text of the proposals was published on January 6, 2023 and will be covered in the next Digest.

Joint Agreement to Accelerate Access to HealthTech in the UK. On December 16, 2022, the UK's Life Sciences Council, MHRA, ABHI, and others agreed to accelerate the delivery of the future UK HealthTech regulatory system. The various bodies have established a new advisory group to drive the reform, which will publish initial proposals in February 2023 to accelerate access to innovative technologies. The proposals are likely to address how recognizing the approvals of technologies in other trusted countries could aid both industry and the UK system. The MHRA will also publish a roadmap on delivering the regulatory arrangements.

MHRA Receives Funding for Regulatory Innovation Projects. On December 19, 2022, it was announced that the MHRA received funding of £970,688 from a fund within the UK government's Department for Business, Energy & Industrial Strategy for three projects addressing scientific and digital innovation:

1. The first project, which will take between 12-18 months, involves developing synthetic datasets for control groups in clinical trials. Such datasets would mimic real patient data for use in clinical trials and would enable more patients to receive new potential treatments.
2. The second project is to develop a methodology for clinicians to know whether to follow or overrule decisions made by 'black-box' AI products.
3. The third project—not directly related to virtual and digital health—is to develop guidelines regulating microbiome therapeutics and diagnostics.

PRIVACY AND CYBERSECURITY

Code of Practice for App Developers and Operators. On December 9, 2022, the UK government published a voluntary code of practice (Code) for app developers and operators. The Code consists of eight principles, which sets out minimum security and privacy requirements to protect consumers. These principles include the requirement for apps to have a "vulnerability disclosure process" whereby security experts can report software vulnerabilities to developers, and the greater transparency of security and privacy information to users. The Code is aimed at all apps and therefore includes virtual and digital health-related apps. Developers of apps that qualify as medical devices are reminded to consult and comply with the UK Medical Device Regulation, accompanying guidance and NHS Digital Technology Criteria (DTAC). The Code also notes that NHS England and MHRA are considering "whether an enhanced regime focused on clinical safety for health apps are appropriate" so further regulation could be expected. The UK government will now work with app operators and developers to support them in the implementation of the Code over a nine-month period.

New Cybersecurity Requirements for Medical Device Manufacturers. On December 27, 2022, Directive (EU) 2022/2555 on cybersecurity was published in the Official Journal of the European Union (the NIS 2 Directive). The NIS 2 Directive repeals and replaces the Directive (EU) 2016/1148 on the Security of Network and Information Systems (the NIS Directive).

A number of interlocking rules regulate cybersecurity for medical devices. For example, the (now repealed) NIS Directive aimed to build cybersecurity capabilities across the EU by requiring companies and institutions to take measures to manage cybersecurity and report major security incidents. In addition, the MDR sets out a number of cybersecurity requirements for medical devices. For example, devices shall be designed and manufactured to remove or reduce "risk associated with the possible negative interaction between software and the IT environment within which it operates and functions." MDCG 2019-16 sets out specific guidance on how to comply with the cybersecurity requirements in the MDR. However, to keep up with technological developments (and threats) in this area, the NIS 2 Directive has now been adopted. This has a broader scope and now specifically imposes cybersecurity requirements on manufacturers of medical devices and in vitro diagnostic medical devices. Such manufacturers may be classified as an "important entity" or an "essential entity"; the latter being those entities that manufacture medical devices considered to be critical during a public health emergency. Essential entities are subject to an ex ante and ex post supervisory regime to ensure compliance with the NIS 2 Directive and higher possible fines, whereas important entities are only subject to ex post supervision. To ensure compliance with the NIS 2 Directive, device manufacturers will need to carry out

appropriate cybersecurity risk-management measures and report cybersecurity incidents within certain timeframes. The NIS 2 Directive will enter into force in January 2023 and Member States will have until October 17, 2024 to transpose the measures into national law.

It is worth noting that a recently proposed regulation on horizontal cybersecurity requirements for products with digital elements will not apply to medical device manufacturers.

TELEHEALTH

UK Announces Digital Health Check Trial. On December 5, 2022, the UK's Department of Health and Social Care (DHSC) announced a trial to introduce digital healthcare checks into the NHS. The trial is a part of the UK government's plan to digitise routine health checks and involves selected patients completing an online questionnaire, using a kit to take and submit their own blood samples, and completing a blood pressure check at pharmacies or doctor's surgeries. The aim is to reduce pressure on doctor's surgeries, whilst being more convenient for patients. Results and feedback from the trial will inform the development of the planned "NHS Digital Health Check."

REIMBURSEMENT

Early Value Assessment Statement From NICE. On December 15, 2022, the UK's National Institute for Health and Care Excellence (NICE) published an interim statement on the methods and processes being tested for the early value assessment (EVA) and further evidence generation of medical and digital health technologies. EVA is a new evidence-based approach aimed at facilitating quicker access to health technologies addressing unmet needs or priority areas. Part of this approach is for NICE to conditionally recommend the health technology for use while further evidence is generated in accordance with an evidence generation plan. NICE is running at least 10 pilot cases and the learnings from the pilot will be used to inform the final design of the EVA process, which will be documented in a guidance manual in 2023-2024.

ANTITRUST/COMPETITION AND FOREIGN INVESTMENT

Additional Deals Blocked Under the NSIA. On December 19, 2022, two additional transactions were blocked by the UK government under the National Security and Investment Act (2021) (NSIA). The first transaction is the acquisition by Luxemburg-registered private equity firm LetterOne Core Investment over UK-based fibre network provider Upp Corporation. After the transaction closed on January 21, 2021, the UK government ordered LetterOne to sell 100 percent of Upp Corporation over concerns around the acquirer's links to a number of sanctioned Russian oligarchs. The second transaction being prohibited is the proposed acquisition of HiLight Research, a UK-based designer of integrated circuits, by Chinese SiLight (Shanghai) Semiconductor.

As mentioned in the November edition of this Digest, the NSIA, which came into force on January 4, 2022, introduced a mandatory and suspensory filing obligation for transactions in 17 sectors considered as particularly sensitive to the UK national security—among these are advanced materials, advanced robotics, and, importantly, AI. Looking back to the first year of the NSIA's application, in addition to a number of deals cleared without remedies, five deals have been blocked in total and nine have been approved subject to remedies. To read more about the NSIA, including the separate voluntary notification regime, see our Advisory.

Proposed Acquisition in Hearing Implants Sector Faces In-depth Merger Review. On December 20, 2022, the UK Competition and Markets Authority (CMA) referred the anticipated acquisition by Cochlear Limited over Oticon Medical (the hearing implants business of Danish Demant A/S) to a Phase II in-depth investigation. The CMA is concerned that the merger between two leading suppliers of surgically implanted hearing devices could result in reduced competition in the bone conduction solutions market, possibly leading to higher prices for the NHS and reduced quality and slower innovation for UK patients needing bone conduction hearing implants. In a recent press release concerning the deal, the CMA reminded industry that "healthy competition in the medical technology sector is central to continued innovation, more choice and improvements in patient treatments". The deadline for the CMA to either clear the deal, impose remedies, or issue a blocking decision is June 5, 2023.

Questions/Comments?

Contact a member of our Editorial Committee

Allison Shuren
Partner
Washington, DC

Abeba Habtemariam
Partner
Washington, DC

Jackie Mulryne
Partner
London

Nancy L. Perkins
Counsel
Washington, DC

Monique Nolan
Counsel
Washington, DC

Ludovica Pizzetti
Counsel
EU/UK

Amanda Cassidy
Sr. Health Policy Advisor
Washington, DC

Emma Elliston
Associate
London

Alison Peters
Associate
Washington, DC