Arnold&Porter

VIRTUAL AND DIGITAL HEALTH DIGEST

Welcome to the second installment of Arnold & Porter's Virtual and Digital Health Digest. This edition primarily covers November 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

FDA Updates Medical Device Cybersecurity Playbook for Healthcare Organizations. On November 15, 2022, FDA, in collaboration with MITRE, released an update to the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook (Cybersecurity Playbook). First published in 2018, the Cybersecurity Playbook outlines a stakeholder-derived, open source and customizable framework for healthcare delivery organizations (HDOs) and other stakeholders to prepare for and respond to medical device cybersecurity incidents, namely attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in medical devices. FDA asked MITRE to update the Cybersecurity Playbook due to the recent growth in ransomware attacks, the increasing connectivity of medical devices and emerging healthcare technologies. The healthcare and public health sector has continued to experience growing numbers of cyber incidents, with 82 percent of healthcare systems reporting a cyber incident between mid-2020 through 2021 (34 percent of which involved ransomware). As updated, the Cybersecurity Playbook includes more explicit alignment with the Hospital Incident Command System for managing complex incidents, considerations for the widespread impacts and extended downtimes that are common during cyber incidents, and an appendix of resources.

The high-level structure of the recommendations in the Cybersecurity Playbook follow the incident response lifecycle from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61r2, *Computer Security Incident Handling Guide*. This lifecycle has four phases: (1) preparation phase; (2) detection and analysis phase; (3) containment, eradication and recovery; and (4) post-incident activity. Preparation phase recommendations include ones relating to medical device procurement, medical device asset inventory, hazard vulnerability analysis, medical device cybersecurity support to the hospital incident management team, incident response communication plan, and user awareness training and cybersecurity exercises. Detection and analysis phase recommendations include ones relating to incident detection and validation, incident categorization and prioritization, incident reporting, incident analysis, and incident documentation. Under containment, eradication and recovery, the Cybersecurity Playbook discusses considerations for selecting the appropriate containment strategy and recommends that HDOs plan for a potentially lengthy recovery period of weeks or even months because resolving incidents is not always straightforward. During the post-incident phase, the Cybersecurity Playbook suggests examining what went well and what did not with regards to the HDO's response to the incident and using that information to improve the response plan for future incidents.

In conjunction with the updated Cybersecurity Playbook, FDA and MITRE also released a Quick Start Companion Guide (Quick Start Guide". The QuickStart Guide as a shorter version of the playbook that discusses preparedness and response activities healthcare organizations might want to start with as they are developing their medical device incident response program. The Quick Start Guide consists of tables that distill the high-level tasks presented in the corresponding section of the Cybersecurity Playbook.

FTC, FDA, Other Agencies Create Mobile Health App Interactive Tool. On December 7 2022, the FTC released a mobile health app interactive tool (Mobile Health App Navigator) to help app developers navigate the various US federal laws and regulations that may apply to such apps. Representing a cross-agency effort, the Mobile Health App Navigator was produced in cooperation with the US Department of Health and Human Services (HHS), the FDA, the Office of the National Coordinator for Health Information Technology (ONC), and the office for Civil Rights (OCR) within HHS. The Mobile Health App Navigator is intended "for anyone developing a mobile app that will access, collect, share, use, or maintain information related to an individual consumer's health, such as information related to diagnosis, treatment, fitness, wellness, or addiction." However, the FTC cautions that the Mobile Health App Navigator is provided for informational purposes only and use of the tool "can[not] guarantee compliance with applicable federal requirements." Instead, the Mobile Health App Navigator is meant to provide app developers with a snapshot of potential compliance obligations and point them to educational materials and best practices for delivering safe, accurate services while safeguarding the privacy and security of consumer information.

The interactive tool provides an overview of various federal laws and regulations that may apply to a mobile health app, such as the following:

- Health Insurance Portability and Accountability Act (HIPAA) Rules
- Federal Food, Drug and Cosmetic Act (FDCA) and FDA Regulations
- 21st Century Cures Act and ONC Information Blocking Regulations
- FTC Act (e.g., Sections 5 and 12)
- FTC's Health Breach Notification Rule
- Children's Online Privacy Protection Act

The Mobile Health App Navigator uses a series of questions to help guide app developers through an analysis of whether all or certain of the above laws and regulations could apply to a proposed mobile health app. Examples of questions covered in the interactive tool include ones about the app's functionality, whether the app is intended for use by consumers, the type of information the app collects, shares or uses, whether the app is being offered by or on behalf of a HIPAA-covered entity, whether the app connects with wearables or other devices, whether the app accesses information in or sends information to personal health records or provides services to an entity that maintains health records for consumers, and whether the app is intended for children or uses child-oriented activities or design.

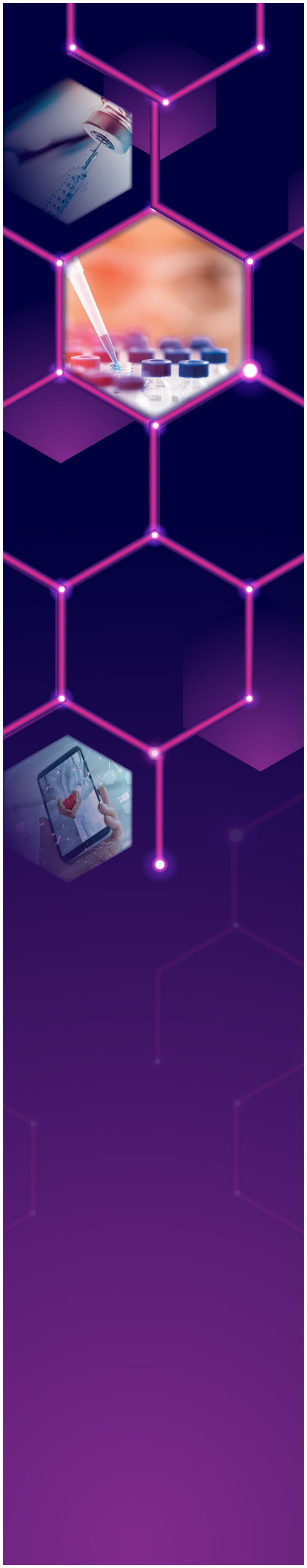
Questions relating specifically to whether a proposed app is potentially regulated as a medical device by the FDA are covered in questions 7-10 of the Mobile Health App Navigator. These include questions intended to assess whether an app is intended to diagnose, prevent or treat a disease or condition, whether the app could potentially fall under one of the 21st Century Cures Act statutory exemptions from the device definition for certain low risk software functions, or whether the app, even if not statutorily exempt, could potentially be subject to enforcement discretion under FDA policies for certain low risk device software functions. For an overview on the latest FDA digital health guidances, including the agency's recently issued final guidance on clinical decision support tools, please refer to the November 2022 issue of Arnold & Porter's Virtual and Digital Health Digest.

FDA Releases List of Augmented Reality and Virtual Reality Medical Devices. On December 7, 2022, FDA released a list of medical devices authorized for marketing that incorporate augmented reality (AR) and virtual reality (VR). This move follows FDA previously releasing a list of artificial intelligence (AI)/machine learning (ML)-enabled devices authorized for marketing by the agency and signals continued FDA efforts for greater transparency about advancements in the digital health space. Additional information about FDA's list of AI/ML-enabled devices can be found in the November 2022 issue of Arnold & Porter's Virtual and Digital Health Digest.

In conjunction with release of the AR/VR devices list, FDA provided background information on AR/VR technologies. FDA defines AR as "a real-world augmented experience with overlaying or mixing simulated digital imagery with the real world as seen through a camera or display, such as a smartphone or head-mounted or heads-up display," and defines VR as "a virtual world immersive experience that may require a headset to completely replace a user's surrounding view with a simulated, immersive and interactive virtual environment." FDA highlights a few examples of AR and VR applications already being used to treat patients, including a VR system that is used to treat post-traumatic stress disorder in army veterans and an AR system that overlays medical images onto a patient during an operation to help guide the surgeon's techniques. FDA identifies a number of treatment domains where AR and VR are used to treat patients, including pediatric diagnostics and treatments, pain management, neurological disorders, surgery planning, telemedicine, virtual care, and ophthalmic diagnostics. While acknowledging potential benefits of AR/VR devices, FDA also identifies potential risks, such as cybersickness, head and neck strain, cybersecurity risks, privacy risks, and distraction in the operating room.

FDA's initial list of AR/VR devices authorized for marketing contains 39 devices that the agency identified by searching FDA's publicly facing information. The vast majority of the devices on the list appears to have been cleared for marketing through FDA's premarket notification (510(k)) process, while a few appear to have been authorized through the *de novo* classification process for novel devices. FDA explains that the list is not intended to be exhaustive or comprehensive, but rather that it is a list of devices that incorporate AR and VR based on information provided in the summary descriptions of their marketing authorization documents. FDA plans to update the AR/VR devices list on a periodic basis.

FDA Publishes Digital Health Regulatory Science Opportunities Spotlight. FDA's Digital Health Center of Excellence (DHCoE) recently issued a publication entitled "Spotlight: Digital Health Regulatory Science Opportunities" (Digital Health Spotlight). The Digital Health Spotlight describes areas of research that



stakeholders, both internal and external to the FDA, identified as important and is intended to advance digital health regulatory science by encouraging discussions and stakeholder collaborations throughout the healthcare ecosystem and beyond. The Digital Health Spotlight identifies three main categories of research: Advancing Patient Engagement, Leveraging Connectivity and Improving Healthcare Through Software. Under Advancing Patient Engagement, the Digital Health Spotlight highlights patient-generated health data (PGHD) and the development of medical extended reality devices as important areas of research. PGHD, including biometric data, symptoms and patient-reported outcomes, can be used in patient monitoring, diagnosis and prognosis, shared decision-making, and assessment of patient safety. FDA notes PGHD data can be used not only to improve the quality of clinical care, but also to evaluate innovative medical products and treatment paradigms, especially decentralized clinical investigations. The Digital Health Spotlight identifies several PGHD-related research areas, such as maintenance and management of large volumes of PGHD, standardization of PGHD from different sources, performance specifications for use when considering interchangeability of wearables (e.g., "bring your own wearable" approaches to clinical investigations), and reliable metrics to compare standard disease outcomes as measured by digital health technologies.

Under Leveraging Connectivity, the Digital Health Spotlight focuses on cybersecurity, wireless connectivity and interoperability as important areas of research. FDA explains that it is actively engaged in both internal and external efforts to help mature cybersecurity, interoperability and wireless connectivity efforts. A few examples of cybersecurity-related research areas discussed in the Spotlight include cybersecurity considerations for cloud domains, cybersecurity considerations for AI and ML technologies, and cybersecurity standards development. And under Improving Healthcare Through Software, the Digital Health Spotlight emphasizes the importance of research involving advanced manufacturing technologies, AI and ML, and digital imaging. Examples of AI/ML-related research areas include transparency of AL/ML-enabled devices, AL/ML algorithm training for clinical datasets, robustness and resilience of algorithms to withstand changes in patients, data and sources, and real-world performance monitoring for AI/ML software.

In issuing the Digital Health Spotlight, FDA explained that the spotlight on research areas is for informational purposes only, and that it is not meant to indicate that the identified topics are areas for regulation. Further, the Digital Health Spotlight is not intended to propose or implement policy changes regarding regulation of any of the digital health topic areas described within.

FDA Report Highlights Potential Use of Modeling & Simulation in Digital Health Product Reviews. In November 2022, FDA released a report entitled "Successes and Opportunities in Modeling & Simulation for FDA." The report explores how modeling and simulation (M&S) tools are used throughout FDA and presents a selection of M&S case studies from across FDA centers. M&S tools are used, for example, for premarket product review, postmarket product assessment, policy development, and policy implementation. The report also identifies opportunities for FDA to better harness M&S in upcoming years by embracing computational advances and new (and big) data streams to develop improved public health solutions. As relates specifically to digital health, one of the M&S opportunities highlighted in the report is to provide evidence supporting safety or effectiveness of medical imaging devices and computer-aided diagnostic software. Specifically, leveraging radiation transport simulations to generate evidence that can assist in the regulatory process for medical imaging devices and computer-aided diagnostic software. Noting that industry already invests heavily in developing tools that can simulate radiological devices for internal R&D, the report states that there is an opportunity to use these tools in the regulatory process, especially for submissions which do not normally require clinical data (e.g., some 510(k) devices). Another opportunity discussed in the report is establishment of Good Simulation Practice to foster harmonization across the FDA, and where appropriate, with international

regulatory bodies. The report explains that it is critical to develop a common set of expectations or guidelines for model verification, validation, credibility assessment and maintenance between industry and regulators, as well as between regulatory scientists/modelers and reviewers within the FDA, and states further publication and/or usage of relevant guidance documents will promote better alignment on best practices and expectations between stakeholders (e.g., International Council on Harmonization items Q13 and M7, and the International Medical Device Regulators Forum on Software as a Medical Device).

HEALTHCARE FRAUD AND ABUSE UPDATES

AMA Future of Health Report. On November 9, 2022, the American Medical Association (AMA) released the Future of Health Report, addressing issues in digitally enabled care. The Report summarizes what AMA calls the "digital health disconnect," which AMA defines as a "chasm between the theoretical potential that digitally enable care models promise and the reality of 'parallel' care that predominates today." The Report offers a "blueprint" for optimizing digitally enabled care.

To realize the potential of digitally enabled care and appreciate the drivers of the digital health disconnect, the AMA asked stakeholders for their perspectives on how the digital health industry evolved over the past ten years. Though the stakeholders' perspectives varied, almost all of them agreed that in order to close the digital health disconnect, it was important to avoid perpetuating the failures of today's healthcare system, including:

- Lack of patient, family, and physician centricity in care model design.
- Care fragmentation.
- Data silos.
- Overly complex payment models that disincentivize high-value care.
- Asking too much of overburdened physicians.
- Too slow to scale effective care models.

Multiple Health Care Providers charged in Telehealth Fraud as OIG/DOJ Continue Crackdown. On November 18, 2022, an indictment was unsealed detailing how six individuals, including two doctors and the operators of three pain clinics, were charged with conspiring to illegally distribute over 500,000 opioid pills worth over $2.6 million. This drug conspiracy involves Schedule II controlled substances including Oxycodone, Oxymorphone, Oxycodone-Acetaminophen (Percocet), and Hydrocodone (Norco) opioids known for being highly addictive and having a significant street value. Several pain clinics in the Metro Detroit area allegedly used "patient recruiters" to recruit patients to see Drs. Juan Bayolo and Renee Gonzales Garcia via telehealth. Bayolo and Garcia received payments in exchange for illegally issuing medically unnecessary opioid prescriptions to patients without first conducting a physician examination of the patients.

These charges are particularly salient in light of the ongoing debate of whether to extend COVID-19 telehealth flexibilities, including the ability to prescribe controlled substances via telemedicine. For example, in a December 1, 2022 letter to Drug Enforcement Agency Administrator Anne Milgram, the American Hospital Association urged the DEA to release regulations for prescribing controlled substances via telehealth after COVID-19 public health emergency (PHE) regulations end.

In another case, Ruth Bianca Fernandez was sentenced to three years in federal prison for conspiracy to commit healthcare fraud and making a false statement in a matter involving medically unnecessary durable medical equipment (DME) paid for by federal healthcare programs. The telemarketing operation allegedly relied upon a "telemedicine" vendor who purportedly was paying illegal bribes to physicians to sign orders for the DME. Fernandez and her co-conspirators caused approximately $25 million in fraudulent DME claims to be submitted to Medicare, leading to approximately $12 million in improper payments.

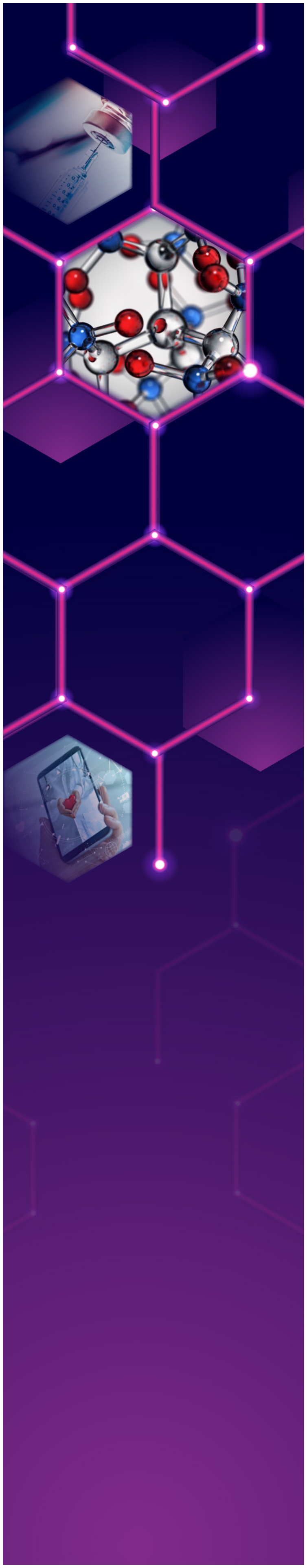
MassHealth Providers Engage in Improper Telehealth Billing Practices. On November 23, 2022, the Commonwealth of Massachusetts Office of the State Auditor (OSA) released a performance audit on MassHealth, the Massachusetts's Medicaid program, expenses between January 1, 2020, and June 30, 2022, focusing on whether "MassHealth monitor[s] telehealth practices for behavioral health services to ensure compliance." Specifically, with respect to MassHealth's telehealth services, OSA found that MassHealth made payments totaling at least $91,852,881 to its providers for telehealth behavioral health services that were not properly documented. OSA's November audit also cited previous MassHealth performance audits that identified "weaknesses" in MassHealth's coding and billing practices," which OSA stated "resulted in millions of dollars in potentially improper payments." OSA recommended that "MassHealth should train its providers, and establish monitoring controls, to ensure that telehealth services are documented in accordance with its All Provider Bulletins."

OIG Insights on Telehealth Use and Program Integrity Risks Across Selected Health Care Programs During the Pandemic. On November 30, 2022, OIG released the "Insights on Telehealth Use and Program Integrity Risks Across Selected Health Care Programs During the Pandemic" Report on the expansion of telehealth in federal programs during the pandemic. According to the Report, the use of telehealth has helped multiple federal healthcare programs provide continued access to healthcare to approximately 37 million individuals during the first year of the pandemic, an increase from the 3 million that accessed telehealth in the year prior. The OIG's Pandemic Accountability Committee (PRAC) Health Care Subgroup's Report focuses on the use of telehealth in programs across six participating OIGs—HHS, the Department of Defense, the Office of Personnel Management, the Department of Veterans Affairs, the Department of Labor, and DOJ—during the first year of the COVID-19 pandemic and highlights telehealth risks identified by these federal agencies. Further, the Report advises stakeholders, such as Congress, federal and state agencies, and healthcare organizations, on how the expanded use of telehealth during the COVID-19 pandemic helped individuals access healthcare during a crisis and raised awareness about the critical importance of safeguarding expanded telehealth services against fraud, waste and abuse. PRAC explained that the Report may be used to "inform decisions on which telehealth changes should remain after the pandemic."

The Report's findings from the OIGs include, for example:

- The OIGs took measures to provide accessible telehealth services during the pandemic.
- The OIGs supplied fairly similar coverage of telehealth services during the pandemic.
- Compared to the year prior to the pandemic, the use of telehealth drastically increased during the first year of the pandemic for each of the OIGs.

- OIGs identified several program integrity risks associated with billing for telehealth services that were similar across multiple programs:
  - Inappropriate billing for the highest, most expensive level of telehealth services;
  - Duplicate claims and high-volume billing;
  - Billing for services that were seemingly not appropriate for telehealth or ineligible for payment as a telehealth service; and
  - Ordering unnecessary durable medical equipment or laboratory tests associated with telehealth visits.
- Added safeguards to oversee telehealth services could strengthen program security within the selected programs in the six federal agencies.



HHS Solicitation of Proposals for New and Modified Safe Harbors and Special Fraud Alerts.

While not directly related to virtual and digital health, OIG and HHS have issued its Solicitation of Proposals for New and Modified Safe Harbors and Special Fraud Alerts. With the growing development and utilization of digital tools and virtual care delivery models, consideration should be given to possible proposals and recommendations for the OIG to develop new, or modify existing, safe harbor provisions under section 1128B(b) of the Social Security Act, the Federal Anti-Kickback Statute, as well as developing new OIG Special Fraud Alerts, to more directly support care models that may involve engagement by providers, suppliers and manufacturers of products.

As specified by section 205 of the Health Insurance Portability and Accountability Act of 1996 (HIPPA), OIG and HHS consider multiple factors when reviewing proposals for modified or additional safe harbor provisions, including the extent that the proposals could lead to an increase or decrease in:

- Access to healthcare services;
- Quality of healthcare services;
- Patient freedom of choice among healthcare providers;
- Competition among healthcare providers;
- Cost to federal healthcare programs;
- Potential overutilization of healthcare services; and
- Ability of healthcare facilities to provide services in medically underserved areas or to medically underserved populations.

OIG and HHS also consider factors such as the existence or nonexistence of any likely financial benefit to healthcare professionals or providers that may influence their decision to: (i) order a healthcare item or service or (ii) arrange for a referral of healthcare items or services to a particular practitioner or provider.

When determining whether to release more Special Fraud Alerts, OIG and HHS consider whether and to what extent the practices identified in a new Special

Fraud Alert could result in any of the aforementioned consequences, in addition to the volume and frequency of the conduct that would be identified in the Special Fraud Report. **Public comments are due by 5 PM on January 27, 2023.**

INVESTMENT/TRANSACTIONS

Q3 2022 Digital Health Funding: The Market Isn't the Same as It Was

2021 saw record venture funding in the virtual and digital health space resulting in deployment of capital approaching $29.2 billion; however, the pace of investment and volume of transactions during 2022 has slowed to almost half of that amount, predominately in response to a bevy of macroeconomic factors including inflation, rising interest rates and fears of a recession. RockHealth attributes this pullback in late-stage digital health funding to the following three reasons:

1. A portion of the "missing deals" already happened, pulled forward to 2021 in order take advantage of last year's funding-friendly climate
2. Another portion of deals are in fact happening, but behind closed doors via arrangements like round extensions and venture debt
3. A final portion of deals are simply not taking place

Further, while Q3 saw digital health acquisitions by Amazon (One Medical) and CVS (Signify Health) there were just two raises totaling $100 million or more during the same period: one from heart attack prediction app Cleerly ($223 million) and another from mental health provider support toolkit Alma ($130 million).

Looking forward to 2023, there remains a large amount of dry powder in the hands of healthcare focused investors and, given continued interest and further regulatory clarity, it is anticipated that the pace of virtual and digital health transactions will increase; however, the variable is whether 2022 reflected a correction in valuations that will result in lower multiples going forward.

PROVIDER REIMBURSEMENT UPDATES

Top of Mind for Health Systems 2023 Report. A new report published by the Center for Connected Medicine (CCM), in partnership with KLAS Research, provides a fuller picture of the digital health landscape, as seen by healthcare executives. Through surveys from 61 leaders from 59 hospital and health systems across the United States, the Top of Mind for Health Systems 2023 Report identifies telehealth as the area of healthcare technology with the greatest progress and improvement over the last two years. The report identifies patient convenience as the largest benefit of telehealth, according to surveyed leaders.

While healthcare executives generally view telehealth favorably, they also see many challenges to its continued growth. Specifically, the report cites insufficient reimbursement as the largest barrier to telehealth adoption, particularly for larger health systems. The "uncertain reimbursement landscape" is also a worry for executives. The report notes that many executives wonder whether reimbursement for telehealth will continue to have parity with in-person appointments following the end of the PHE. With regard to Medicare, payment parity has been afforded temporarily during the PHE. Specifically, the Centers for Medicare & Medicaid Services (CMS) modified its billing policy and has allowed payment to physicians and practitioners for Medicare telehealth services at the same reimbursement rate as services furnished in-person. See 87 FR

69466. This policy will end, however, the latter of the end of calendar year 2023 or the end of the calendar year in which the PHE ends. *See* 87 FR 69467.

In addition to reimbursement, the report highlighted patient technology barriers and the lack of provider adoption as the second and third greatest challenges, respectively, to wider telehealth adoption. Surveyed leaders cited patient access as the problem in healthcare with the greatest potential to be improved with digital health technology and innovation. To address these ongoing needs, the report finds that some healthcare organizations created specific executive-level roles to oversee patient access strategy.

Advancing Interoperability and Improving Prior Authorization Processes: Proposed Rule CMS-0057-P. On December 6, 2022, CMS released a proposed rule aiming to "improve the electronic exchange of healthcare data and streamline processes related to prior authorization, while continuing CMS' drive toward interoperability in the healthcare market." *See* 87 FR 76238. This proposed rule builds upon the *CMS Interoperability and Patient Access* final rule published in May 2020. And, in light of public comments, this rule formally withdraws the *CMS Interoperability and Prior Authorizatio*n proposed rule from December 2020.

CMS is proposing changes to prior authorization processes in light of provider burnout and patients abandoning treatment due to lengthy delays caused by system inefficiencies. To address these challenges and reduce burden, the proposed rule would require impacted payers to build and maintain a Prior Authorization Requirements, Documentation and Decision Application Programming Interface (PARDD API) to automate and manage the entire prior authorization process. Specifically, the API would determine when a prior authorization is required, identify key documents and facilitate the exchange of such requests from patient electronic health records or practice management systems. *See* 87 FR 76424.

In addition, the proposed rule proposes a new electronic prior authorization measure for Merit-based Incentive Payment System (MIPS) eligible clinicians and for eligible hospitals and critical access hospitals under the Medicare Promoting Interoperability category of MIPS and the Medicare Promoting Interoperability Program, respectively. Under this proposal, these three groups would be required to report the number of prior authorizations they receive for medical items and services that are electronically requested from a PARDD API database using data from certified electronic health record technology. *See* 87 FR 76243. Additionally, in a departure from the December 2020 proposed rule, CMS declines to propose that Implementation Guides (IGs) be required for the implementation of APIs and indicates it will continue to monitor and evaluate the development of such IGs for consideration in future rulemaking. *See* 87 FR 76316.

The proposed rule also includes five requests for information (RFIs) seeking feedback for possible future rulemaking or other initiatives. CMS requests information related to barriers to widespread adoption of these standards related to social risk data, as well as how CMS could better leverage APIs for the electronic exchange of behavioral healthcare information. CMS also seeks comments "on how using data standards and electronic health records can improve maternal health outcomes" as well as strategies to improve usage of exchange under the Trusted Exchange Framework and Common Agreement (TEFCA). *See* 87 FR 76243.

PRIVACY UPDATES

HHS OCR Warns That Online Tracking Technologies May Trigger HIPAA Violations.

On December 1, 2022, the Office for Civil Rights (OCR) at HHS issued a bulletin highlighting the risks under the Health Insurance Portability and Accountability Act privacy and security regulations (collectively, the HIPAA Rules) of using online tracking technologies, such as Google Analytics and Meta Pixel. Many HIPAA "covered entities" and their "business associates" (HIPAA-regulated entities) have websites or mobile applications that may use such tracking technologies. Generally, tracking technologies developed by vendors such as Google and Meta send information directly to the vendors, who can continue to track website or mobile application users and gather information about the users after they leave the site or cease use of the mobile app. OCR is concerned that this information may include personally identifiable health information, which is "protected health information" (PHI) if received or created by a HIPAA-covered entity or its business associate, and that the use of online tracking technologies may involve unauthorized disclosures of PHI.

As the OCR Bulletin clarifies, all individually identifiable health information collected on a HIPAA-regulated entity's website or mobile app is generally considered PHI, because the use of online tracking technologies connects the individual to the regulated entity and thus indicates that the individual has received or will receive healthcare services or benefits from the covered entity. Depending on (i) the specific information and (ii) the particular online tracking environment (i.e., whether a user-authenticated webpage, an unauthenticated webpage or a mobile application), a covered entity using tracking technologies may be disclosing PHI to the tracking technology vendor. This could occur on login pages or registration pages; patient or health plan beneficiary portals or telehealth platforms; webpages with general information about the regulated entity such as their location, services provided or their policies and procedures; webpages addressing specific symptoms or health conditions; and webpages that permit an individual to search for doctors or schedule appointments.

Under the HIPAA Rules, HIPAA covered entities may disclose PHI to their vendors if they bind the vendors to protect the PHI under so-called "business associate agreements" (BAAs). Online tracking technology vendors are considered business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity in order to assist the covered entity in performing its healthcare and operational activities. A tracking technology vendor is a business associate and is directly subject to the HIPAA Rules if it meets the definition of a business associate, regardless of whether the required BAA is in place. Yet many tracking technology vendors, if they have not been asked to sign a BAA, may be unaware that they are subject to the HIPAA Rules. And without a BAA in place, a covered entity violates the HIPAA Rules in disclosing PHI to vendors without authorization from the individuals to whom the PHI pertains.

The OCR Bulletin is likely to cause many covered entities to question whether they can use tracking technologies without running afoul of the HIPAA Rules and may be a wake-up call to tracking technology vendors whose customers include healthcare providers, health plans and entities servicing those HIPAA covered entities as well.

EU and UK News

REGULATORY UPDATES

New WHO Guide on Implementing Telemedicine. On November 10, 2022, the World Health Organization (WHO) issued a consolidated guide to help policy-makers, decision makers and implementers design and deliver effective telemedicine services. The aim of the guide is to provide an overview of the key steps and considerations for implementing telemedicine interventions, optimizing its benefits, impact and sustainability and mitigating potential risks. The guide is split into 3 "phases" ((i) situational assessment; (ii) implementation; and (iii) monitoring, evaluation and continuous improvements) and each phase is split into several steps, to help support countries at different stages in their telemedicine implementation. The guide concludes with several case studies of countries that have implemented a telemedicine intervention, discussing the main challenges that were encountered and the lessons learned.

A WHO Review on Digital Health Technologies. On November 22, 2022, the WHO Regional Office for Europe published Monitoring the Implementation of Digital Health: An overview of Selected National and International Methodologies. The report summarized that the international community made significant efforts in monitoring the adoption and use of digital health technologies but that improvements could be made. In particular, the report suggests that the development, collection and publication of comparable data and indicators could help to evaluate the impact of digital health technology initiatives and countries could share their knowledge on measuring digital health maturity levels. Furthermore, the study highlighted that telehealth needed to be more systematically monitored and new indicators to monitor digital health inequalities should be devised.

Digitalization Identified as a Key Enabler in the EU Global Health Strategy. On November 30, 2022, the European Commission adopted a new EU Global Health Strategy to improve global health security and deliver better healthcare. Digitalization, including the use of AI, is identified as a key enabler for strengthening health systems and advancing universal health coverage. Guiding principle 4 of the strategy outlines various action points for EU leaders to take to foster global digitalization including, for example: (i) addressing the underinvestment in digital health in low- and middle-income countries; (ii) building the EU's capabilities as a pioneer in the regulation and leveraging of health data; and (iii) contributing to shaping the digital health ecosystem globally using EU examples and best practices. The strategy provides specific examples of how digital health could transform universal health coverage. For example, telemedicine may facilitate access to expertise from geographically remote locations and AI's use of health data could improve diagnosis and treatment worldwide.

MedTech Europe Report on AI in Healthcare Systems. On November 2, 2022, MedTech Europe published a report regarding its October event in which participants discussed the benefits of AI in healthcare systems and their views on a future AI regulatory system. Participants agreed that AI has great potential to improve patient outcomes by utilizing the vast amounts of available health data to help the healthcare sector manage workloads, aid researchers in the discovery of new medicines and help patients manage and monitor their conditions. The report notes that the newly proposed EU AI Act (discussed in the November edition of the digest) creates uncertainty for the well-regulated medical technology sector and that policy makers need to provide a consistent framework to ensure the continued availability of innovative, AI-enabled medical technologies.

Recommendations to the UK Government on the Regulatory Framework for AIaMD. The Regulatory Horizons Council (RHC), an independent expert committee that provides the UK government with advice on the regulatory reform required to introduce technological innovations, published a report on November 30, 2022 regarding the regulation of artificial intelligence as a medical device (AIaMD). The report discusses the regulatory challenges of AIaMD, the gaps in the current regulatory system and proposes a number of recommendations to address those gaps. The recommendations include devising a "legislatively light" AIaMD regulatory framework that makes use of standards and guidance (so they can be updated more frequently as the technology advances). This is similar to the position taken in the UK Government's Policy Paper on AI (discussed in our blog post) and in the MHRA's AI Change Programme and response to the consultation on the future regulation of medical devices (discussed in our blog posts here and here). The recommendations also suggest requiring manufacturers to provide evidence that they have evaluated and mitigated the risks of poor generalizability and AI bias. Annex B to the report also provides a helpful snapshot of how AIaMD is regulated around the world. The UK government stated that the Department of Health and Social Care will respond to the RHC's recommendation.

The Potential of Digital Endpoints in Patient-Focused Health Management. On November 30, 2022, European Federation of Pharmaceutical Industries and Associations (EFPIA) published an article which discusses how digital endpoints have the potential to better inform regulatory and HTA decisions. Digital endpoints are those derived from data generated from digital health technologies, often collected by patients outside of the clinical setting. EFPIA notes that their use could provide improved and stronger evidence that is more objective and meaningful to patients, as well as decreasing the time and costs related to clinical trials. The article discusses how the Digital Evidence Ecosystem and Protocols (DEEP) initiative and the Innovative Health Initiative (IHI) are addressing gaps in the current digital endpoints ecosystem. EFPIA notes that an important component relates to facilitation of regulatory interactions and that these concepts are being piloted with the EMA.

PMCPA Advice on Adverse Event Reporting Statements in Digital Materials. On November 18, 2022, the PMCPA released advice to clarify its position with regards to the provision of the adverse event reporting statement in digital materials, particularly banner advertisements. The PMCPA reported that there had been confusion around the requirement to include a statement on how adverse events should be reported and whether including this information within the prescribing information by way of a link would satisfy the requirements. This method is used in digital advertising materials given the limited space on a screen and ease of including links. The PMCPA confirmed that the adverse reporting statement is a separate requirement to the prescribing information requirement and there is no allowance in the Code for the adverse reporting statement to be provided by way of a link. PMCPA clarified that the statement must be included within digital materials including banner advertisements "in a way where it is unlikely to be missed."

REIMBURSEMENT UPDATES

Working Towards a European Evaluation Framework for Digital Medical Devices. Towards the end of October 2022, a European taskforce was launched to develop a European evaluation framework for digital medical devices. The aim of the taskforce is to harmonize the health technology assessment (HTA) evaluation criteria in the EU by reaching a consensus with national competent agencies. France and Germany, two countries that have implemented fast track mechanisms for the reimbursement of digital technologies, are key participants in the taskforce. The taskforce will focus on three work packages: (i) harmonizing the classification of different types of digital medical devices according to their application; (ii) harmonizing clinical requirements to assess digital medical devices whilst respecting the mandates of national authorities; and (iii) propositions of an evaluation framework to include the socioeconomic dimension of digital medical devices in the context of their integration into health systems. Their findings will be presented at the end of the first quarter of 2023.

Proposal From MedTech Europe on the Implementation of the HTA Regulation. On November 24, 2022, MedTech Europe proposed that a "dedicated medical and digital technologies method subgroup" should be established as part of the European Regulation on Health Technology Assessment to enable the better assessment and reimbursement of medical and digital technologies. The HTA Regulation entered into force in January 2022 and applies as of January 2025 and seeks to harmonize certain aspects of the HTA process across the EU. The proposed subgroup would develop and implement adaptive joint clinical assessments methodologies, addressing the specificities of medical technologies by Q4 2026. MedTech Europe expressed its willingness to collaborate with the European Commission and Member States on the implementation of the HTA Regulation.

COMPETITION AND FOREIGN DIRECT INVESTMENT UPDATES

Another Deal Blocked Under the NSIA. On November 16, 2022, the UK government blocked the acquisition of control by Nexperia (a Dutch subsidiary of a Chinese group) over semiconductor manufacturer Newport Wafer Fab under the National Security and Investment Act 2021 (NSIA). Prior to that, the UK government blocked two other transactions: (i) a licensing agreement for the transfer of IP rights concerning AI-related vision sensing technologies (which has the potential to apply to the healthcare industry—e.g. in radiological diagnostics and medical imaging) from the University of Manchester to Chinese firm BIVT (blocked on July 14, 2022) and (ii) the attempted acquisition of Bristol-based software company Pulsic by Hong Kong firm Super Orange HK (blocked on August 17, 2022). More details about the deals in which the UK government has intervened can be found in our recent advisory.

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; non-compliance with the mandatory filing requirement risks significant criminal and civil sanctions. The definitions of the 17 mandatory sectors are broad, as made clear by the UK government under its guidance, and a number of transactions in the med-tech, medical devices and digital health sectors have the potential to be captured. Mandatory sectors that are particularly relevant to digital health include advanced materials, advanced robotics and AI. Based on the NSIA annual report 2022, in the first months of the NSIA's application, AI ranked among the top sectors where mandatory notifications have been made. To read more about the NSIA, including the separate voluntary notification regime, see our Advisory.

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

Ludovica Pizzetti
Counsel
EU/UK

Amanda Cassidy
Sr. Health Policy Advisor
Washington, DC

Emma Elliston
Associate
London

Alison Peters
Associate
Washington, DC

Amsterdam | Brussels | Chicago | Denver | Houston | London | Los Angeles | Newark
New York | San Francisco | Seoul | Shanghai | Silicon Valley | Washington, DC

arnoldporter.com