SPECIAL REPORT

2019 DIGITAL HEALTH YEAR IN REVIEW

January 2020

McDermott Will & Emery

McDermott Will & Emery

SPECIAL REPORT

TABLE OF CONTENTS

McDermott
Will & Emery

INTRODUCTION

Throughout the past year, the healthcare and life science industries experienced a proliferation of digital health innovation that challenged traditional notions of healthcare delivery and payment, as well as product research, development and commercialization, for long-standing and new stakeholders alike. Lawmakers and regulators made meaningful progress towards modernizing the existing legal framework to both protect patients and consumers and encourage continued innovation, but these efforts still lag behind the pace of digital health innovation. As a result, some obstacles, misalignment and ambiguity remain, and 2020 will likely be another year of significant legal and regulatory change.

Read on for a review of key developments that shaped digital health in 2019 and set the groundwork for trends in 2020.

US FOOD & DRUG ADMINISTRATION

Many industry stakeholders embraced and applauded the US Food and Drug Administration's (FDA's) pragmatic efforts in 2019 to create new and expedited market pathways for digital health and innovative technologies.

GUIDANCE ON DIGITAL HEALTH

As discussed in depth here, FDA released six guidance documents in September 2019—five final guidance documents and a re-issued draft guidance document—as part of its continued focus on updating the regulatory stance on software as a medical device and other digital health products. These guidance documents were:

- Clinical Decision Support Software (draft)
- Changes to Existing Medial Software Policies Resulting from Section 3060 of the 21st Century Cures Act (final)
- Policy for Device Software Functions and Mobile Medical Applications (final)
- Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices (final)
- General Wellness: Policy for Low-Risk Devices (final)
- Off-the-Shelf Software Use in Medical Devices (final)

In general, the updated guidance documents reflect the need for a more flexible, risk-based approach to regulation that accommodates a rapidly evolving technological landscape.

On February 5, 2019, FDA released the Principles of Premarket Pathways for Combination Products draft guidance, which provides FDA's current thinking on principles for premarket review of combination products. The draft guidance, discussed in our 2019 FDA Year in Review, is part of FDA's efforts to implement § 3038 of the 21st Century Cures Act. Although the draft guidance does not explicitly reference digital products, former Commissioner Gottlieb previously acknowledged the particular challenges of developing combination products containing digital health technologies and the need to enhance clarity, predictability, efficiency and consistency of premarket review for these and other combination products.

OTHER DIGITAL HEALTH ANNOUNCEMENTS AND DEVELOPMENTS

In April 2019, FDA issued a white paper, Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device, announcing FDA's plans to consider adapting its existing regulatory framework to promote the development of safe and effective medical devices that use advanced AI algorithms. AI, and specifically ML, are "techniques used to design and train software algorithms to learn from and act on data." FDA's proposed approach would allow developers to make modifications to previously-cleared or previously-approved algorithms based on real-world learning and adaptation without requiring a new clearance or approval for the modified product. If finalized as outlined in the white paper, FDA's plans would attempt to better accommodate the iterative nature of AI products while ensuring that FDA's standards for safety and effectiveness are maintained. The white paper is discussed in detail here.

As part of its digital health software precertification program, further described here, FDA sought test cases from software organizations planning to submit a *de novo* request or 510(k) submission for software as a medical device (SaMD) in 2019 or shortly thereafter to meet the goals of its 2019 Test Plan.

In 2020, FDA intends to select precertification program test case participants that best match particular selection qualities, one of which is a company's intention "to submit a De Novo Request or 510(k) submission for a software product that meets

the definition of a device . . . prior to June 2020."

In 2019 FDA also provided lists of prioritized guidance documents (both draft and final) that the Center for Devices and Radiological Health (CDRH) intends to publish in FY 2020, and guidance documents that CDRH intends to publish as guidance development resources permit in FY 2020. Among the prioritized guidance documents, digital-health-related final guidance topics include:

- Safer Technologies Program for Medical Devices
- Clinical Decision Support Software
- Multiple Function Device Products: Policy and Considerations.

Draft guidance topics include:

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- Computer Software Assurance for Manufacturing, Operations, and Quality System Software.

The agency will hold a public workshop, Evolving Role of Artificial Intelligence in Radiological Imaging, on February 25–26, 2020, to discuss emerging applications of "AI in radiological imaging, including devices intended to automate the diagnostic radiology workflow as well as guided image acquisition." Similarly, on March 5, 2020, the agency will hold a public workshop on Medical Extended Reality: Toward Best Practices for Virtual and Augmented Reality in Medicine to discuss evaluation techniques for hardware, standards development, and assessment challenges for applications of Extended Reality (XR) in medicine.

REVISED ADVAMED CODE

In 2019, the Advanced Medical Technology Association (AdvaMed) updated its Code of Ethics on Interactions with U.S. Health Care Professionals. The revised Code went into effect on January 1, 2020, and contains new provisions and revisions to existing language that touch on many common industry activities. Changes include express reference to digital health and software technologies as covered by the Code, and clarifications on topics such as "legitimate need" for consulting services, development of fair market value methodologies, and guardrails around research grants and charitable donations. Changes in the 2020 AdvaMed Code are discussed in detail here.

PRIVACY AND SECURITY

Privacy and cybersecurity continue to be among the most material and prevalent enterprise risks, affecting all healthcare providers and other stakeholders in the digital health space. The finalization of the California Consumer Privacy Act underscores the complex and evolving challenge posed by consumer privacy concerns. As patients and consumers become increasingly sensitized to whether and how their privacy is protected, digital health stakeholders should diligently identify and assess privacy and security risks, and establish, maintain and update privacy and cybersecurity risk management programs that address all relevant laws, regulations and standards in the ever-evolving digital health landscape.

BIOMETRIC PRIVACY UPDATE

Since the passage of the Illinois Biometric Information Privacy Act (BIPA) in 2008, plaintiffs' attorneys have used it aggressively to bring class action lawsuits against companies that use biometric identification technologies. Traditionally, courts dismissed many BIPA suits for failure to allege proof of actual damage or injury. However, on January 25, 2019, in *Rosenbach v. Six Flags Entertainment Corporation et al.*, the Illinois Supreme Court held that a plaintiff need not demonstrate actual injury or harm to receive monetary damages under BIPA.

BIPA generally grants individuals the right to control their biometric information by requiring an organization to obtain individuals' informed written consent before collecting their biometric information. The Illinois Supreme Court determined that failure to adhere to these procedures is not merely a "technical" violation of BIPA, but results in "the right of the individual to maintain her biometric privacy vanish[ing] into thin air." This constitutes a "real and significant" injury that is the "precise harm the Illinois legislature sought to prevent" by enacting BIPA.

The cost of non-compliance with BIPA can be substantial. Private entities are potentially liable for $1,000 per violation in liquidated damages or the amount of actual damages in cases of negligence, and $5,000 per violation in liquidated damages or the amount of actual damages in cases of recklessness or intentional disregard.

In the weeks following the *Rosenbach* decision, dozens of class actions were filed in Illinois state courts, with initially scant guidance from the courts regarding which defenses would be viable post-*Rosenbach*. In March 2019, the Illinois Appellate Court answered one key question: it refused to narrow the *Rosenbach* holding and unequivocally stated that a plaintiff has standing under BIPA even if the only alleged violation relates to the collection of biometric information and not any improper storage or use of biometric information. No further

damages must be alleged, because the statutory violation can result in liquidated damages and penalties under BIPA.

To avoid BIPA lawsuits, organizations using or implementing new biometric technologies should maintain robust programs for compliance with BIPA and other laws regulating the collection and processing of biometric information. In particular, organizations should ensure that they meet the BIPA written informed consent and other requirements, and properly train employees regarding BIPA requirements.

DIVERGENT HIPAA AND CCPA DE-IDENTIFICATION STANDARDS

The California Consumer Privacy Act (CCPA) regulating personal information about California consumers became effective on January 1, 2020. Because the CCPA defines "deidentified data" differently from the de-identification standard under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), CCPA created a potential compliance challenge for digital health companies using or commercializing data de-identified under the HIPAA standard, which dates back to the adoption of the HIPAA Privacy Rule in 2003.

The HIPAA Privacy Rule uses the term "de-identified" to refer to data that is not regulated as protected health information (PHI) for purposes of HIPAA.[1] The CCPA uses the term "deidentified" to refer to data that is no longer regulated as personal information under the CCPA.[2] This different language used in the CCPA creates a risk for HIPAA covered entities and business associates that a data set de-identified under the HIPAA standard would be deemed to include personal information about CCPA consumers under the CCPA. Moreover, the CCPA extends de-identification requirements beyond patients and consumers to encompass those healthcare providers whose personal information may be included in a data set.

[1] See 45 CFR §164.514 for HIPAA's definition of de-identified protected health information.

[2] Under the CCPA, "deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer. For a business to count information it has collected about consumers as "deidentified" under the CCPA, the following criteria must be met: (a) The information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular customer; (b) The business must have implemented technical safeguards and business processes that prohibit re-identification; (c) The business must have implemented business processes to prevent inadvertent release even of the de-identified data; and (d) The business must not make any attempt to re-identify the information. Cal. Civ. Code § 1798.140(h).

A business can take steps to reconcile the HIPAA and CCPA de-identification requirements and mitigate the risk of CCPA exposure when licensing or otherwise disclosing HIPAA de-identified data. These steps include:

- Updating HIPAA expert determinations to address CCPA requirements
- Updating privacy and security policies to reflect the technical and procedural safeguards under the CCPA definition of de-identified data
- Amending data license agreements and other contracts with third parties to prohibit re-identification of California healthcare providers and other California consumers
- Removing identifiers of physicians and other California consumers who served as patients and are identified in the data
- Obtaining documentation from legal counsel to memorialize the legal analysis and safeguards supporting the conclusion that data is de-identified in accordance with the CCPA.

By following these steps, a business may mitigate the risk that it is subject to the notice, "do not sell," opt-out and other requirements of the CCPA.

OTHER HEALTH INFORMATION TECHNOLOGY DEVELOPMENTS

ONC Proposed Rule on Information Blocking

On February 11, 2019, the Office of the National Coordinator for Health Information Technology (ONC) released its long-awaited proposed rule implementing the "information blocking" prohibition of the 21st Century Cures Act. The Cures Act and the ONC proposed rule generally define information blocking as a practice that, except as required by law or covered by an exception, is likely to interfere with, prevent or materially discourage access, exchange or use of electronic health information. The information blocking prohibition regulates four categories of actors:

- Healthcare providers
- Developers of certified health information technology
- Health information exchanges
- Health information networks.

ONC proposed seven exceptions that identify conduct (including pricing practices) that is not prohibited information blocking.

Publication of a final rule is expected in early 2020, and would have a significant impact on data sharing arrangements and other relationships among healthcare providers, health IT developers and other regulated actors.

CMS Proposed Rule to Advance Interoperability

On the same day that the ONC released its proposed rule, the Centers for Medicare & Medicaid Services (CMS) issued a long-awaited proposed rule aimed at enhancing interoperability and increasing patient access to health information. This proposed rule would require CMS-regulated payors and agencies to implement application programming interfaces that allow patient information to be shared more readily between patients, healthcare providers and payors. It would also require hospitals that have adopted electronic health record (EHR) systems to engage in event reporting with community providers and others as a condition of participation in the Medicare program. CMS hopes that the new requirements will allow patients greater access to their health information and improve care coordination between hospitals and other healthcare providers.

If finalized, CMS's proposed rule may require hospitals and payors to make significant investments in their health information technology to comply with the new requirements.

SAMHSA Proposed Rule to Reduce Barriers to Care Coordination

On August 26, 2019, the Substance Abuse and Mental Health Services Administration (SAMHSA) published a long-awaited proposed rule that would modify the federal regulations at 42 CFR Part 2 governing the confidentiality of substance use disorder (SUD) patient records created by federally assisted SUD treatment programs. The SAMHSA proposed rule includes several provisions aimed at reducing barriers to the coordination of care for SUD patients between Part 2 programs and non-Part 2 providers, particularly in today's healthcare delivery system, which increasingly aims to reward providers for effectively managing patient care across multiple care settings, and to penalize providers who fail to do so.

If finalized, the SAMHSA proposed rule is likely to help non-Part 2 providers and recipients of records created by Part 2 programs in certain situations. Non-Part 2 providers will likely benefit from the ability to separately document SUD diagnoses in their own medical records without such records becoming subject to Part 2, and third-party payors may benefit from being able to seek consent from members to disclose Part 2 records to a care coordination entity rather than individual employees of the entity.

Several areas of the SAMHSA proposed rule would benefit from further clarification. For example, it is unclear whether health plans and recipients of records created by Part 2 programs who are not healthcare providers are permitted to create separate records containing SUD information that would not be subject to Part 2.

Stark Law and Anti-Kickback Statute Proposed Rules

On October 17, 2019, the US Department of Health & Human Services (HHS) published proposed rules that would amend existing and create new exceptions to the physician self-referral law (Stark Law) and safe harbors to the Anti-Kickback Statute (AKS), in connection with HHS's Regulatory Sprint to Coordinated Care. Among the many proposals, HHS would amend the exception and safe harbor for EHR items and services, and would create a new exception and safe harbor for donations of certain cybersecurity technology and related services. Please see the Fraud & Abuse section of this Year in Review for a summary of these proposed changes and new exceptions.

HIPAA Enforcement

Last year, the HHS Office for Civil Rights (OCR) continued to vigorously enforce the HIPAA Privacy, Security and Breach Notification Rules against both covered entities and business associates. In 2019, OCR entered into eight HIPAA settlements and imposed civil money penalties on two HIPAA-regulated entities, resulting in approximately $12.27 million in penalties and settlements. This total is less than half of the record-breaking $28.7 million collected by OCR in CY 2018, which was due in significant part to the resolution of OCR's largest HIPAA settlement in history (at $16 million, the settlement was almost three times higher than OCR's previous record). The reduction in OCR's HIPAA enforcement collections from 2018 to 2019 may be explained, in part, by OCR's revised interpretation of the annual civil money penalty limits for multiple violations of the same HIPAA provision during a calendar year set forth in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, which OCR explained in a Notice of Enforcement Discretion in April 2019.

> Regardless, HIPAA covered entities and business associates should expect OCR to aggressively pursue HIPAA enforcement actions.

In its FY 2020 Justification of Estimates for Appropriations Committees, HHS stated:

> The FY 2020 request for the Operations and Resources Division discretionary budget request of $19,738,000 is $7,115,000 below the FY 2019 Enacted level. OCR will offset reductions with the use of settlement funding for health information privacy, security and breach notification enforcement activities. OCR plans to expend $15,647,000 in settlement funding which is $7,480,000 more than the previous year.

The federal government's 2020 fiscal year began on October 1, 2019. Since then, OCR has announced

seven of the 10 enforcement actions the agency took in CY 2019.

Below is a snapshot of noteworthy 2019 OCR enforcement actions:

- OCR launched its Right of Access Initiative, which focuses on enforcing patients' rights under HIPAA to access copies of their medical records. So far, OCR has entered into settlements with two covered entities, each for $85,000, to resolve allegations that they failed to provide individuals with timely access to their PHI. Expect access rights to continue to be a priority area for OCR going forward. Covered entities should ensure that they have processes in place to timely respond to patients' access requests in accordance with OCR's guidance on the Privacy Rule's access provisions.
- A dental practice paid $10,000 to OCR to settle a complaint alleging that the practice impermissibly disclosed PHI when it issued public responses to reviews posted by patients on a prominent social media site without first obtaining the patients' authorizations to do so. This case is the most recent in a series of similar OCR settlements involving public disclosures of limited PHI by providers in response to traditional or social media coverage. Digital health providers and vendors should be mindful of potential HIPAA implications when using social media or other public platforms to engage with patients.
- OCR entered into a $3 million settlement with a covered entity that had reported breaches in 2013 and 2017 resulting from the loss and theft of unencrypted mobile devices storing PHI. OCR found that the covered entity failed to complete an accurate and thorough HIPAA risk analysis, implement device and media controls, and encrypt the mobile devices, even though the covered entity had identified lack of encryption as a high risk when it previously interacted with OCR in 2010. Risk analysis and risk management continue to be priority areas of enforcement focus for OCR. Digital health providers and vendors should not only perform a sufficient HIPAA risk analysis, but also take steps to reduce any identified risks to acceptable levels.
- A hospital system paid $2.175 million to OCR to settle allegations that it failed to properly report a breach to OCR involving the misdirected mailing of 577 affected individuals' PHI. Digital health providers and vendors should assess their procedures for identifying, analyzing and reporting breaches of unsecured PHI in compliance with the HIPAA Breach Notification Rule.
- OCR agreed to a $100,000 settlement with an electronic medical record vendor (a HIPAA business associate), which suffered a breach in 2015 when a cyber-attacker gained access to the PHI of about 3.5 million individuals. OCR found that the business associate had failed to perform a comprehensive, enterprise-wide HIPAA risk analysis before the breach occurred. This settlement underscores that covered entities and business associates alike have found compliance with the HIPAA risk analysis requirement to be challenging. Notably, this OCR settlement preceded the vendor's $900,000 settlement with 12 state attorneys general, which is the first multi-state HIPAA enforcement action by state regulators. As information privacy and data security remained top-of-mind both publicly and for regulators in 2019, state attorneys general continued to supplement OCR's enforcement efforts by flexing their own HIPAA enforcement authority under the HITECH Act.

FRAUD AND ABUSE

In recent years, government oversight and enforcement agencies have increasingly focused their sights on digital health. That trend continued in 2019 with active enforcement involving EHR vendors, telehealth providers and others. However, there were some positive notes, highlighted by the potential relaxation of certain fraud and abuse laws and the release of health technology-related advisory opinions that offered potential pathways forward for emerging technologies.

ENFORCEMENT ACTIONS IN THE EHR SPACE

In 2019, the federal government continued to increase its oversight and enforcement attention on EHR vendors that allegedly misrepresented the capabilities of their software and paid kickbacks to customers. On February 6, 2019, the US Department of Justice (DOJ) announced a settlement with EHR vendor Greenway Health LLC for $57.25 million to resolve allegations that Greenway caused its customers to submit false claims by misrepresenting its software functions during the certification process, miscalculating certain meaningful use measures, and making payments and providing other remuneration to customers for recommending its software to others.

The Greenway settlement was accompanied by a five-year corporate integrity agreement with strict compliance oversight, and came two years after the DOJ's groundbreaking $155 million settlement agreement with eClinicalWorks that set the stage for enforcement actions against EHR vendors. The allegations against eClinicalWorks, which were similar to those raised in the Greenway case, stemmed from a *qui tam* action by a whistleblower. However, DOJ pursued the Greenway case directly, not in response to a relator's allegations.

Expect continued government and relator scrutiny of EHR vendors in 2020. EHR vendors should:

- Take care to accurately and transparently demonstrate their software during HIT certification program testing
- Review and consider improvements to their systems and other procedures for identifying, responding to and correcting software design and quality issues that call into question EHR software's conformity to applicable EHR certification criteria or present patient safety or clinician usability risks
- Review existing customer reference, referral and marketing arrangements for compliance with the AKS.

DOJ ENFORCEMENT ACTIVITY IN THE TELEMEDICINE SPACE

Throughout 2019, DOJ continued its focus on enforcement activity in telemedicine, presumably in response to recent expansion of reimbursement in this evolving field.

In April 2019, DOJ announced charges against 24 defendants, including owners of various telemedicine companies, for their alleged involvement in a healthcare fraud scheme resulting in loss of $1.2 billion. This scheme involved payment of kickbacks and bribes by durable medical equipment companies to medical professionals working with telemedicine companies, in exchange for the referral of Medicare beneficiaries. DOJ alleged that the defendants paid doctors to prescribe medically unnecessary durable

medical equipment without seeing patients or after only a brief telephone conversation.

In July 2019, DOJ prosecuted a New York-based anesthesiologist for her alleged role in a $7 million telemedicine conspiracy to fraudulently bill Medicare, Medicare Part D plans and private insurance plans. Telemedicine-related allegations and convictions also featured prominently in DOJ press releases describing September 2019 healthcare fraud takedown activities coordinated across DOJ, HHS Office of the Inspector General (OIG) and other government agencies, including allegations related to genetic testing activities.

In light of this recent enforcement trend, healthcare companies should exercise extreme caution and consult with experienced regulatory counsel prior to opening telemedicine practices.

PROPOSED CHANGES TO STARK LAW AND AKS REGULATIONS

In October 2019, HHS released its long-awaited proposed changes to the Stark Law, the AKS and the Beneficiary Inducement Civil Monetary Penalty Law (CMPL) regulations in connection with its Regulatory Sprint to Coordinated Care. Several proposals could affect the use of digital health tools directly.

Proposed Modifications to the EHR Exception and Safe Harbor

The existing EHR exception and safe harbor protect certain donations (*i.e.*, licenses and other arrangements for less than the fair market value) of interoperable EHR software or information technology and training services to physicians and other referral sources. By meeting the conditions of the EHR exception and safe harbor, a donor and donation recipient will not violate the Stark Law's referral prohibition or the AKS's prohibition on remuneration to induce referrals of items and services covered by federal healthcare programs. HHS proposes making the following changes to the EHR exception and/or safe harbor:

- Expand the scope of protected donors in the EHR safe harbor to permit donations by entities other than those that submit claims or requests for payment
- Limit or eliminate the requirement in the EHR exception and safe harbor that the donation recipient pay 15% of the donor's cost of donated EHR items and services (in advance of receipt of the items and services)
- Modify the definition of "interoperability" for purposes of the EHR exception and safe harbor, and clarify the related deeming provision

- Modify the prohibition against limiting or restricting the interoperability of donated items or services to explicitly reference the concept of information blocking as defined under the Cures Act in connection with a donation of EHR items and services under the EHR exception and safe harbor.

Depending on which proposals are adopted, the final rules could make the EHR exception and safe harbor less burdensome by removing unnecessary administrative requirements associated with making protected donations.

Additional detail regarding these proposals is available here.

New Cybersecurity Exception and Safe Harbor

HHS proposed to create a new cybersecurity exception and safe harbor in order to help improve the healthcare industry's overall cybersecurity posture by permitting donations to address the growing cyber threat that the industry faces. The proposed cybersecurity exception and safe harbor are broader and include fewer conditions than the EHR exception and safe harbor. If finalized, and depending on which alternative proposals, if any, are adopted, the new cybersecurity exception and safe harbor could provide a useful pathway for potential donors to help protect their own systems through donations to connected recipients. Additional information about the proposed cybersecurity exception and safe harbor is available here.

New CMPL Exception for Telehealth In-Home Dialysis

OIG proposed to create a regulatory exception to the CMPL to permit patients with end-stage renal disease to use telehealth technologies for their in-home dialysis treatment. This proposal would interpret and incorporate the statutory exception originally added by the Bipartisan Budget Act of 2018.

In addition to these digital health-specific proposals, HHS proposed other changes that could create new pathways for arrangements involving digital health tools, including in connection with value based enterprises and related to patient engagement. The deadline for public comments was December 31, 2019. Given the variety of options on the table, comments from the healthcare industry will be important to informing the agencies' final rules. Additional information about HHS's other proposals is available in McDermott's Regulatory Sprint to Coordinated Care Resource Center.

FAVORABLE DIGITAL HEALTH ADVISORY OPINIONS

Through the advisory opinion process, industry stakeholders can seek OIG guidance on the application of certain laws, including the AKS, to proposed and existing arrangements.

If an opinion requestor receives a favorable advisory opinion, the requestor receives prospective immunity under the relevant laws. Advisory opinions serve as a useful resource to help understand how OIG views certain types of arrangements.

In 2019, OIG issued two favorable advisory opinions related to digital health and the use of technology to facilitate care.

In January 2019, OIG published OIG Advisory Opinion No. 19-02, in which it approved a pharmaceutical manufacturer's proposal to implement a program that involved loaning certain limited-functionality smartphones to optimize patients' adherence to a medication protocol. OIG determined that the arrangement meets the "Promotes Access to Care" exception to the prohibition on beneficiary inducements under the CMPL and would pose a low risk of fraud and abuse and, as such, that OIG would not impose sanctions under the AKS.

In September 2019, OIG published OIG Advisory Opinion No. 19-04 in response to a request from an online platform that allows users to search and book medical appointments with healthcare professionals. The requestor proposed an arrangement pursuant to which the requestor would charge healthcare professionals a per-click or per-booking fee in connection with their listing in its directory and would allow certain sponsored advertisements in exchange for per-click or per-booking fees. OIG indicated that it would not impose sanctions on the requestor because the risk for fraud or abuse presented by the proposed arrangement is low.

TRANSACTIONS

On the transactions front, 2019 was another highly active year. Out of the many deal trends in 2019, several stand out as illustrative of trends that will continue into 2020.

PATIENT-FOCUSED SOLUTIONS

In previous years, some of physicians' top complaints related to the paperwork and administrative tasks associated with maintaining EHRs. In 2019, digital health companies responded to this concern with collaborations aimed at using technology to help physicians re-focus on patient care. For example, Nuance Communications announced a partnership and preparation for the 2020 launch of its ambient clinical intelligence product, which leverages AI and ambient sensing technology to record and document each patient encounter, enabling healthcare providers to reduce the distraction of a computer screen during patient visits and the amount of after-hours time dedicated to clinical documentation. As another example, Doctor on Demand also focuses on putting the patient back at the center of a healthcare encounter, and similarly announced a new partnership to enable broader access to its platform.

Providing a technology solution to a technology problem can raise issues, however. Some clinicians

have expressed understandable skepticism about digital health tools, particularly when it comes to patient privacy and potential for error. Digital health companies should carefully consider and have a plan for how their tools use patient data and the associated privacy and security concerns, and should remain cognizant that technology's role is to augment (but not supersede) the judgment of a physician.

DIGITAL THERAPEUTICS

In 2019, transaction activity continued to focus on digital therapeutics—software tools that deliver evidence-based therapeutic interventions to patients to prevent, manage or treat a medical disorder or disease. Notably, three key digital therapeutics players focused on software to treat disease (Click Therapeutics, Pear Therapeutics and Akili Interactive Labs) announced partnerships in the past 12 months. The introduction of new CPT codes in 2019 to enable reimbursement for remote patient monitoring also seemed to encourage a wave of activity for digital therapeutics providers focused on tools that track and manage disease (such as Voluntis and Geneva Healthcare).

Digital therapeutics partnerships can be challenging because they involve collaboration between the technology and life sciences industries. Pharma is highly structured, with numerous detail-driven standard operating procedures, strategically run development and clinical programs, and other mechanisms to deal with the regulatory framework that must be navigated to launch a prescription product. By contrast, the tech industry is designed for rapid response given the shorter development times and fast evolution of technology.

Collaborating across these two industries, while strategic, can be challenging from a cultural and operational standpoint, and raises important concerns, particularly with respect to technology development, intellectual property and data rights, and privacy and security.

Digital therapeutics will remain a focus going forward, but adapting to deal terms and structures to address these concerns will be important as these innovative transactions continue to expand and evolve.

DATA ANALYTICS

The year 2019 saw many digital health companies innovate to improve quality of care and lower healthcare costs, fueled in part by data analytics. Recognizing the need to reduce variations in radiology diagnoses, Wal-Mart partnered with Covera Health to leverage Covera's novel clinical analytics platform,

which analyzes patient scans to direct patients to quality providers and provide physicians with insights to improve their practice, lower variations in scan results, minimize misdiagnoses and reduce healthcare expenditures. In the M&A category, Dassault Systèmes acquired Medidata for $5.8 billion, representing a significant investment by a technology company in the healthcare data analytics and precision medicine space.

DIGITAL HEALTH INVESTMENT

While digital health investments were down in 2019 from a record-breaking 2018, they still continued to be strong. IPO activity in particular was notable, with six companies (including a few in the "health and wellness" category) filing for IPOs. These IPOs revealed two trends:

- The majority of digital health companies with IPOs in 2019 used the tech-heavy NASDAQ exchange, likely seeking to take advantage of lower listing fees (important for unprofitable growth companies living on seed funds), the ability to associate themselves with other high-tech companies, and more relaxed rules for compensation committees and nominating committees.
- IPO performance for companies with high-touch, consumer-centric offerings was particularly strong out of the gate, while healthcare analytics company performance builds at a slower pace.

LOOKING AHEAD: 2020 OUTLOOK FOR DIGITAL HEALTH TRANSACTIONS

The digital therapeutics space likely will continue as an area teeming with opportunity as pharma's interest in the area continues, particularly as the space adapts based on lessons learned from recent high-profile setbacks. Investment in the digital health sector as a whole should continue at or near its current rate, with investors being more disciplined in investing in technology that has a reasonable path to deployment in today's market. Cross-industry deals should continue as well, as companies learn how to align their efforts in the face of cultural and strategic differences. Lastly, data collaborations will continue to proliferate, as companies with vast data resources seek partnerships with companies looking to use data for analytics and development of digital health tools.

CONTRIBUTORS

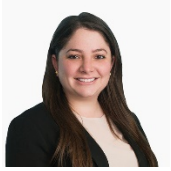
STEPHEN BERNSTEIN
PARTNER
sbernstein@mwe.com
Tel +1 617 535 4062

BERNADETTE BROCCOLO
PARTNER
bbroccolo@mwe.com
Tel +1 312 984 6911

JAMES CANNATTI III
PARTNER
jcannatti@mwe.com
Tel +1 202 756 8866

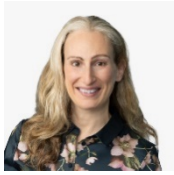
JIAYAN CHEN
PARTNER
jychen@mwe.com
Tel +1 202 756 8722

DALE VAN DEMARK
PARTNER
dcvandemark@mwe.com
Tel +1 202 756 8177



DANA DOMBEY
PARTNER
ddombey@mwe.com
Tel +1 305 329 4453

AMANDA ENYEART
PARTNER
aenyeart@mwe.com
Tel +1 312 984 5488



JENNIFER GEETTER
PARTNER
jgeetter@mwe.com
Tel +1 202 756 8205

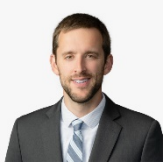
DANIEL GOTTLIEB
PARTNER
dgottlieb@mwe.com
Tel +1 312 984 6471

SARAH HOGAN
PARTNER
shogan@mwe.com
Tel +1 617 535 3911

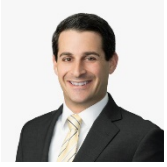
MARSHALL JACKSON, JR.
PARTNER
mjackson@mwe.com
Tel +1 202 756 8019

LISA MAZUR
PARTNER
lmazur@mwe.com
Tel +1 312 984 3275

VERNESSA POLLARD
PARTNER
vpollard@mwe.com
Tel +1 202 756 8181



MICHAEL RYAN
PARTNER
mryan@mwe.com
Tel +1 202 756 8088



SCOTT WEINSTEIN
PARTNER
sweinstein@mwe.com
Tel +1 202 756 8671

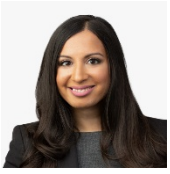
EDWARD ZACHARIAS
PARTNER
ezacharias@mwe.com
Tel +1 617 535 4018

STACEY CALLAGHAN
ASSOCIATE
scallaghan@mwe.com
Tel +1 312 984 2026

ADAM CAMIEL
ASSOCIATE
acamiel@mwe.com
Tel +1 617 535 4058

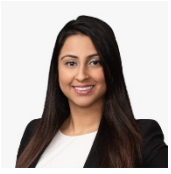
EMMA CHAPMAN
ASSOCIATE
ejchapman@mwe.com
Tel +1 202 756 8423

MATTHEW CIN
ASSOCIATE
mcin@mwe.com
Tel +1 312 984 2099



DEEPALI DODDI
ASSOCIATE
ddoddi@mwe.com
Tel +1 312 984 3265

ELESE HANSON
ASSOCIATE
ehanson@mwe.com
Tel +1 312 984 3686



GUGAN KAUR
ASSOCIATE
gkaur@mwe.com
Tel +1 202 756 8890

ANISA MOHANTY
ASSOCIATE
amohanty@mwe.com
Tel +1 202 756 8286

NICOLE SANDLER
ASSOCIATE
nsandler@mwe.com
Tel +1 305 329 4487

McDermott
Will & Emery

mwe.com |