2022 Law And Policy Highlights In Digital Health Care

By **Allison Shuren, Mahnu Davar and Raqiyyah Pippins** (December 22, 2022)

Allison Shuren

Mahnu Davar

Raqiyyah Pippins

The SARS-CoV-2 public health emergency ushered in an urgent reliance on and consumer desire for virtual health care delivery, as well as extraordinary investment in technology to enable broader capabilities to monitor and diagnose patients remotely.

While 2021 saw record investment in and acquisitions of virtual and digital health assets resulting in the deployment of capital approaching $60 billion,[1] the pace of investment and volume of transactions during 2022 slowed to almost half of that amount. This is predominately in response to a bevy of macroeconomic factors including inflation, rising interest rates and fears of a recession.

The health information technology, telehealth and mental health technology subsectors received the largest funding.[2] Mental health, oncology and cardiovascular care were the top three therapeutic areas[3] garnering investor interest in 2022.

There appears to be sufficient momentum as we enter 2023 from health care providers, payors, patients and life science companies to find new ways to engage virtually to continue attracting health care-focused investors. Increasing regulatory clarity as to the state of virtual care after the public health emergency will be a key factor.

Food and Drug Administration

In 2022, the U.S. Food and Drug Administration made good on several agency commitments in the Digital Health Innovation Plan, and new legislation has set the stage for promising new opportunities for innovative technology developers.

The FDA's apparent narrowing of the parameters of its enforcement discretion for patient-focused clinical decision support software is one of the most notable updates of the year. Also notable was the change in leadership at the Center for Devices and Radiological Health's Digital Health Center of Excellence.

Further, the agency announced that it intends to withdraw its COVID-19-related enforcement discretion policies either 180 days after the termination of the public health emergency declaration or 180 days after a prior point in time that FDA determines is appropriate, whichever occurs first.

Digital health product developers relying on FDA enforcement discretion policies should take time to understand these developments and prepare regulatory engagement strategies to ensure their products remain in compliance. A summary of this year's material updates follows.

On Sept. 28, the FDA issued its clinical decision support software guidance,[4] finalizing the 2019 draft guidance governing the regulation of clinical decision support and software as medical devices. The guidance provides further clarity as to how the FDA intends to

interpret the four 21st Century Cures Act clinical decision support exemption criteria.

Other edits suggest that FDA intends to take a more expansive view of clinical decision support software functions subject to agency oversight by eliminating the enforcement discretion policy for certain low-risk patient and caregiver device clinical decision support functions described in the draft guidance.

The FDA also issued a policy for device software functions and mobile medical applications guidance,[5] which specifies the types of software functions, including mobile medical application software functions, that the FDA intends to regulate as devices actively. The FDA also released a revised medical device data systems, medical image storage devices and medical image communications device guidance,[6] updating the 2019 final version.

While it was reported early this year that the FDA had ended its software precertification pilot program, in September the FDA issued a report[7] with findings from the now completed pilot.

The FDA established the program in 2017 to explore an innovative total product lifecycle for regulatory oversight of software as a medical device. The FDA's ability to implement the program flexibly as originally intended was stymied by a lack of sufficient legislative authority and limited participation from the industry.

However, the findings from the pilot could be useful to inform a future software regulatory framework, particularly regarding good manufacturing practice and quality systems regulation requirements.

In September, President Joe Biden signed the FDA User Fee Reauthorization Act of 2022, which included the sixth reauthorization of the Prescription Drug User Fee Act. The FDA's PDUFA VII commitment letter[8] includes a commitment to enhancing the use of digital health technologies to support drug development, review and regulatory decision-making.

In October, the FDA updated its webpage on artificial intelligence- and machine learning-enabled medical devices webpage to include 178 additional AI- and machine learning-based devices. The webpage identifies FDA-cleared, approved or authorized medical devices that incorporate artificial intelligence or machine learning marketed in the U.S.

Federal Trade Commission Developments

Key areas of focus for the Federal Trade Commission in 2022 have been dark patterns, endorsements and consumer reviews, as well as privacy and security.

Dark Patterns

On Sept. 15, FTC staff published a report[9] highlighting design practices in digital media that the staff consider reflecting dark patterns.

According to the FTC staff report, dark patterns are "deceptive design practices that trick or manipulate" consumers into making choices, such as buying goods or services or giving up their privacy, and which cause consumer harm.

While the strategies highlighted in the report are not per se violation of the FTC Act, the agency's concern in this area is reflected in its investigation[10] into Cerebral Inc., a subscription-based mental health startup, regarding the use of negative option programs

that purportedly made it difficult for consumers to cancel subscriptions for the company's health services.

The FTC's concept of dark patterns extends beyond subscription programs, implicating practices such as the use of endorsements without disclosing material connections, promoting apps as free when they contain in-app purchases, and the use of ambiguous language, i.e., double negatives, to steer a consumer's choice. Thus, any company engaged in digital health should consider the FTC staff report on dark patterns.

Endorsements, Including Consumer Reviews

The FTC also is scrutinizing the use of endorsements and consumer reviews across industries, including health care. The agency has issued proposed revisions to its endorsement guides,[11] announced plans to similarly update its .com disclosures[12] guidance to businesses on digital advertising and brought several actions against companies' use of fake reviews to promote their products.

Notably, the agency's amended endorsement guides, provide nine examples involving medical doctors or promotion of drug products, indicating the FTC's particular concern over the use of endorsers in health product advertising.

Thus, any digital health promotional strategy should be vetted in the context of the FTC's enforcement related to use of endorsements, testimonials and consumer reviews, including whether such strategies meet the legal requirements concerning disclosure of material connections, typicality and claim support.

Privacy and Cybersecurity

Data sets generated through digital and virtual health care encounters are valuable assets, but the collection of such information carries the risk of scrutiny, enforcement and litigation, particularly when security safeguards fail and lead to a loss of or unauthorized access to health data.

This year the FTC filed multiple lawsuits, issued warnings to the industry[13] and commenced broad rulemaking[14] aimed at protecting consumer data, effectively broadening a breach notification rule related to health information not covered by Health Insurance Portability and Accountability Act.

Notably, FTC has taken notice of companies alleged to have misused consumers' health information. For instance, the FTC recently filed an action[15] against data broker Kochava Inc. for selling geolocation data that makes it possible to obtain consumers' personal health information, and settled[16] a lawsuit against Flo Health Inc., a period-tracking app alleged to have disclosed its users' sensitive health information to third parties.

The FDA showed its increased focus on cybersecurity this year. In November, the FDA, through the MITRE Corp., created an incident response preparedness and response playbook[17] to help all relevant stakeholders, including hospitals, medical device manufactures and other health care delivery organizations, and it updated its draft guidance[18] on cybersecurity in medical devices for premarket submissions.

State attorneys general have similarly focused on the privacy and security of health data. As an example, the California attorney general settled an investigation against Glow Inc., for failing to secure health data and for providing health information without notice and

consent. At the same time, several states, including California, Colorado, Connecticut, Utah and Virginia, either enacted or revised comprehensive state privacy laws in 2022.

Given the relatively narrow scope of HIPAA, digital and virtual health initiatives may have significant compliance obligations arising from state laws, including with respect to data obtained from many digital health apps, connected medical devices and software as a medical device.

The obligations can include managing a consent-based regime where patients may be required to give consent to process data, as well as compliance obligations to ensure appropriate notice of data practices and affording rights to users to access and delete their data, as well as withdraw consent, among others.

Congress also signaled its interest in digital health and related privacy with the introduction of several bills introduced in 2022 that could foreshadow things to come in the 118th Congress. These include the following.

The Health Data Use and Privacy Commission Act

This is a bipartisan bill sponsored by soon-to-be U.S. Senate Health, Education, Labor and Pensions Committee ranking member Bill Cassidy, R-La., and Sen. Tammy Baldwin, D-Wis. The bill would establish a temporary commission to study existing health data privacy protections, the benefits of sharing this information and recommendations for federal legislation.

The Healthcare Cybersecurity Act

Sponsored by Cassidy and Sen. Jacky Rosen, D-Nev., this bill would require additional coordination between the Cybersecurity and Infrastructure Security Agency and the U.S. Department of Health and Human Services.

Along similar lines, Sen. Mark Warner, D-Va., chairman of the Senate Intelligence Committee, released a white paper[19] this fall outlining a range of health-related cybersecurity policy options, though he has yet to turn those proposals into legislative text.

The American Data Privacy and Protection Act

Led by U.S. House of Representatives Energy and Commerce Committee leaders Frank Pallone, D-N.J., and Cathy McMorris Rodgers, R-Wash., this is a broad privacy bill that would set new federal privacy standards for companies, nonprofits and other entities. This bill would cover health data held by non-HIPAA-covered entities, such as technology companies.

Medicare Reimbursement

Regulatory flexibilities established at the beginning of the pandemic to improve Medicare beneficiary access to telehealth and remote monitoring services remain in place, but the Centers for Medicare and Medicaid Services has signaled that providers should start planning for the end of the public health emergency.

For telehealth, waivers that eliminated restrictions on coverage of telehealth services based on the site of service and location where a service originated will sunset in accordance with the Consolidated Appropriations Act of 2022,[20] 151 days after the end of the public health

emergency.

Medicare also will no longer cover audio-only visits for physical health encounters but will continue to reimburse for the furnishing of audio-only mental and behavioral health care furnished to Medicare beneficiaries in their homes, provided certain conditions are met. There also will be continued coverage of video-based mental health visits for federally qualified health centers and rural health clinics.[21]

As demonstrated through the dozens of bills introduced in the 117th Congress,[22] there is bipartisan support for virtual care that is expected to be carried over into the next Congress. The incoming House Republican majority outlined some of those priorities through the Healthy Future Task Force, a 17-member panel led by Reps. Brett Guthrie, R-Ky., and Vern Buchanan, R-Fla.

The task force's modernization subcommittee[23] expressed additional support for telehealth, patient data-sharing standards that prioritize privacy and security, and the interoperability of electronic health records.

There also were meaningful payment changes in 2022. New current procedural terminology codes — 98975-77 and 98980, 98981 — for remote therapeutic monitoring for certain conditions took effect in January.

While Medicare covers remote monitoring services, Medicaid programs have been slower to do so. Four states — Massachusetts, Kentucky, Hawaii and West Virginia — added coverage in 2022, but 16 states and Washington, D.C., still do not cover remote patient monitoring, according to the Center for Connected Health Policy.

CMS also created a new code, A9291, for prescription digital cognitive or behavioral therapy. While the existence of this code may make it easier for commercial payors to process claims for prescription digital therapeutics, to date.

CMS has held fast to its position that there is no Medicare benefit category allowing coverage of this service. The Access to Prescription Digital Therapeutics Act,[24] introduced in early 2022, would have addressed this limitation.

Much work remains for Medicare to fully integrate software as a medical device and artificial intelligence into the physician fee schedule payment methodology. Today software is considered an indirect cost under the physician fee schedule, and it is not well-captured in the rates for an individual service.

Moreover, while CMS recognizes that use of software-as-a-medical device and AI are changing how some physician services are delivered, the agency has yet to take any definitive actions to address payment for these innovations. CMS again solicited comment on these issues in rulemaking during 2022, but there is no clear timetable for any specific payment proposals.

Fraud, Abuse and Waste

Not all the news surrounding virtual care has been positive in 2022.

With a surge in the utilization of telemedicine during the public health emergency, U.S. enforcement agents continued their health care enforcement and oversight efforts in 2022, including a multiagency criminal, civil and regulatory focus on fraud and abuse related to

telehealth services.

On July 20, the U.S. Department of Justice announced[25] a nationwide coordinated law enforcement action focused on telemedicine, clinical laboratory and durable medical equipment fraud — including charges against 36 defendants in 13 federal districts across the U.S. for more than $1.2 billion in alleged health care-related fraud.

By August, the DOJ's coordinated effort included 49 defendants, and there have several additional cases reported in the last half of 2022.

In particular, the DOJ has been targeting alleged schemes involving the payment of kickbacks by laboratories and marketers in exchange for the referral of patients by health care professionals working with fraudulent telemedicine and digital medical technology companies.

Among the defining features of many of the DOJ's recent telemedicine actions are the alleged lack of legitimate provider-patient relations, often with limited to no patient interaction, and indifference to medical necessity, and arrangements involving clinical and genetic laboratory diagnostic companies.

On the same day as the DOJ announcement in July, HHS' Office of Inspector General also issued a special fraud alert[26] highlighting the growth and prevalence of fraudulent and suspect arrangements within telemedicine and telehealth — mirroring in large part the DOJ's focus on sham arrangements where providers had limited, if any, interaction with patients and without regard to medical necessity, as well as other hallmarks and indicators of potential sham virtual care.

In September, the HHS-OIG determined[27] that the billing of 1,714 providers for telehealth services during the first year of the pandemic poses a high risk to Medicare, indicating that telemedicine appears poised to draw increased regulatory scrutiny as well. The U.S. Government Accountability Office and MedPAC also noted the need to better assess the quality of care furnished through telehealth, particularly audio-only services.

The special fraud alert, continued criminal and civil enforcement actions and increased regulatory scrutiny strongly suggest that the DOJ and HHS will remain focused on telemedicine and telehealth in 2023.

Conclusion

We close 2022 anticipating what new innovations in virtual care 2023 will bring and the quality of care improvement that may be achieved, as well as braced for another faced paced year full of legal and policy initiatives.

Allison Shuren is a partner and co-chair of the life sciences and health care regulatory practice at Arnold & Porter.

Mahnu Davar is a partner at the firm.

Raqiyyah Pippins is a partner and co-leader of the firm's consumer products practice group and consumer products and retail industry team.

Partners Christopher Anderson and Jami Vibbert, senior associate Bobby McMillin, associate Michael Wood, and senior health policy adviser Amanda Cassidy contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.cbinsights.com/reports/CB-Insights_Digital-Health-Report-Q3-2022.pdf?.

[2] https://www.cbinsights.com/reports/CB-Insights_Digital-Health-Report-Q3-2022.pdf?.

[3] https://rockhealth.com/insights/q3-2022-digital-health-funding-the-market-isnt-the-same-as-it-was/.

[4] https://www.fda.gov/media/109618/download.

[5] https://www.fda.gov/media/80958/download.

[6] https://www.fda.gov/media/88572/download.

[7] https://www.fda.gov/media/161815/download.

[8] https://www.fda.gov/media/151712/download.

[9] https://www.ftc.gov/system/files/ftc_gov/pdf/P214800 Dark Patterns Report 9.14.2022 - FINAL.pdf.

[10] https://www.wsj.com/articles/ftc-launches-probe-of-cerebrals-business-practices-11655241983.

[11] https://www.ftc.gov/system/files/ftc_gov/pdf/P204500 Guides Concerning-Endors-and-Testimonials.pdf.

[12] https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-looks-modernize-its-guidance-preventing-digital-deception.

[13] https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

[14] https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[15] https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

[16] https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about.

[17] https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response.

[18] https://www.fda.gov/regulatory-information/search-fda-guidance-

documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions.

[19] https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf.

[20] https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117HR2471SA-RCP-117-35.pdf.

[21] https://www.cms.gov/medicare/medicare-fee-for-service-payment/physicianfeesched.

[22] See, for example, American Telemedicine Association's Federal legislation tracker at https://app.hubspot.com/documents/5096139/view/112649529?accessId=79b988.

[23] https://republicanleader.house.gov/wp-content/uploads/2022/06/HFTF-Modernization.pdf.

[24] https://www.capito.senate.gov/imo/media/doc/03-10-2022%20Digital%20Therapeutics%20Bill.pdf.

[25] https://www.justice.gov/opa/pr/justice-department-charges-dozens-12-billion-health-care-fraud.

[26] https://oig.hhs.gov/documents/root/1045/sfa-telefraud.pdf.

[27] https://oig.hhs.gov/oei/reports/OEI-02-20-00720.asp.