DIGITAL HEALTH
Telehealth | Health IT | AI

SheppardMullin

Top 5 Legal Issues in Digital Health to Watch for in 2022

By: Allison Fulton, John Carroll, Sara Shanti, Julia Kadish, Erica Kraus and Matt Shatzkes

The use of digital health to deliver healthcare has seen unprecedented growth over the past few years, with significant acceleration due to the COVID-19 Public Health Emergency (PHE). As patients seek ways to empower themselves and take more control of their health and well-being, this demand is being met by flexible and innovative tools and technologies. The latest health technology advancements in diagnostics, treatment, and ongoing patient management have the potential to improve health and disease outcomes more than ever before. Companies in this industry have also raised a record-setting amount of capital, particularly during the PHE.

Like many other segments that go through rapid growth and innovation, the industry faces a complex and shifting set of laws and regulations. While many temporary waivers and policies during the PHE created an ecosystem allowing companies to flourish, companies in this space should begin to expect heightened scrutiny from various regulators as we turn the page to 2022.

In this article, we highlight some of the key legal considerations that the digital health industry can expect in the coming year from the perspective of: (1) telehealth related laws and regulations, (2) FDA, (3) privacy and cybersecurity, (4) fraud and abuse, and (5) antitrust issues. As companies look ahead to allocate legal and compliance resources and think about risk mitigation strategies, this article showcases those areas where we expect to see further developments or regulator attention this year.

Telehealth

In response to the PHE, the federal and state regulatory landscape swiftly created a makeshift of temporary waivers, executive orders and regulations, to expand access to telehealth services, but leaving providers and patients uncertain about, among other things, scope of practice issues (e.g., licensure) and reimbursement for these services. With many of these federal and state flexibilities tied to the PHE set to expire, providers offering telehealth services, regardless of the modality or specialty, will need to continue to be aware of and track the status of certain flexibilities implemented

in response to the PHE. For example, the Centers for Medicare & Medicaid Services (CMS) released the Calendar Year (CY) 2022 Medicare Physician Fee Schedule (PFS) final rule (Final Rule), which extended or made permanent a number of PHE related changes (e.g., permanently removing geographic originating site restrictions on telehealth services used for purposes of diagnosis, evaluation, or treatment of mental health disorders). Also at the federal level, there is still no guidance on whether the "dormant" Ryan Haight Act, which, absent limited exceptions, prevented the prescription of controlled substances via telehealth without first conducting an in-person examination, will be enforced following the expiration of the PHE.

Likewise, on the state side, there have been a number of actions making permanent changes expanding access to telehealth services. This includes removing restrictions on the delivery of telehealth via certain modalities (e.g., audio-only telephone, e-mail, text message) and addressing insurance parity coverage of telehealth services. While these examples suggest a positive trend towards increased access to telehealth and making telehealth a permanent and critical part of the healthcare delivery system, other states have rolled back certain of the flexibilities implemented in response to the PHE. All of these matters will significantly impact the way providers and patients continue to utilize telehealth services, and will impact scope of practice, mode of practice and reimbursement matters going forward.

FDA

Companies developing software medical devices, whether in the wellness or in the therapeutic and diagnostic spaces, should continue to monitor FDA's developing approaches to regulating digital health. In late 2021, FDA published multiple resources for companies developing medical devices that incorporate software with Artificial Intelligence and Machine Learning (AI/ML) functions. These documents, including "GMLP for Medical Device Development: Guiding Principles" (27 Oct 2021), "List of AI/ML-Enabled Medical Devices," (22 Sep 2021), and FDA Guidance "Content of Premarket Submissions for Device Software Functions" (04 Nov 2021), demonstrate the Agency's efforts to be transparent with industry on its expectations as it develops a framework for reviewing and approving AI/ML technology. The newly minted FDA Digital Health Center of Excellence promises to foster high-quality digital health and innovative regulatory approaches in 2022 (and the coming years). While the Agency is still developing these approaches, companies seeking clearance or approval of digital health devices with AI/ML should consider engaging FDA in premarket submission meetings to understand the Agency's expectations for clinical data and software performance data. We also expect the FDA to finalize its draft guidance on Clinical Decision Support (CDS) software before the close of the year. CDS software provides healthcare professionals and patients with intelligently filtered knowledge, coupled with person-specific information, to inform healthcare options. The finalized CDS guidance will provide companies developing CDS with some clarity on whether, and to what extent, their product may be regulated in 2022 and beyond. We also expect FDA to continue to partner with its international counterparts to harmonize the regulation of digital health products.

Privacy and Cybersecurity

HIPAA became somewhat of a social media star during the PHE, with individuals attempting to use the law to protect more than the protected health information within its purview. HHS/OCR offered guidance to help entities share public health information, manage drive-through testing and vaccination sites, and resolve telehealth hurdles. Enforcement in 2022, however, will continue to be focused on entities taking action to prepare for and reduce ransomware and other attacks, including through the performance of risk analyses of electronic infrastructure and ensuring individuals' access to their information, including interoperability standards.

HIPAA's stardom has accelerated the appetite for the industry to offer HIPAA compliance as a "best practice," whether or not any entity falls under HIPAA's legal jurisdiction. While such practices may be admirable, entities should proceed with caution to ensure actions and representations do not overreach contractual terms or create grounds for unfair and deceptive claims under federal and state laws. HIPAA's mainstream persona has also helped push the discussion of a federal privacy law, and the states' impatience with that idea stalling.

Therefore, even where HIPAA may not apply to certain business models, the ever-growing patchwork of state and federal privacy and data security laws creates a confusing sea of requirements. Throughout 2021, the FTC continued to flex its muscles in this space sending a clear message of its intent to more closely scrutinize companies collecting health information that sit outside HHS/OCR's reach. Companies are continuing to grapple with the new and broad interpretations in the FTC's policy statement about the Health Breach Notification Rule released in the Fall of 2021. Namely, how to comply with the comments around sharing of "covered information" subject to an individual's authorization and what will be considered a "breach" under this law. This year, companies will also want to be mindful of the forthcoming "comprehensive" state privacy laws coming into effect in 2023 in Virginia and Colorado and the expansion of California's existing law. With conflicting exemptions across these state laws for entities that may be regulated by HIPAA, and newly introduced "consent" requirements for the collection of "sensitive" information, digital health companies will likely have steps in the coming months to prepare for these laws. Finally, sophisticated cyber threat actors continue to find ways to attack even the most prepared companies, particularly due to the value of health-related information. This reinforces the importance of having cyber insurance – though the market has become increasingly costly for these policies with more detailed diligence from carriers to obtain coverage.

Fraud and Abuse

During the COVID-19 pandemic, the use of digital health tools and solutions has accelerated due to necessity and to temporary waivers and flexibilities granted by HHS in response to the PHE. Enforcement response to this uptick has been mixed. For instance, the HHS Office of Inspector General ("OIG") issued a policy statement to notify physicians and other practitioners that they will not be subject to administrative sanctions for reducing or waiving any cost sharing obligations incurred for telehealth services furnished consistent with applicable coverage and payment rules during the PHE. However, though OIG recognizes the benefits that digital health technologies have for improving care coordination and health outcomes, it has also announced "significant oversight work" assessing telehealth services during the PHE. Specifically, OIG is currently conducting *eight* reviews related to the use of telehealth services. Many of the OIG audits focus on compliance with Medicare and Medicaid requirements for documenting and billing home health services - in a sense, traditional billing and coding audits applied to telehealth services.

The government has also pursued fraud and kickback allegations related to telehealth. For instance, in October 2020, DOJ announced Operation Rubber Stamp, a nationwide enforcement action involving criminal charges against 345 defendants across 51 federal districts, including more than 100 doctors, nurses and other licensed medical professionals, mostly related to schemes involving telemedicine. In addition to these criminal charges, the investigation resulted in CMS' revocation of the Medicare billing privileges of more than 250 additional Medical professionals, a record-breaking number of administrative actions. Beyond audit activity related to compliance with coding and documentation rules, providers can expect the government's continued focused attention on the use of digital health technologies in ways that it believes may result in excess costs to the government and in patient harm.

Antitrust

Digital health companies may find themselves increasingly in the antitrust enforcement cross-hairs, as they are at the center of the two most frequently targeted industries: healthcare and technology. In recent years, the FTC has devoted more resources to investigating and challenging conduct by healthcare providers than any other industry (even tech), and the DOJ has ramped up its efforts in the sector as well. Both agencies have aggressive new leaders in place – FTC Chair Lina Khan and DOJ Assistant Attorney General Jonathan Kanter – who are coordinating on a number of enforcement priorities and who recently characterized corporate concentration as a "crisis" for the American economy. Chief among the agencies' focus is a growing concern about whether transactions involving upstart digital health companies may be chilling competition. As digital health companies consider transactions, including joint ventures, they should carefully analyze potential antitrust issues, even if those deals do not involve direct competitors.

Looking Ahead

The digital health ecosystem being created by new entrants and healthcare industry incumbents re-inventing themselves will continue to evolve from fixed solutions to a more widespread overhaul of the healthcare system. These digital tools and products changing the infrastructure supporting the delivery of healthcare will be matched by increased regulatory scrutiny, as law and policy try to keep pace with technology to ensure patient safety and treatment efficacy.

For More Information, Please Contact:

Allison Fulton (FDA)
Partner | Washington, D.C.
202.747.2195
afulton@sheppardmullin.com

bio

John Carroll (Antitrust)
Partner | Washington, D.C.
202.747.1951
jcarroll@sheppardmullin.com

bio

Sara Shanti (Privacy & Cybersecurity)
Partner | Chicago
312.499.6358
sshanti@sheppardmullin.com

bio

Julia Kadish (Privacy & Cybersecurity)
Associate | Chicago
312.499.6334
jkadish@sheppardmullin.com

bio

Erica Kraus (Fraud & Abuse)
Associate | Washington, D.C.
202.747.2645
ekraus@sheppardmullin.com

bio

Matt Shatzkes (Telehealth)
Former Sheppard Mullin Partner;
now Chief Legal Officer and
General Counsel at Aditxt, Inc.