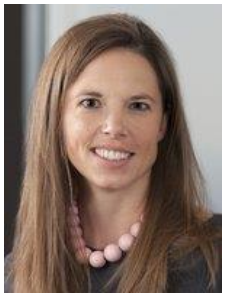
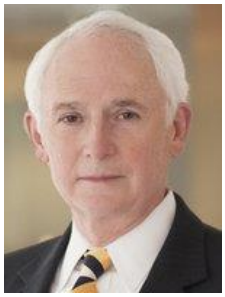
The Legal Implications Of Mobile Health Advancements

By **Sarah Rathke, Kristin Bryan and John Wyand** (November 5, 2020)



Sarah Rathke

Kristin Bryan



John Wyand

Health care has been among the last industries to go remote, in part due to concerns about fully evaluating patient diagnostics, and in part due to data privacy and patient confidentiality concerns, a condition precedent for receiving medical treatment and advice has traditionally been physically going to the doctor.

This is changing.

Both the World Health Organization[1] and the National Institutes of Health[2] have adopted definitions of "mobile health," meaning, essentially, the use of wireless devices to inform health care decisions.

Conceptually, mobile health could become to human health care the analogue of what automotive computers are to vehicles — diagnostic tools that allow continual and contemporaneous monitoring of the functioning and performance of the system.

As such, mobile health has the potential to improve health status though early detection of health problems, promote personalized medicine, reduce frontline health care provider workloads, expand access to medical care into underserved areas, and with the promise of reducing overall health care system costs.

Even before March, health care and technology experts predicted that mobile health was on the verge of rapid expansion. Peter Diamandis and Steven Kotler's 2020 book, "The Future Is Faster Than You Think" — published, notably, before the pandemic — contains this vivid and memorable passage:

> On a wintery Wednesday in January 2026, you're being watched. Carefully watched. Technically, you're asleep in your bed, but Google's home assistant knows your schedule. Thanks to your Oura ring, it also knows you've just completed a REM cycle and are now entering Stage 1 sleep – making it the perfect time to wake you up.
>
> A gentle increase in the room's lighting simulates the sunrise, while optimized light wavelengths maximize wakefulness and improve mood. By the time you've gone through your bathroom rituals – toilet, toothbrush, etc. – you realize mood isn't the problem. It's that tightness in your joints, the chill in your bones ...
>
> "Your microbiome looks perfect," Google tells you. "Also, blood glucose levels are good, vitamin levels fine, but an increased core temperature and IgE levels ... You've got a virus."

But now COVID-19 has rapidly accelerated the timeline for this change in the health care diagnostic supply chain. Since the start of the pandemic, the U.S. Centers for Medicare & Medicaid Services has issued what it calls an "unprecedented array of temporary regulatory waivers and new rules to equip the American healthcare system with maximum

flexibility"[3] to respond to the pandemic.

These include allowing health care providers to provide more primary care services using telecommunications technology, with the express understanding that this allowance "may result in changes to the frequency or types of in-person visits."

The U.S. Department of Health and Human Services' Office for Civil Rights mirrored this approach by announcing that it would exercise its enforcement discretion and not impose penalties for noncompliance with regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 against covered health care providers "in connection with the good faith provision of telehealth"[4] during the pandemic. Undoubtedly, these developments are just the beginning.

This brave new world is not without legal implications and risks, however.

First, mobile health will expand upon the myriad ways companies use biometric data for commercial purposes. Biometric information encompasses unique identifiers such as retina scans, fingerprints, DNA, voice recognition and facial-geometry recognition, among others.

Although protected under the Health Insurance Portability and Accountability Act when it is part of an individual's medical records, there is currently no other federal law regulating the collection and disclosure of biometric information, notwithstanding that Sens. Jeff Merkley, D-Ore., and Bernie Sanders, I-Vt., proposed the National Biometric Information Privacy Act earlier this year.[5]

Additionally, several states have statutes that regulate the use of biometric technologies. The California Consumer Privacy Act defines biometric information broadly as "an individual's physiological, biological, or behavioral characteristics, including [DNA], that can be used ... to establish individual identity."[6]

This includes "keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."[7]

The Illinois Biometric Information Privacy Act is another example. While many biometric laws are enforced by state attorneys general, some have private rights of action. In addition to HIPAA, entities using mobile health will have to ensure that their practices conform to the patchwork of state biometric laws to minimize litigation and regulatory risk.

Second, mobile health also implicates significant cybersecurity concerns. In 2019, the health care sector was the most frequent target of hackers.[8] This trend has persisted in 2020.

Just last week, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Agency, the Federal Bureau of Investigation and U.S. Department of Health and Human Services issued a joint alert regarding an "increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[9] Entities operating in the mobile health space should anticipate that they will receive similar attention from cybercriminals.

To counter this threat, it will be critical that providers of mobile health services have appropriate safeguards to secure individuals' information to protect against unauthorized access, destruction, use, modification or disclosure of data. Failure to invest in technical and physical safeguards could be cataclysmic.

Just as implantable medical devices have security vulnerabilities that if exploited could put

an individual's health in jeopardy,[10] as former Vice President Dick Cheney famously had the wireless signal in his pacemaker turned off to eliminate the risk of hacking, the same concern would apply equally to devices involved with the provision of mobile health.

Third, mobile health will also likely revolutionize health care research and treatment for substance use disorders. The development of mobile health technologies will enable scientists and physicians to collect real-time streams of information concerning an individual's biology, cognitive state and behavior. The dynamic nature of this information has the potential to operate as a transformative force in health care research.

Similarly, mobile health data could be utilized to report and prompt immediate changes in individual behavior to reduce health risks — particularly in the area of substance use disorders. However, HIPAA governs the privacy of personal health information and other federal regulations apply to health care research and the treatment of substance use disorders. As such, privacy and security concerns are intertwined with future developments in this area.

Sarah Rathke is a partner, Kristin Bryan is a senior associate and John Wyand is a senior partner at Squire Patton Boggs LLP.

[1] https://www.who.int/goe/publications/goe_mhealth_web.pdf.

[2] https://grants.nih.gov/grants/guide/pa-files/PAR-14-028.html.

[3] https://www.cms.gov/files/document/covid-home-health-agencies.pdf.

[4] https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

[5] https://www.congress.gov/bill/116th-congress/senate-bill/4400/text.

[6] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.140.

[7] Id.

[8] https://healthitsecurity.com/news/health-sector-most-targeted-by-hackers-breach-costs-rise-to-17.76b#:~:text=However%2C%20attacks%20targeting%20this%20sensitive,to%2037%20percent%20of%20attacks.&text=Medical%20records%20were%20the%20second,comprising%2039%20percent%20of%20breaches.

[9] https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

[10] https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities.