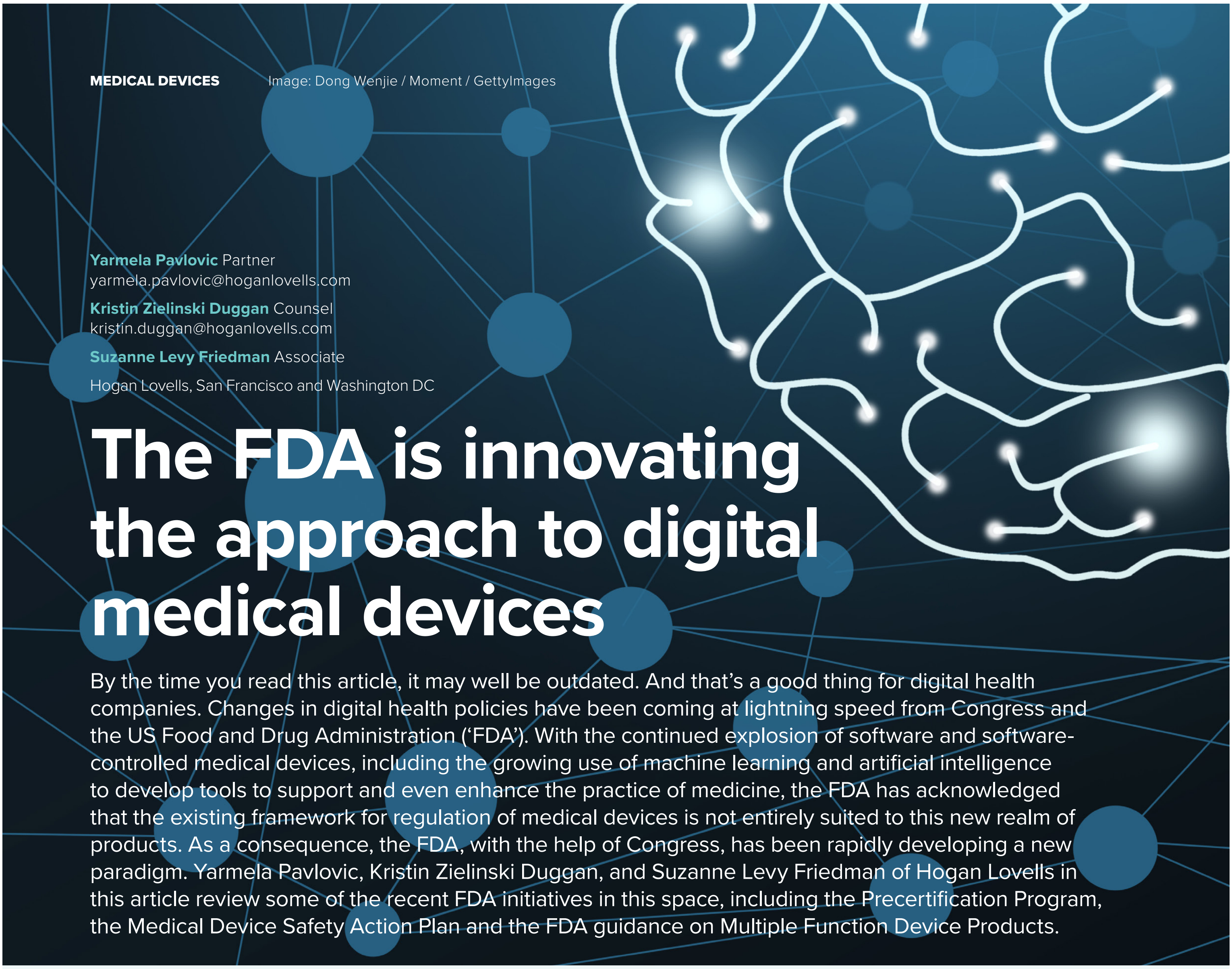

Image: Dong Wenjie / Moment / GettyImages

Yarmela Pavlovic Partner
yarmela.pavlovic@hoganlovells.com

Kristin Zielinski Duggan Counsel
kristin.duggan@hoganlovells.com

Suzanne Levy Friedman Associate

Hogan Lovells, San Francisco and Washington DC

The FDA is innovating the approach to digital medical devices

By the time you read this article, it may well be outdated. And that's a good thing for digital health companies. Changes in digital health policies have been coming at lightning speed from Congress and the US Food and Drug Administration ('FDA'). With the continued explosion of software and software-controlled medical devices, including the growing use of machine learning and artificial intelligence to develop tools to support and even enhance the practice of medicine, the FDA has acknowledged that the existing framework for regulation of medical devices is not entirely suited to this new realm of products. As a consequence, the FDA, with the help of Congress, has been rapidly developing a new paradigm. Yarmela Pavlovic, Kristin Zielinski Duggan, and Suzanne Levy Friedman of Hogan Lovells in this article review some of the recent FDA initiatives in this space, including the Precertification Program, the Medical Device Safety Action Plan and the FDA guidance on Multiple Function Device Products.

Summary of recent initiatives

The Precertification Program

The Software Precertification (Pre-Cert) Program represents potentially the most dramatic shift in the FDA's paradigm for digital health products. Pre-Cert Program development, which began in early 2017, is currently focused only on software as a medical device ('SaMD'), but the Agency has indicated that it may ultimately encompass hardware products as well. The Program shifts the review from being predominantly product focused (e.g., is the product sufficiently safe and effective) to focusing more holistically on the culture and practices of the manufacturer. Once finalised, it would provide a pathway for certification of companies who meet certain design, development and production excellence metrics. After certification, a company would be granted either an exemption from, or a streamlined, US pre-market review for future software products that are subject to FDA regulation[1].

In the winter of 2017/2018, the FDA engaged in a 'pilot' Program with nine participants to further educate the Agency regarding the approaches that existing companies use to ensure that they are producing quality products. That pilot was followed by a public workshop in early 2018. On 27 April 2018, the FDA released a working model reflecting the Agency's vision for the Pre-Cert Program, outlining its most critical components, and including a number of "challenge questions" on areas in which the FDA is still seeking input from stakeholders to further refine the Program. The working model was further updated in June 2018 to v0.2 based on stakeholder comments to date[2].

As currently proposed, the Program would be built on trust in organisations that have demonstrated a culture of quality and organisational excellence to develop high quality products and a commitment to monitoring real world performance, and will leverage transparency of an organisation's excellence and its product's performance across the entire lifecycle. There are four key components to the Pre-Cert Program: (1) excellence appraisal and pre-certification, (2) review pathway determination, (3) streamlined pre-market review, and (4) real world performance, i.e., post-market surveillance and feedback.

The Agency envisions launching a new phase of the pilot Program this autumn, followed by a full "PreCert 1.0" by the end of 2018. While many of the details are still evolving, the emerging framework is a much needed response to the limitations presented by applying traditional medical device approaches to digital health and software products. The FDA has stated that it continues to evaluate whether new statutory authority is needed to implement the Program or whether its existing authority suffices.

The Medical Device Safety Action Plan

In mid-April, the FDA released a Medical Device Safety Action Plan (the 'Plan')[3] to re-emphasise its mission to simultaneously protect patients and bolster access to products that are safer, more effective, and address unmet medical needs. The Plan encourages innovation specifically to improve

continued

safety, detect risks earlier, and keep doctors and patients better informed.

Notably, the Plan highlights the FDA's increasing focus on cyber security. In announcing the Plan, FDA Commissioner Dr Scott Gottlieb emphasised the importance of cyber security in ensuring patient safety. The Plan recognises that the increased interconnectedness of medical devices of all types can lead to safer, more effective technologies, but also introduces increased potential for security breaches and exploitation of device vulnerabilities. To that end, the FDA plans to require medical device manufacturers to incorporate cyber security into their products, and to provide related software information and data (1) to the FDA in their 510(k), De Novo, and PMA submissions, to enable appropriate assessment of cyber security capability as part of the pre-market review process, and (2) to customers through a Software Bill of Materials, to make users aware of potential vulnerabilities and help better manage networked assets.

The Plan requested additional authority and budget allocation to address these and related issues. Subsequently, the House of Representatives voted on the 2019 budget appropriation for the FDA, authorising additional funds for these efforts and requesting that the FDA produce a report in 120 days of the Bill's passage outlining a path forward.

In addition, the FDA intends to update its pre-market guidance on medical device cyber security[4] to better protect against both moderate risks (i.e., those that could disrupt clinical operations and/or delay patient care) and major risks (i.e., those that exploit a vulnerability to enable a remote, multi-patient, catastrophic attack). This appears to be in part a reaction to the significant ransomware cyber attacks that occurred in 2017 involving WannaCry and Petya/NotPetya. In the post-market sphere, the FDA will consider requiring firms to adopt policies and procedures for coordinated disclosure of cyber security vulnerabilities as they are identified. This would supplement the expectations set forth in the FDA's existing guidance documents, Postmarket Management of Cybersecurity in Medical Devices (Dec. 2016)[5] and Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (May 2005)[6], adherence to which is strongly recommended but not legally binding.

In conjunction, the FDA has proposed the development of a CyberMed Safety (Expert) Analysis Board ('CYMSAB') to complement existing resources and address the unmet need for a holistic, multi-disciplinary approach in this area. The CYMSAB would be a public-private partnership comprised of individuals from government, private industry, and academia with a broad range of expertise to assess and validate high-risk/high-impact device vulnerabilities and incidents. The new board would also adjudicate disputes, assess proposed mitigations, advise entities on how to properly disclose vulnerabilities under the new requirements intended to be established, and investigate suspected or confirmed device compromises at the request of either a manufacturer or the FDA. This may be a further development of a more informal response team approach that the FDA has been using over the past year or so.

FDA guidance on Multiple Function Device Products

Consistent with the effort to reduce regulatory burden, on 27 April 2018, the FDA released the draft document Multiple Function Device Products: Policy and Considerations, addressing the Agency's regulatory approach to medical devices that include both regulated and unregulated functions. Documenting the Agency's existing informal policy and building on changes enacted by the 21st Century Cures Act ('Cures Act'), this guidance clarifies that unregulated functions are not the focus of the FDA's review and oversight (i.e., incorporating a regulated functionality into an existing unregulated product does not necessarily make the entire product regulated).

Section 520(o)(2) of the FD&C Act, added by the Cures Act, explicitly directed that otherwise unregulated software functions would not become regulated solely because they are included in a product with a regulated function. Consistent with existing FDA policy, the draft guidance broadens the scope of the policy to all multiple function products (not just software products) that contain at least one device function. It also treats product functions which may be 510(k)-exempt or subject to enforcement discretion in a similar way as non-device functions (collectively referred to as 'other functions'). For such 'other functions,' the FDA will focus on any impact on the medical device function under review, as determined by the company. In general, the guidance is consistent with how the FDA has been treating multiple function products for several years and is expected to encourage less variation in this approach between review groups.

Conclusions

In the fast paced world of software development, waiting six months for FDA clearance of a new software version is not practical; and active regulation of the rapidly growing number of software products would be impossible for the FDA given existing resources. As a result, Congress and the FDA are actively developing a nimble approach to regulation of digital health by reinventing the product approval process for software via the Pre-Cert Program, as well as continuing to clarify the scope of FDA review. The FDA has already accomplished many of its goals for this area signaled in the Digital Health Innovation Action Plan[7] issued last summer. The FDA's ongoing re-assessment and clarification of how it regulates software used in healthcare presents notable opportunities for industry.

[1] Once an organisation demonstrates excellence in all five excellence principles, it would be assigned to one of two levels of pre-certification depending on its level of maturity (practical experience).

[2] https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/UCM611103.pdf?utm_campaign=Update%20on%20Software%20Precertification%20Pilot%20Program%3A%20FDA%20seeks%20public%20input&utm_medium=email&utm_source=Eloqua&elqTrackId=e1c7064ae5a74b18ad1f1f7eb2743760&elq=a6108fc2d73d431885277d321d49ed5b&elqaid=3959&elqat=1&elqCampaignId=3082

[3] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm604672.htm

[4] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

[5] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[6] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM077823.pdf

[7] https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf