



EU and US Regulatory Challenges Facing AI Health Care Innovator Firms

By Suzan Slijpen, Mauritz Kop & I. Glenn Cohen

1. Introduction: A Fragmented AI in Healthcare Regulatory Landscape

In the past few years, we have witnessed a surge in artificial intelligence-related research and diagnostics in the medical field. It is possible that in some fields of medicine in the future AI tools used in diagnostics will generally perform far better than a human clinician. Prime examples of this can be found in radiology, particularly in the detection -and even the prediction- of malignant tumors.

Although the actual development of a clinically usable, deployable deep-learning algorithm is a challenge in and of itself, we have moved from an early period where there was not enough guidance as to ethical and other issues to [an era where many guidelines have proliferated](#). While one might ordinarily say “let a thousand flowers bloom,” the fact that they partially overlap, sometimes diverge, and are often written at different levels of generality make it difficult for well-meaning companies to keep up. This is specifically the case for innovative firms who aim to bring their product into the European market.

2. Cross-sectoral EU laws

First and foremost, the product as a whole must comply with the Medical Device Regulation (MDR) and the specific norms incorporated therein, as well as with GDPR requirements and ESG considerations, just to name a few. On top of that a firm will -in the near future- need to comply with all the [specific requirements for ‘high risk’ AI technology](#) as stipulated in the [Proposal for a Regulatory Framework for Artificial Intelligence](#) (EU AI Act), and navigate its way through the future [European Health Data Space](#). All these regulations and frameworks have an overlapping scope, but take a different approach to what ‘[compliant AI-powered technology](#)’ means and how it must be achieved in practice. With every introduction of legislation, guidelines and best practices are developed that are meant to further elaborate on the logic behind legislative terminology, the rationale of codified norms, and proportionality, subsidiarity, and consistency with existing policy provisions. Often, these guidelines contain ethical considerations as well. And then there are the private initiatives, such as quality management schemes, which become increasingly important for sectoral standardization on top of existing legislation.

Beyond the health care sector-specific Medical Devices Regulation (EU) 2017/745 (MDR) and the In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (IVDR), this mix of AI & Data related regulatory requirements stems from a series of generalized, [cross-sectoral EU laws of the last 5 years](#). Chasing its North Star of establishing a Europe fit for the digital age, the European Commission’s Digital Strategy introduced a sweeping array of Directives and Regulations, including the AI Act, the AI Liability Directive, the Cybersecurity Resilience Act, the Network and Information Security (NIS2) Directive, the ePrivacy Regulation, the Digital Services Act, and the Digital Markets Act. On top of that comprehensive rulebook, the European Data Strategy bundle of laws encompasses the EU General Data Protection Regulation (GDPR), the Free Flow of Non-Personal Data Regulation, the Data Governance Act and the Data Act, as part of the EC’s ambition to establish a single unified market for



data. The latest scion to the [EU legislative tree](#) is the draft regulation on the European Health Data Space ecosystem, as part of the European Cloud Strategy.

Although the cross-sectoral AI legislation that is now introduced by the European Commission's Digital Strategy aims to [be integrated with existing sectoral legislation](#) such as the MDR, the IVDR and the Machinery Directive, it is uncertain how overlapping regulatory compliance requirements for AI-driven medical devices will be managed in practice.

3. Sectoral US Laws

In the U.S., AI regulation has, for the most part, been sectoral rather than cross-sectoral. The main federal health privacy law, the [Health Insurance Portability and Accountability Act of 1996](#) (HIPAA) applies only to "covered entities" like health insurers, claims-processing clearinghouses, and health care providers and their business associates, and only to a subset of protected health care information. It provides several rules for sharing information and exceptions keyed directly to the realities of the health care setting, such as permitting information sharing for treatment, payment, or health care operations, some public health situations, and if certain identifiers have been stripped from the data set. In a similar vein, FDA only considers medical AI that falls in one of its [existing regulatory categories](#) (most often medical device), and even then by way of Congressional action and FDA's own interpretation of its authority, and its discretion only regulates a subset of [medical AI](#).

The sectorialism of the U.S. approach has pluses and minuses. In the [privacy space](#), it is sometimes argued that it is a distinct advantage of the European cross-sectoral approach that it governs beyond the boundaries of traditional health care, and is thus better able to operate in spaces that are adjacent to the traditional encounter with a physician, such as health data garnered from wearables, internet searches, etc. But there is a downside to cross-sectoral regulation as well, in that it may not always take into account the economic realities of different sectors (such as some of the regulatory costs of getting drug approval) or the fact that there may be existing legal structures in that sector that already are doing some of the work – medicine has overlapping rules about licensure, malpractice, etc., that may not be true for dating apps, to give one example.

A different example has to do with how the U.S. FDA has struggled with how to regulate adaptive rather than locked algorithms. The fundamental difficulty is that it is desirable that algorithms be able to learn "out in the world" as they are deployed in different contexts, but it is challenging to determine when have they changed enough that [regulatory re-review](#) is needed. The [agency's 2023 guidance](#) on predetermined change control plans represents a sophisticated way to work with industry in a bespoke way rather than imposing one-size-fits-all criteria. Of course, the devil is in the details when it comes to implementation, but the guidance does represent the kind of creative, interactive, and iterative approach we would like to see more of in the AI regulatory field.

4. Additional Challenges for AI Health care Innovator Firms

A different challenge for AI health care innovator firms pertains to the materials used to build physical devices, especially in the quantum/AI space. These include export, import, and trade controls on algorithms, chips, and rare earths, [fragile supply chains](#), potential dual use, intellectual property protection, and national & economic safety and security concerns.



Another challenge has to do with the tempo of change and how well that fits the current mold of health innovators. The rise of generative AI is an example par excellence. The EU AI Act was the result of a long set of negotiations that seemed to be coming to a consensus just as the disruptive scope of [generative AI systems like Open AI's ChatGPT](#) became most apparent. The result has been disagreement as to [how to regulate these foundational models under the Act](#), as well as questions on [to what extent different foundational models comply with the Act](#).

Relatedly, AI in health care is a fast moving target. General, all-encompassing, civil law-inspired regulations such as the AI Act to ensure AI is developed and used in trustworthy and responsible ways are bound to become quickly obsolete or even bizarre. The world is transitioning with exponential speed from pretrained applied and generative AI models, to reinforcement and transfer learning-based interactive, multimodal AI models that do not need labeled data corpora, nor human feedback, nor training, testing, and validation datasets to properly function. Regulators must be aware of this increasing tempo of innovation and make an effort to truly understand this disruptive technology, to avoid lagging behind.

5. Best of Both Worlds: A Mixed Horizontal-Vertical Approach

Compared to the EU, the historic US permissionless, *ad libitum* innovation approach is pragmatic, agile, iterative, surgical, problem based, yet fragmented and [often viewed as insufficient](#), especially with regard to the promises and pitfalls of [AI in health care](#). But it does have the advantage of allowing innovation more easily. Some argue that the GDPR and the AI in Europe Act have a chilling effect on fragile startups and scaleups, reducing the chances of creating EU-origin health care innovator unicorn firms. A critic might say the U.S. approach means too much fragmentation and free enterprise, while the EU approach is overly precautionary, in legal, ethical, and socio-economic terms.

What the sector needs is regulation that is sensible (with a focus on patient safety and sound technology), practical (easy to understand and implement), and tailored to the specific needs of the sector. The economic realities, such as the costs of clinical trials, and existing legal structures, such as production and market licenses, are different from other industries/sectors and need to be taken into account by regulators. If this is not done correctly on either side of the transatlantic spectrum, regulation is rendered useless and ineffective quickly, either by lack of specificity or by failure to address the regulatory topics that truly matter. In order to create a regulatory environment that truly benefits both innovator firms and patients, we suggest mixing the best of both precautionary and permissionless innovation worlds into a workable middle ground tailored to the specifics of AI & quantum-driven innovation in health care.

* * *

<https://blog.petrieflom.law.harvard.edu/2024/04/04/eu-and-us-regulatory-challenges-facing-ai-health-care-innovator-firms/>

Slijpen is an attorney in the Netherlands; Kop is the Founder and Executive Director of the Stanford Center for Responsible Quantum Technology, and a Stanford Law School TTLF Fellow; Cohen is a professor at Harvard Law School where he directs Harvard Law School's Petrie-Flom Center.



THE PETRIE-FLOM CENTER
FOR HEALTH LAW POLICY, BIOTECHNOLOGY,
AND BIOETHICS AT HARVARD LAW SCHOOL