Ref. Ares(2020)3357399 - 26/06/2020

A White Paper on Artificial Intelligence. EURORDIS additional remarks and considerations

1. General comments about the White Paper on Artificial Intelligence

Being aware of the ground-breaking advantages that technological innovation can offer in the area of rare diseases, EURORDIS welcomes the White Paper on Artificial Intelligence. AI technologies have the ability to integrate and analyse data from different sources that can be used to overcome rare disease challenges (e.g., low diagnostic rates, reduced number of patients, geographical dispersion, and so on).[1]

Given the fast pace in which developments in the area of artificial intelligence happen, the European Commission is proposing the revision of **the Coordinated Plan**, as many of the actions described there have either taken place or are outdated. EURORDIS strongly supports this need, especially as many of the examples that are given have an impact on the area of health. Nevertheless, building on past experiences, we urge the Commission to engage stakeholders and especially patient organisations in the development of these plans. The results that are aimed for through the various policy initiatives and funding programmes should meet the needs of patients and be prioritised accordingly. We regret that none of the options provided by the Commission's consultation explicitly mention the importance of civil society in identifying the areas where the focus should lie.

Although the idea of "**excellence and testing centres**", seem promising, further clarity is needed on the scope of them. Given EURORDIS' experience with European Reference Networks in the area of research in the area of rare diseases, we feel that there are many elements we could contribute to improving the design of those centres. As mentioned, more clarity is when it comes to their scope, the overseeing institution, the way in which they will function, etc.

The White Paper mentions a **Public Private Partnership on AI**. In the area of health, the Innovative Medicines Initiative (IMI) has provided tremendous results, but also a lot of lessons learnt that could be implemented in a similar way in IMI. First and foremost, we regret that patients, as the target of all benefits coming out IMI, are still not included in either the management board, or virtually any other governance structure.

The proposed follow up of the IMI, the European Partnership for innovative health will focus on "blending health digital technologies", which raises the question of overlap between the two initiatives. Given the existence of this initiate dedicated to health, EURORDIS calls for health research to be prioritised under the European Partnership for innovative health programme rather than the creation of a new cross-sectoral PPP, as this will allow for the specificities of the healthcare sector to be better addressed.

We welcome the Commission's approach to **regulating certain aspects relating to the application of AI in the area of health**. Although we see great potential in the use of technologies for better understand the various diseases and developing therapies (especially in the area of rare diseases which is characterised by urgent needs), any solutions applied to the healthcare sector entail

[1] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6947640/

particular risks, that need to mitigated by robust legislation. In developing this legislation, special attention should be given to the wishes and needs of patients. In this context, and given the technical nature of the topic, we call upon the Commission to support patient organisations to provide input into the consultation phase of the legislation by allowing sufficient time, and considering alternative ways of engaging with stakeholders (like workshops, and focus groups).

One of the elements mentioned in the White Paper relates to **liability** and the way that it should be addressed to "actors who is are best placed to address any potential risks". In almost all situations, patients are either the final end user of healthcare applications or the ones experiencing the benefits coming out of used technologies. At the same time, they are also the ones experiencing the possible shortcomings of the use of innovations, including AI. What we call for is clarity and not an ad hoc system where the liability might lie anywhere within the chain of actors contributing to the development and deployment of new AI solutions. This will provide patients with clarity and confidence on who they can hold accountable.

Lastly, we call more clarity regarding the propose the governance structure proposed. We remind the importance of engaging civil society organisations in the governance and we call a balanced approach in engaging cross-cutting and sector-specific organisations.

COMMENTS ON AN ECOSYSTEM OF TRUST

1. Adjusting existing sectoral and horizontal legislation to cover gaps rather than adopting new legislation for AI systems

Whilst we acknowledge that there may be gaps in the current regulatory framework, notably as the WP identifies in the areas of traceability, transparency and human oversight, introducing new horizontal EU legislation on AI could be detrimental for the healthcare sector that is already governed by a very complex EU regulatory framework integrated by sector-specific and horizontal regulations.

At a time when the healthcare sector is still struggling to implement the Medical Device Regulation and the GDPR, introducing a new legislative has the risk of adding a layer of complexity, create inconsistencies between the different rules and uncertainty for users, patients and companies.

For this specific sector, the option of covering these gaps by updating, adjusting and modifying where needed existing horizontal and vertical legal instruments, would possibly be less disruptive and render the regulatory framework fit for purpose.

2. Scope of the future AI regulatory framework – High-risk approach.

The approach seems sensible to guarantee proportionality and avoid an excessive burden on SMEs. However, for the healthcare sector this approach does not seem to bring such a benefit and it does have one important drawback.

It will not alleviate the burden for SMEs given that the vast majority of AI systems developed to be used in the healthcare sector will be considered high risk according to the definition included in the White Paper (the sector and the intended uses will most of the times involve significant risks).

At the same time, having clear criteria to define whether or not a certain product or service should be considered high risk has proven to be very challenging in the past. It has taken the Classification and Borderline Expert Group 3 years to update the MDR guidance for borderline classification (Borderline manual - May 2019, v1.22), including guidance on the rules to determine what software qualifies as a

medical device and falls under the scope of the MDR. It remains to be seen if the working group has managed to create a clear set of rules, but we have received reports from companies in the digital health sector that are still unclear as to whether their products fall under the scope of the MDR.

There are good reasons to believe that any rules and criteria to draw a line between low and high-risk AI systems will raise similar challenges and uncertainty.

3. Compliance and Enforcement

The White Paper correctly identifies effective application and enforcement of new rules on AI as a risk. In fact, there is already a major problem with the application and enforcement of the data protection legislative framework especially when it comes to mHealth apps. Several security and privacy analysis of mobile health applications performed over the years have consistently shown[2] that companies are failing to implement current data protection rules. It appears that substantial resources are needed to guarantee the enforcement not only of an eventual future AI legislative framework, but more generally to ensure that health IT companies, big and small, comply with the current legislative framework, and that national authorities can European authorities can investigate and identify breaches.

4. Support SMEs on compliance

Regardless of whether the Commission decides to develop new legislation or to adjust existing instruments, we would encourage the allocation of sufficient resources to develop tools and resources to limit the burden on SMEs. As it stands today, the EU healthcare regulatory environment is already complex enough and represents an important competitive disadvantage for SMEs working in digital health as they lack the resources and capacities to ensure compliance. Poor compliance and continuous breaches undermine trust, is a major concern for patients' safety and privacy and discourages healthcare professionals from using digital technologies to support the provision of care.

5. Voluntary Labelling for non-high risk AI applications

As already explained, it is problematic to draw a clear line between high and low risk AI systems. Also some of these systems may evolve from low to high risk, as the system learns or the company adds new features. Keeping the assessment scheme robust and dynamic enough to respond to the pace of

---

[2] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas and C. Patsakis, "Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice," in *IEEE Access*, vol. 6, pp. 9390-9403, 2018, doi: 10.1109/ACCESS.2018.2799522.

Tobias Dehling et al., "Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android," JMIR MHealth and UHealth 3, no. 1 (2015): 1–26, https://doi.org/10.2196 /mhealth.3672.

Soumitra S. Bhuyan et al., "Privacy and Security Issues in Mobile Health: Current Research and Future Directions," Health Policy and Technology, January 2017, https://doi.org/10.1016/j.hlpt.2017.01 .004;

Borja Martínez-Pérez, Isabel de la Torre-Díez, and Miguel LópezCoronado, "Privacy and Security in Mobile Health Apps: A Review and Recommendations," Journal of Medical Systems 39, no. 1 (2015), https://doi .org/10.1007/s10916-014-0181-3. 51.

Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," Open Effect, 2016, https://openeffect.ca/fitness-trackers.

Sarah R. Blenner et al., "Privacy Policies of Android Diabetes Apps and Sharing of Health Information," JAMA 315, no. 10 (2016): 1051–52, https://doi.org/10 .1001/jama.2015.19426

innovation and up to date will be costly. Voluntary self-regulation has not seemed to work for mHealth apps and privacy, so we would suggest allocating these resources to guarantee that all, high and low-risk AI applications, comply with the mandatory legal requirements imposed by the sector-specific and horizontal legislative instruments.