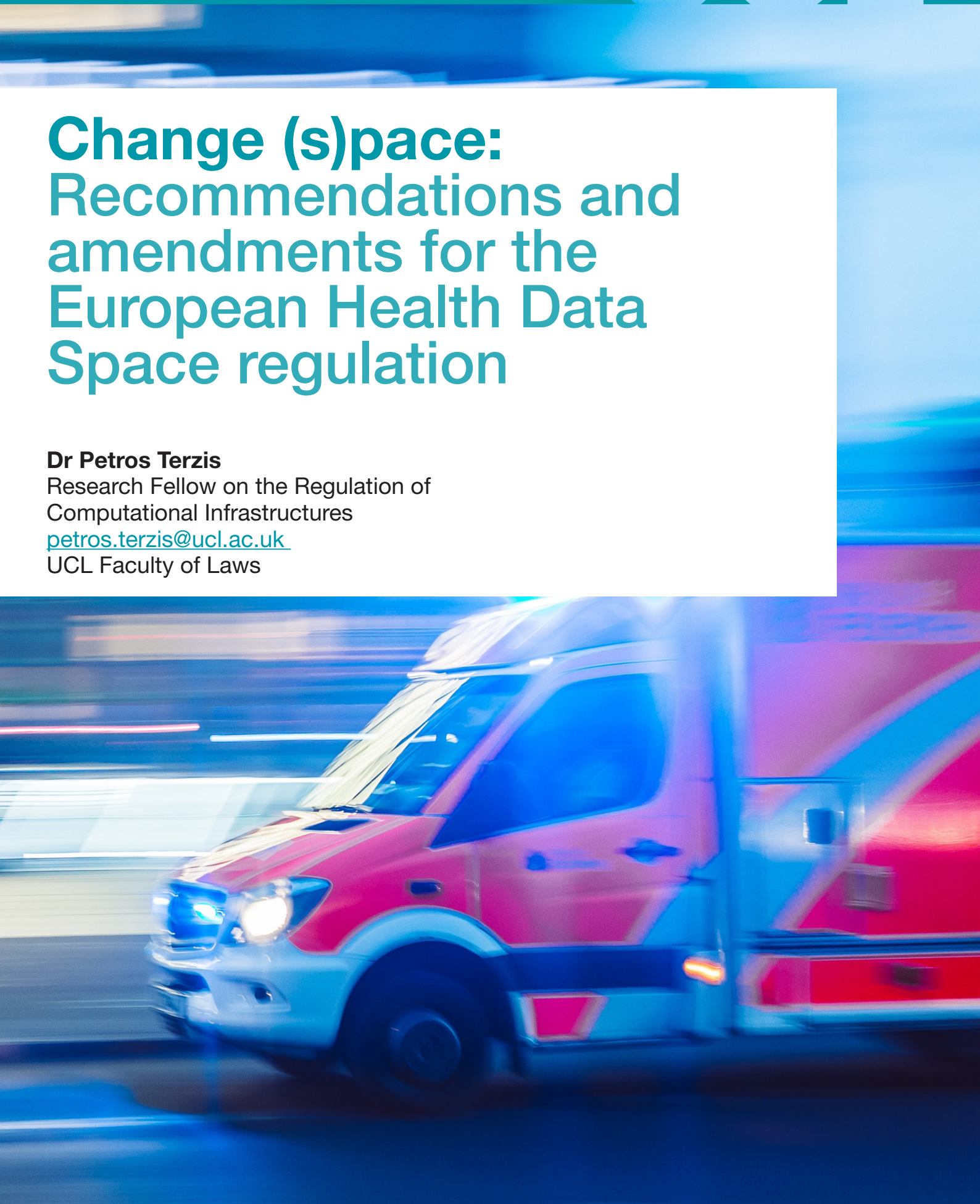
FACULTY OF LAWS

UCL

Change (s)pace: Recommendations and amendments for the European Health Data Space regulation

Dr Petros Terzis
Research Fellow on the Regulation of Computational Infrastructures
petros.terzis@ucl.ac.uk
UCL Faculty of Laws



Introduction

The European Health Data Space (EHDS) initiative represents the first sector-specific legislation for the governance and administration of sensitive data (in this case electronic health data) in the European Union.

It aims at *'empowering individuals through increased digital access to and control of their electronic personal health data*' **(primary use of data)** and *'providing a consistent, trustworthy and efficient set-up for the use of health data for research, innovation, policy-making and regulatory activities'* **(secondary use of data)**. As such, the proposal supplements - and in some cases supersedes – relevant legislation on data protection and governance, namely the General Data Protection Regulation (GDPR), the Data Act, and the Data Governance Act. Fundamentally, what differentiates the EHDS proposal from its closest legislative relatives, is that the former creates legal rights (for example, accessing health data for secondary use) over what, under the previous regimes, used to be mere possibilities to be dealt with under certain criteria.

However, getting the legal framework right is challenging and requires caution due to the scale of the enterprise and the sensitive nature of the data in question. The institutional mechanisms that will result from the EHDS are likely to remain in place for generations as the standard for governance of health data in the European Union. For this reason, policymakers should resist the Siren song of administrative efficiency that data (and its interoperability) promises even at the expense of lengthier legal, political, and technical discussions.

This policy brief examines core aspects of the EHDS proposal (the Proposal), offering recommendations for centring the legislative and parliamentary debate on the rights of individuals and the collective value of public health.

At the time of writing, deliberations are ongoing in search of compromises among the members of the joint committee (LIBE-ENVI). The committee is expected to vote on a draft report in July.

Problems and Challenges

Summary

- Despite its central significance, the issue of privacy and data protection is scarcely mentioned in the interoperability chapter of the EHDS proposal
- Despite their importance for data protection within inter-organisational data flows, the issues of user authorisation (i.e. who will be authorised to access what information across systems) and audit of logs (who accesses what information) are insufficiently addressed by the Proposal's specifications
- Data exchange driven by the formal laws and informal norms of the doctor–patient relationship is transformed into an ill-defined landscape where information is circulated among and across systems without patients' knowledge, let alone implicit or explicit consent
- The Proposal's provisions for the secondary use of health data merit further consideration, since they risk disregarding fundamental pillars of data protection for the sake of administrative efficiency
- The broad definition of electronic health data coupled with the overly permissive approach to the entities that can request access to electronic health data, as well as the list of AI-related reasons that may justify such access, risk creating a backdoor to troves of individuals' health data

The EHDS proposal has two pillars. The first deals with the issue of interoperability of Electronic Health Records (EHR) systems and wellness applications, while the second establishes the conditions for the re-use of health data (secondary use of health data) by interested parties (data users) for reasons different from those that justified the collection of the health data in the first place. In both cases, the quest for administrative efficiency means privacy compromises.

Interoperability and data protection have a peculiar relationship and the case of health data is no different. Fundamentally, interoperability brings efficiency and inter-organisational alignment, but at the same time, it engenders privacy risks, since access to (health) data becomes more comprehensive and longitudinal (Rothstein and Tovino, 2019; Bincoletto, 2020). But we should not assume that this relationship is zero-sum. Privacy protections can enable interoperability while respecting the privacy of the individuals. For example, the DP-3T team demonstrated during the Covid-19 pandemic that one can build an interoperable infectious disease exposure notification system without necessarily compromising people's privacy (Troncoso et al., 2020).

Despite its central significance, the issue of privacy and data protection is scarcely mentioned in the interoperability chapter of the EHDS proposal, despite featuring prominently in an earlier recommendation by the European Commission (Terzis and Echeverria, 2023).

Meanwhile, despite their importance for data protection within inter-organisational data flows, the issues of user authorisation (i.e. who will be authorised to access what information across systems) and audit of logs (who accesses what information) are insufficiently addressed by the Proposal's specifications. Viewed alongside the provisions for the voluntary labelling of wellness applications, these omissions become even more troubling, since Art. 31 enables developers of wellness applications to achieve interoperability with EHR systems through a self-declaratory labelling scheme that would feed EHR systems with new (sources of) data (e.g. data on wellbeing and lifestyle generated by smartwatches and IoT (Internet of Things) devices). As a result, what used to be a data exchange driven by the formal laws and informal norms of the doctor–patient relationship risks becoming a hazy landscape where information is circulated among and across systems without patients' knowledge, let alone implicit or explicit consent.

Likewise, the Proposal's provisions for the secondary use of health data merit significant caution and further consideration. Fundamental pillars of data protection, such as consent and transparency, are disregarded for the sake of administrative efficiency (European Data Protection Supervisor [EDPS], 2020). This is not necessarily surprising, since the EHDS proposal aims to facilitate exchange of data and scientific research by dispensing with the high transaction costs of the consent requirement.

However, achieving an equal status of protection to that of consent is not a simple matter and the EHDS proposal fails in meeting the standards set by the GDPR (EDPS, 2020). The broad definition of electronic health data set out in Art. 33 coupled with the overly permissive approach to the entities that can request access to electronic health data (Art. 33(3) and Art. 47), as well as the list of AI-related reasons that may justify such access (particularly, Art. 34 (f-h)), risk creating a backdoor to troves of individuals' health data (Terzis, 2020). This is because entities (not necessarily

healthcare entities) will be able to apply for access to health data for reasons such as 'algorithmic testing' merely by submitting an application that will be judged on its administrative and procedural grounds rather than its substantive and methodological basis.

It is entirely unclear whether an 'easy access' pathway to health data for AI and algorithmic applications is the correct response to the scientific as well as practical problems facing medical professionals and researchers. This is because, contrary to other areas of algorithmic decision-making systems where accurate interpretability of an outcome may not be essential or significant, physicians are likely to be more interested in the thought process behind an outcome than the outcome itself. Providing access to more data does nothing to solve the problem of 'explainability' (Ahmad et al., 2018) (Habibzadeh et al., 2020). If anything, it complicates it further.

DP-3T

The Decentralised Privacy-Preserving Proximity Tracing (DP-3T) protocol is an open protocol that was developed during the COVID-19 pandemic to enable digital contact tracing (DCT) through sensors on consumer mobile phones. Using Bluetooth technology to broadcast ephemeral identifiers (EphID) to neighbouring devices, the DP-3T protocol differs from centralised approaches insofar as it allows: 1) local storage of the received EphIDs and 2) calculation of the exposure risk on the user's device (based on the strength of the received signals). Despite initial conflicts with competing protocols that favoured DCT systems with centralised features and capabilities of/for information collection and control, the DP-3T protocol set the standard for DCT worldwide. Eventually, Google and Apple developed their - very similar to DP-3T - own protocol that scaled up smartphone-based DCT across Europe, North America, and South America by baking its functionality into their operating systems (Android and iOs, respectively). Although important questions over the deployment, affordances, and actual usage of the Exposure Notification system remain, DP-3T exemplified a collective socio-computational effort which provided a highly interoperable solution for public health without compromising the privacy of the individuals.

Recommendations

To address the concerns outlined above substantive amendments to key areas are recommended.

1. Interoperability of Electronic Health Records

Art. 23 & associated Annexes

Articles 14-27 of the Proposal set out a self-regulatory scheme that invites manufacturers to declare their conformity with the general specifications of the Proposal and its Annex—primarily linked to issues of interoperability and data security. However, as explained above, interoperability often comes with privacy risks and compromises. For this reason, the addition of explicit clauses for, or references to the principles of *'data protection by design and by default', and 'privacy by design and by default'* in the common specifications (Ar 23 (2) & (3)) and relevant Annexes of the Proposal are necessary to ensure future development of privacy-preserving protocols and standards for EHR interoperability.

2. Voluntary registration of wellness applications

Art. 31

Interoperability of wellness applications with the Electronic Health Records risks creating more problems than it is expected to solve:

a) Data subjects will not be able to opt out from sharing wellness app data with EHR providers;

b) Data overload hinders rather than helps healthcare professionals;

c) Interoperability requirements will disproportionately benefit Big Tech companies due to their control over gateways to the EHR market (ie app stores) and ownership of native wellness applications (Apple's Health) and EHR tools (Amazon Clinic).

Given the increasing importance of the smartphone in healthcare provision and research and the fact that of the majority of such devices are shipped with native health applications, interoperability of wellness applications with EHR systems requires more nuanced and holistic treatment. For this reason, Art. 31 should be removed along with all references to 'wellness applications' throughout.

3. Categories of electronic health data and consent

Art. 33

The Proposal's definition of electronic health data is extremely broad and, as a result, it risks creating an open-ended scheme for access to sensitive data. Two amendment strategies seem possible:

a) condition the sharing of electronic health data on the data subject's explicit consent; or

b) limit the scope of electronic health data that can be shared.

Recommendation re a): Amend Art. 33 (1)

'Data holders shall make the following categories of electronic data available for secondary use in accordance with the requirements of consent and explicit consent as set out in the Regulation (EU) 2016/679 and in accordance with the provisions of this Chapter'.

Recommendation re b): Amend Art. 33 (1)

Delete Art. 33 (1) (f), (g), (n) or add a new paragraph indicating:

Data under Art. 33 (1) (f) (g) and (n) are electronic health data for the purposes of this regulation when access is requested for one or more of the purposes set out under Art. 34 (1) (a), (b) or (c).

4. Asymmetry between who gives data and who can access it

Art. 33(3) and Art. 47

The Proposal adopts an open-ended classification of the entities that will be entitled to access health data. At the same time, it constrains the range of the 'data holders' to those entities that belong in the sphere of healthcare (either as providers of such services or as researchers). The policy rationale behind this asymmetry is unclear and requires further elaboration and justification by the drafters. Regardless, to remedy this anomaly, it is recommended that the remit of the entities entitled to submit a data access request is restricted by amending Art. 47 (1):

Entities and bodies in the health or care sectors, including public and private providers of health or care as well as entities or bodies performing research in relation to these sectors, may submit a data request for the purposes referred to in Article 34.

5. Unduly permissive approach to algorithmic research and AI

Art. 34 (f-h)

The Proposal allows data applications for AI-related activities. Art. 34 in combination with Art. 47 and Article 33 of the Proposal create a backdoor for accessing electronic health data by Big Tech or by any other entity with the infrastructural, logistical, and financial capacity to experiment with machine learning, algorithms, and personalised 'smart' technologies. Such confidence in the ability of AI to help with medical research requires a solid scientific basis, capable of justifying treating AI developers equally to trained medical researchers and practitioners. Equating AI developers with medical researchers requires rigorous theoretical and methodological evidence before becoming a legal reality. This evidence is currently lacking. For this reason, Art. 34 (f-h) should be removed altogether. Alternatively, Art. 34 (g) and (h) should be included as sub-sections under Art. 34 (f) with the latter being amended as follows:

'development and innovation activities for reasons of public interest'.

6. Consent and Transparency

Art. 37, 38, and Art. 46

The Proposal adopts an ex-post mechanism for providing general information by noting that health data access bodies will make public any data permit (or their response in any other case) within 30 working days of issue. As a result, access on the basis of consent is replaced by a transparency obligation. This is problematic considering who may access health data for secondary use and under what circumstances.

In this context, Art. 38(2) should be amended as follows:

Health data access bodies shall not be obliged to provide the specific information […] to each natural person concerning the use of their data for projects subject to a data permit following a request from any natural or legal person. In addition, Health data access bodies shall keep a public online depository of all data applications and shall provide general public information on all the data permits issued pursuant to Article 46.

Art. 38 (3) should be amended as follows:

The electronic health data referred to in paragraph 1 shall cover data processed for the provision of health or care or for public health, research, innovation, policy making, official statistics, patient safety or regulatory purposes, collected by entities and bodies in the health or care sectors following the patient's explicit consent, including public and private providers of health or care, entities or bodies performing research in relation to these sectors, and Union institutions, bodies, offices and agencies.

Art. 38 (5) shall be removed and Art. 37 (1) (a) should be amended as follows:

decide on data access applications pursuant to Article 45, and following the patient's explicit consent, authorise and issue data permits pursuant to Article 46 to access electronic health data falling within their national remit for secondary use and decide on data requests in accordance with Chapter II of Regulation [...] [Data Governance Act COM/2020/767 final] and this Chapter;

7. Technical infrastructure

Art. 50 (2)

The Proposal allows data users to download non-personal data from the secure processing environment instead of processing it therein. Given the broad scope of electronic health data as adopted by the Proposal and the omnipresent risk of de-anonymisation (particularly from those entities with immense data wealth and computational capacity), this measure should be further discussed and justified, or entirely removed:

The health data access bodies shall ensure that electronic health data can be uploaded by data holders and can be accessed by the data user in a secure processing environment.

References

Ahmad M.A., Eckert C. and Teredesai A.. (2018). Interpretable Machine Learning in Healthcare. *Proceedings of the 2018 ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics*, pp. 559–560. https://doi.org/10.1145/3233547.3233667

Bincoletto G. (2020). Data Protection Issues in Cross-Border Interoperability of Electronic Health Record Systems within the European Union. *Data & Policy* 2, E3. https://doi.org/10.1017/dap.2020.2

Habibzadeh H, Dinesh K, Shishvan OR, Boggio-Dandry A, Sharma G, Soyata T. (2020) A Survey of Healthcare Internet-of-Things (HIoT): A Clinical Perspective. *IEEE Internet Things Journal*, 7(1):53-71. https://doi.org/10.1109/jiot.2019.2946359

Rothstein M A and Tovino S. (2019). Privacy Risks of Interoperable Electronic Health Records: Segmentation of Sensitive Information Will Help. *Journal of Law, Medicine & Ethics* 47, pp. 771–777. https://10.1177/1073110519897791

European Data Protection Supervisor. (2020) *A Preliminary Opinion on Data Protection and Scientific Research*
Terzis, P. (2022). Compromises and Asymmetries in the European Health Data Space. *European Journal of Health Law* (published online ahead of print 2022). https://doi.org/10.1163/15718093-bja10099

Terzis, P., & Santamaria Echeverria, (Enrique) OE. (2023). Interoperability and Governance in the European Health Data Space Regulation. *Medical Law International*, *OnlineFirst*. https://doi-org.libproxy.ucl.ac.uk/10.1177/09685332231165692

Troncoso ., Bogdanov D., Bugnion E., Chatel S., Cremers C., Gürses S., Hubaux J.-P., Jackson D, Larus J. R., Lueks W., Oliveira R., Payer M., Preneel B., Pyrgelis A., Salathé M., Stadler T., and Veale M. (2022). Deploying decentralized, privacy-preserving proximity tracing. Communications of the ACM, Vol. 65 No. 9, p. 48-57. https://doi.org/10.1145/3524107

Images
Cover: Photo by Camilo Jimenez on Unsplash
Page 3: National Cancer Institute on Unsplash

FACULTY OF LAWS

UCL