Bimczok, S. P., Godynyuk, E. A., Pierey, J., Roppel, M. S., & Scholz, M. L. How is excellence and trust for using artificial intelligence ensured? Evaluation of its current use in EU healthcare (Policy brief). SEEJPH 2021, posted: 18 April 2021. DOI: 10.11576/seejph-4685

POLICY BRIEF

How are excellence and trust for using artificial intelligence ensured? Evaluation of its current use in EU healthcare

Simon Paul Bimczok[1], Elizabeth Alexandra Godynyuk[1], Joris Pierey[1], Malin Siv Roppel[1], Mirjam Lisa Scholz[1]

[1]Faculty of Health, Medicine, and Life Sciences, Maastricht University, The Netherlands

Corresponding author: Elizabeth Alexandra Godynyuk
Email: l.godynyuk@student.maastrichtuniversity.nl
Address: INTHEALTH department: Duboisdomein 30, 6229 GT, Maastricht, the Netherlands

Abstract

Context: Artificial intelligence (AI) could be a key driver in different healthcare dossiers, ranging from preventive to diagnostic and treatment purposes. The establishment of the Artificial Intelligence High-Level Expert Group in the European Commission, as well as their White Paper, show first attempts of creating policies in the domain of artificial intelligence in the EU. Despite these policy approaches, there is a need for a coherent regulatory framework that enables the efficient use of AI in the field of health. The aim of this policy brief is to evaluate current legislative gaps in terms of the introduction of AI in healthcare, focusing on the domains of Data Protection, Liability & Transparency, as well as Robustness & Accuracy.

Policy Options: This policy brief identified a high degree of eHealth infrastructure fragmentation on member state level and limited action towards a structured and coherent framework for AI in healthcare, under the domains of Data Protection, Liability & Transparency, and Robustness & Accuracy.

Recommendations: A unified approach at EU-level, based on proposed recommendations and merged into the form of a Directive, is advised. The development of the Health-AI-Directive will bring progress and improvement to legal certainty in the European AI-landscape. The introduction of the Health-AI-Directive is recommended to ensure trust and excellence in the use of AI in healthcare.

Keywords: *Artificial Intelligence (AI); European Public Health; Trustworthiness; Health Policy; Digital Health*

Acknowledgments: The authors of this policy brief would like to thank all our tutors, lecturers and professors of the M.Sc. Governance and Leadership in European Public Health, with special thanks to Kasia Czabanowska and Rok Hržič, for enabling and encouraging us in the creation of this policy brief.

Authors' contributions: All authors contributed equally to this work

Conflict of interest: None declared

Source of funding: None declared

Introduction: Pointing Artificial Intelligence in the right direction

Artificial Intelligence (AI) is frequently described as one of the promising technologies that could guide crucial societal and technological change in the upcoming years (1). In the field of public health, AI could be a key driver in different domains, ranging from preventive to diagnostic purposes. Especially, the implementation of medical imaging practices through AI-imaging is likely to revolutionise public health practices (2). In the European Commission's (EC) work programme for 2021, the European Union's (EU) "fit for the digital age" will be attained through the creation of legislative developments of safety, liability, fundamental rights, and data safety of AI (3). This is particularly important, given the fact that the EU lacks a legal framework on the use of AI as there is no legal basis available that regulates the use of AI in healthcare. With respect to the current amendments in different healthcare dossiers, including the expected amendments of the Medical Devices Regulation (4), the creation of a stringent legislative environment of AI in public health is evident. Already in 2018, the EC acknowledged the need for policy action on AI, and established the High-Level Expert Group on Artificial Intelligence (AI-HLEG) (5). As a consequence, the White Paper "On Artificial Intelligence - A European approach to excellence and trust" was published (6) and opened to consultations with relevant stakeholders including civil society, industry, and academics from 19 February to 14 June 2020. Additionally, the EC issued a Communication on Building Trust in Human Centred Artificial Intelligence (7) and thus defined seven characteristics of trustworthy AI, namely (I) human agency and oversight, (II) technical robustness and safety, (III) privacy and data governance, (IV) transparency, (V) diversity, non-discrimination and fairness, (VI) societal and environmental well-being as well as (VII) accountability. Trust and excellence in AI are key requirements for AI-applications in the medical field, since sensitive data is processed. Against this background, the use of AI in healthcare is categorised as high-risk AI-applications.

Despite these policy approaches, the EU currently lacks a coherent legally binding regulatory framework that would enable the efficient use of AI in the field of healthcare. Specifically, the perspectives on data protection, liability and transparency as well as robustness and accuracy should be addressed in such a coherent framework. As such, the following policy brief aims to identify and evaluate current gaps and needs in the respective regulatory framework. The guiding question and corresponding sub-questions are therefore:

Q: Which regulatory legislations are necessary for enabling an adequate use of AI in healthcare?

> SQ (1): Which existing policies address the domains "data protection", "liability & transparency", and "robustness & accuracy" for healthcare-AI?
>
> SQ (2): What are the current gaps in legal regulations regarding AI in healthcare?

The overarching vision is to improve patient-centred healthcare and prevention for all European citizens by ensuring faster, more effective, and more efficient use of AI in healthcare. As such, this policy brief proves its relevance in presenting policy recommendations on the creation of a legal framework for AI-applications in the field of healthcare to the EC's AI-HLEG and other relevant stakeholders.

Infobox 1 – Glimpse of the possibilities: AI in healthcare

Nowadays, AI is getting more and more presence in healthcare. For example, in ophthalmology, the widespread availability of optical coherence tomography (OCT) and a lack of expert interpreting results produced by OCT poses a problem. For such medical image analysis and referral, AI presents a potential solution. If Deep Learning (DL) combined with the results the OCT produces promising outcomes. The AI has an accuracy of 94,5% when identify the type of eye disease (8).

In mammography, AI is also on the rise. Mammography's of 60,886 patients diagnosed with breast cancer were used to train a DL model. After this model was introduced, it detected women at high risk of breast cancer. It put 31% of all patients in the top risk category for potential breast cancer (9).

Figure 1: Infobox 1 - Glimpse of the possibilities: AI in healthcare

Context: Identification of Gaps in Policies and Regulations

This report assessed current gaps and limitations in policies and regulations, based on six requirements highlighted in the 'White Paper on Artificial Intelligence' (6), established by the EC. The White Paper outlines the necessity of elaborating on such topics towards further development in future regulatory frameworks in AI. These requirements include training data, keeping of records and data, information provision, human oversight, as well as robustness and accuracy.

A literature search regarding policies in each of the six requirements was conducted to identify the current situation. The framework was further delineated into three overarching domains: data protection, liability & transparency, and robustness & accuracy. The resulting search yielded current policies and frameworks in use. Findings were established and assembled under 'solutions', which can be found in Table 1. Current gaps in each domain and requirements are addressed, and framework recommendations are described and elaborated in Table 1.

Table 1: Current Policies, Frameworks, and Current Gaps Based on Domains

Domains	Solutions	Current Policy Instruments & Frameworks*				Current Gaps/Needs
Data protection	Training Data: - Assurance that use of products and services are safe - Tackle discrimination - Protection of personal and private data	GDPR: Art. 5 (1)(f) Art. 6 (1)(d&f) Art. 9 (1) Art. 32 Art. 35	Medical Device Regulation (2017/745): Art. 5 (2)	Declaration on Ethics and Data Protection in AI: 4 (a) 6 (a-d)	Charter of Fundamental Rights of the EU: Art. 8 (2) Art. 21	No specific regulation for training data in healthcare with AI in general data protection guidelines, and for medical devices.
	Keeping of Records and Data: - Records of dataset development to use for training data and testing - Methodologies for programming, training, building, testing & validating AI	GDPR: Art. 5 (1)(e) Art. 30				No AI-specific verifiability and compliance measures. No data retention framework; policies only at national level.
Liability & Transparency	Information Provision: - Information about AI's capabilities and limitations - Inform citizens, when they interact with an AI system	GDPR: Art. 13 (2)(f)				Need for clearer transparency guidelines about the functionality of AI-systems.
	Human Oversight: - Output reviewed and validated by a human - Ensure human intervention after AI output - Impose operational constraints on AI system	GDPR: Art. 22				Governance mechanism of how to implement the safeguards is not defined.
Robustness & Accuracy	- Robust and accurate during all life cycles phases - Reproducible outcomes - Adequately able to deal with errors inconsistencies during all life cycle phases - Resilient against cyberattacks	Cybersecurity Act		GDPR		European cybersecurity certificate.

*- citations refer to the General Data Protection Regulation (17), Declaration on Ethics and Data Protection in AI (20), Charter of Fundamental Rights of the European Union (21), and Cybersecurity Act (34)

Policy Options: Identification of needs and recommendations for AI-requirements

AI poses great opportunities for healthcare. To lead this development in a direction that mitigates potential risks, regulations are required. In the following sections the current gaps are discussed, followed by recommendations to address these gaps.

Data Protection

This domain is differentiated into the parts "Training Data" and "Keeping of Records and Data". These parts go into depth on how AI training data should be regulated and how it should be stored.

Training Data

Training data in AI is the personal data that is used to direct the programme to recognise patterns and use the technology (e.g., neural networks) accurately and accordingly (13-15). Training data sets the basis for the functioning of the whole AI-process and -system. Therefore, sufficient training data is fundamental for a sufficient AI-system (13). Several challenges regarding training data arise that have not yet been sufficiently addressed in mandatory legal requirements (6). Assurance of safety of the products and services used by the AI-system, according to the standards of the EU, is necessary (6). A regulation for safety of medical devices can be found in Art. 5(2) of the Regulation (EU) 2017/745 on medical devices (16). The General Data Protection Regulation (GDPR) regulates the general security of processing personal data in Art. 32 (17). Additionally, measures should be addressed which ensure that the use of AI does not lead to discrimination (6). The training dataset is often smaller and differs from the targeted population (18). For this reason, a regulation to detect, avoid, and counteract discrepancies between the target population and the training data is crucial to avoid bias in the output of AI in healthcare (19). Avoidance of bias in AI is mentioned in the Declaration on Ethics and Data Protection in AI (20).

Universal laws protecting people against discrimination can be found in Art. 21 of the Charter of Fundamental Rights of the EU (CFR) (21) and in Art. 9(1) of the GDPR (17). Lastly, regulations for adequate protection of personal data, used in the context of AI in healthcare, is needed (6). Regulations for protection of personal data can be found in Art. 8(2) of the CFR, as well as in the Art. 5(1)(f), Art. 6(1)(d+f), and Art. 35 of the GDPR (17). Additionally, the Declaration on Ethics and Data Protection in AI mentions the need for protection of personal data during the development of AI (20).

Figure 2: Infobox 2 - Biased AI

Infobox 2 – Biased AI
AI that contains existing prejudices of the developers, resulting in discrimination or lack of fairness in automated decision-making. Biases in AI mostly occur through unrepresentative or incomplete training data, especially the underrepresentation of minority groups resulting in disadvantages (11, 12). Groups mostly affected by AI biases are people of black race, people from the Asian continent, woman and disabled (10, 12).

Even though the stated aspects are generally regulated in several legislative documents, there is no specific regulation addressing AI-training data in healthcare. Noted, general regulations apply for AI-training data in healthcare. Nevertheless, the specificity for a sufficient execution of the stated solutions in healthcare with AI in regard to training data is missing. Therefore, a separate legislative regulation addressing the processing of AI-training data in the context of healthcare is advisable.

Keeping of Records and Data

Under the data protection domain, there is a need for verification in compliance within algorithm development and programming. This requires record- and data-keeping within entities that intend to utilise AI-technology at multiple levels, from design to development to implementation, and continuous execution. Art. 30 of the GDPR requires maintenance of records used in data-processing to determine each activity that involves the use of personal data (17). AI-specific measures in record-keeping compliance in healthcare are limited, though. Furthermore, one of the principles in Art. 5(1)(e) of the GDPR states that data, under legal obligations, is to be kept for the shortest time that is applicable (17). Also, data generated in AI-algorithms merges to form an output, making it difficult to find a solution to track or delete inputted data. At EU-level, no data retention policy appears to exist since the removal of Directive 2006/24/EC (22). National level policies have been implemented instead (23).Current methods to respond to this need revolves around 'Verifiable AI'. Verifiable AI aims to certify each step in the process of AI-development for auditing, prior to deployment (24). This would provide mechanisms whereby entities would exercise better practices in retaining data and datasets for the purpose of traceability and to promote compliance. To further propagate a sound regulatory framework and strategy towards record- and data-keeping, audited trails are valuable for accountability (25). Ai4EU, a consortium sponsored by the EC, specifies a toolbox called 'VERIFAI' with the aim to verify steps in design and run time (26). Therefore, an EU-wide policy in AI-specific data retention is recommended, due to the novel risk this type of data poses. This would also have to comply with the CFR.

Liability & Transparency

Under the data protection domain, there is a This domain is divided into "information provision" and "human oversight". This part is an elaboration on how information of the functioning of AI should be regulated. Afterwards, the supervision of AI-systems will be discussed.

Information Provision

In terms of providing information on the development and use of AI in healthcare, a lack of transparency can be described as the main issue. To achieve transparency, it is important to deal with the so-called "black box" of an AI-application. This means understanding the aspects of an AI that influence the decision-making process. Therefore, it is important to strive for transparency, not only regarding the algorithms themselves, but also regarding the data and the automated decision making (ADM) processes, as well as transparency within the conceptual business model. The AI-HLEG identified transparency as a key requirement for AI-applications in healthcare in order to count as trustworthy (7). In their White Paper, a lack of transparency regarding the current legislation was described as a major problem (6). Moreover, the call for transparency and accountability is not only present in the EU, but also in the USA (27). There are two necessary requirements when providing information to achieve transparency, which are 1) clear information regarding the AI-system's capabilities and limitations and 2) clear information to citizens on the fact that they are interacting with an AI-system and not with a human. The latter is covered to some extent in Art. 13(2)(f) of the GDPR, where it is stated that "controllers must, at the time when the personal data are obtained, provide the data subjects with further information necessary to ensure fair and transparent processing about the existence of automated decision-making and certain additional information" (17). To close the regulatory gap of clear transparency guidelines on the functionality of an AI-system, the introduction of mandatory self-identification of these systems is recommended. This particularly applies to the purpose and conditions under which they are planned to function and their estimated level of accuracy (28). Additionally, detailed documentation of the decisions made by the AI-systems and the entire process (including business model transparency) is required (7). The information that is provided needs to be objective, concise, and easily understandable. In order to provide appropriate information about the application of AI-systems, policy makers need to consider the circumstances within their particular context of decision-making.

Human Oversight

Within the domain of liability and transparency, the aspect of human oversight of AI's decision making plays a crucial role. AI presents an undeniable potential to assist health professionnels (e.g radiologists) performance (35) in medical diagnostics. However, human oversight ensures that AI does not undermine human autonomy, whilst defining the liability of decisions made. Human oversight is determined by four main characteristics: (I) output reviewed and validated by a human, (II) ensuring human intervention after AI-output, (III) AI-monitoring and the ability to intervene, as well as (IV) imposing operational constraints on AI-systems (29). Against this background, Art. 22 of the GDPR defines the legal basis for automated, individual decision making and aims to implement safeguarding measures to the data subject's interests. According to Art. 22 of the GDPR, autonomous decisions must always be contested by humans (17). Nevertheless, a gap in the current policy framework shows no information on how to practically implement the mechanism of human oversight. This is especially important to address in the sense of AI's use in the field of (public) health. Hereby, three governance mechanisms are available. Firstly, human-in-the-loop (HITL), which refers to the introduction of human intervention in every step of the decision-making process. Secondly, human-on-the-loop (HOTL), which considers the capability of human oversight within the design-cycle as well as the monitoring of the AI's decision-making. Thirdly, the human-in-command (HIC) approach that allows human oversight of the overall activity of the AI-system, taking into account the economic, societal, legal, as well as ethical perspective (6).

With respect to the use of AI in the health sector, the mechanism of human-in-command (HIC) can be identified as the most desirable one. This governance mechanism covers the cluster of public health holistically, considering the economic, societal, legal, and ethical points of view. In addition to that, the approach is favoured by high EU civil servants, such as Commissioner for Innovation, Research, Culture, Education, and Youth, Mariya Gabriel (30). Nevertheless, effective use of this governance approach entails certain implications, such as sufficiently trained personnel capacities and corresponding financial capacities.

Robustness & Accuracy
In order to be trustworthy, AI-systems, particularly high-risk AI-systems, must be technically robust and accurate. Some AI-requirements need to be ensured to prevent problems according to the EC (6). AI-systems need to be (I) robust and accurate during all life cycle phases, (II) have reproducible outcomes, (III) be able to adequately deal with errors or inconsistencies during all life cycle phases, for example through control algorithms, and (IV) be resilient against cyberattacks (6). In a report by Hamon, Junklewitz & Sanchez (31), the reliability of outcomes, data-protection, and transparency of AI-models to prevent issues is stressed. Accuracy and transparency have a difficult interdependence within AI-applications. It is often the case that the more accurate a model is, the lower the transparency. This raises the question on whether the ability to describe how data is obtained may be less important than the ability to generate those results and validate their accuracy empirically (32).Currently, efforts are being made to provide policies on cybersecurity. This has implications for the robustness of AI-applications. The Cybersecurity Act, adopted in 2019, gives the EU a mandate on cybersecurity as the European Union Agency for Cybersecurity is making European cybersecurity certification schemes, which all the Member States have to comply with once implemented. Hamon et al. (31), propose designing a framework, using the GDPR, to make an evaluation that assesses the impacts of AI-systems on society. They also recommend the introduction of systematic methodologies to test the robustness of AI-models. Finally, sharing identified AI-model vulnerabilities and technological solutions to fix them among AI-practitioners is stressed. The GDPR generally provides meaningful indications for data protection in the context of AI-applications and could be used as a foundation to create a regulatory framework for AI in healthcare (33).

Recommendations: Roadmap for the implementation process

With respect to the identified gaps within the regulatory framework, as stated in the previous section, the following policy recommendations (Table 2) are directed towards the AI-HLEG. Hereby, it is emphasised that there are overlaps in the current framework that are thus mirrored within the recommendations.

Table 2: Policy Recommendations for each Domain

Domains	Solutions	Policy Recommendations
Data protection	Training Data	To introduce a legislative regulation specifically addressing safety, avoidance of bias, and protection of private and personal data in training data of AI in healthcare.
	Keeping of Records and Data	To provide legislation for compliance and verifiability of AI, particularly audit trails and data tracing, and regulate such practices with AI-specific data retention policies.
Liability & Transparency	Information Provision	To ensure transparency by introducing a mandatory self-identification and documentation of AI-systems in healthcare as well as their business models by addressing 1) their exact purposes and ways of automated decision-making, 2) the conditions under which they are planned to function and 3) their estimated level of accuracy.
	Human Oversight	To implement the human-in-command governance approach to AI applications, this implies to train and accumulate personnel capacities able to oversee the AI application (background in governance, health, and life science as well as digitization and its implications).
Robustness & Accuracy		To implement and enforce a framework, based on the GDPR, that would set rules for AI-cybersecurity across the EU e.g. promoting transparency. Within the framework, a platform to share knowledge of AI-vulnerabilities and technological solutions should be incorporated.
Overall Recommendation		To implement one overall legislative regulation for AI in healthcare addressing all three domains of data protection, liability and transparency, and robustness and accuracy.

From recommendation to implementation through legislation: A Health-AI-Directive?

The need for a framework dealing with AI in healthcare has been highlighted in the previous sections. The urgency of implementing this framework could also be shown by pointing out current gaps of AI-related regulations in the GDPR and other EU law, since the gaps within the framework allow space for further policy actions. With respect to the actual implementation of the suggested recommendations, several governance perspectives must be taken into consideration. This is particularly true given the involvement of multi-faceted stakeholders and their interests in the field of healthcare. Debates are likely to arise, questioning the competence of the EU in terms of creating legislation in the field of healthcare. However, in order to compete with and even exceed other global players in the realm of AI in healthcare, such as the USA and China, the EU needs to act unified and develop an accurate AI-framework.

At the EU-level, a unified approach, guided by the AI-HLEG, to transfer the current considerations from the White Paper into the form of a Directive, is advised. The development of this Directive would provide a basis for a legal framework, and merge into national law of the Member States. Additionally, this process would ensure a legally binding basis for a unified policy approach among the EU Member States concerning the use of AI in the field of healthcare.

In practice, this means that political decision-makers must always incorporate the aspects of data protection, accountability and transparency, as well as robustness and accuracy, into any decision-making-process on the use of AI in their specific context.

Against this background, a Health-AI-Directive is the most favourable instrument. On the one hand it allows the Member States a certain degree of flexibility to adapt the regulations on the use of AI in line with the specific conditions of their national healthcare system. On the other hand, a common path in the EU can be fostered by ensuring compliance with the key objectives in the context of AI. Hereby, the contextual national frameworks and differing national priority setting, as well as the urgency of a unified approach, are taken into consideration.

Conclusions

The development and establishment of the Health-AI-Directive as a regulatory EU-wide AI-framework, based on the recommendations above, constitutes one way to bring progress and improvement to legal certainty in the AI-landscape of the EU. It will counteract the fragmentation of the AI infrastructures among the Member States and contribute to the objectives of the AI-HLEG of “trust, legal certainty and market uptake” (6). This will strengthen the EU to pave the way for a trustworthy usage of high-quality AI in healthcare.

References

1. EIT Health and McKinsey & Company. Transforming healthcare with AI. The impact on the workforce and organisations.: EIT Health, European Union; 2020.
2. Oren O, Gersh BJ, Bhatt DL. Artificial intelligence in medical imaging: switching from radiographic pathological data to clinically meaningful endpoints. The Lancet Digital Health. 2020;2(9):e486-e8.
3. European Commission. Communication from the Commission to the European

Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. Commission Work Programme 2021. A Union of vitality in a world of fragility. 2020.

4. MedTech Europe. MedTech Europe welcomes the amendment of the Medical Devices Regulation and urges similar action for the IVD Regulation 2020. Available from: https://www.medtecheurope.org/news-and-events/press/medtech-europe-welcomes-the-amendment-of-the-medical-devices-regulation-and-urges-similar-action-for-the-ivd-regulation/#:~:text=MedTech%20Europe%20welcomes%20the%20recent,of%2026%20May%202021%2C%20and. [Accessed 02 December 2020]
5. European Commission. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe 2018.
6. European Commission. White paper. On artificial intelligence – A European approach to excellence and trust 2020. Available from: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf [Accessed 23 November 2020]
7. European Commission. Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions. Building Trust in Human-Centric Artificial Intelligence. COM(2019)168/F12019.
8. De Fauw J, Ledsam JR, Romera-Paredes B, Nikolov S, Tomasev N, Blackwell S, et al. Clinically applicable deep learning for diagnosis and referral in retinal disease. Nature Medicine. 2018;24(9):1342-50.
9. Yala A, Lehman C, Schuster T, Portnoi T, Barzilay R. A Deep Learning Mammography-based Model for Improved Breast Cancer Risk Prediction. Radiology. 2019;292(1):60-6.
10. Parikh RB, Teeple S, Navathe AS. Addressing Bias in Artificial Intelligence in Health Care. JAMA. 2019;322(24):2377-8.
11. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019;366(6464):447.
12. Kuner C, Svantesson DJB, Cate FH, Lynskey O, Millard C. Machine learning with personal data: is data protection law smart enough to meet the challenge? International Data Privacy Law. 2017;7(1):1-2.
13. Maes F, Robben D, Vandermeulen D, Suetens P. The Role of Medical Image Computing and Machine Learning in Healthcare. In: Ranschaert ER, Morozov S, Algra PR, editors. Artificial Intelligence in Medical Imaging: Opportunities, Applications and Risks. Cham: Springer International Publishing; 2019. p. 9-23.
14. Schmidt FA. Crowdsourced production of AI Training Data: How human workers teach self-driving cars how to see. Working Paper Forschungsförderung; 2019

15. Verma D, Julier S, Cirincione G. Federated AI for building AI Solutions across Multiple Agencies. ArXiv. 2018;abs/1809.10036.
16. European Parliament. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745. [Accessed 23 November 2020]
17. European Parliament and Council of European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) 2016. Available from: https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. [Accessed 27 November 2020]
18. Oakden-Rayner L, Palmer LJ. Artificial Intelligence in Medicine: Validation and Study Design. In: Ranschaert ER, Morozov S, Algra PR, editors. Artificial Intelligence in Medical Imaging: Opportunities, Applications and Risks. Cham: Springer International Publishing; 2019. p. 83-104.
19. Harvey H, Heindl A, Khara G, Korkinof D, O'Neill M, Yearsley J, et al. Deep Learning in Breast Cancer Screening. In: Ranschaert ER, Morozov S, Algra PR, editors. Artificial Intelligence in Medical Imaging: Opportunities, Applications and Risks. Cham: Springer International Publishing; 2019. p. 187-215.
20. International Conference of Data Protection & Privacy Commissioners (ICDPPC). Declaration on Ethics and Data Protection in Artificial Intelligence 2018. Available from: https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_en_0.pdf. [Accessed 27 November 2020]
21. Charter of Fundamental Rights of the European Union (2000/C 364/01) (CFR). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT. [Accessed 27 November 2020]
22. European Commission. The Court of Justice declares the Data Retention Directive to be invalid [Press release]. 2014. Available from:https://ec.europa.eu/commission/presscorner/detail/en/CJE_14_54. [Accessed 25 November 2020]
23. European Commission. Data retention 2016. Available from: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/data-retention_en. [Accessed 23 November 2020]
24. Jacques Robin and Florian Zimmermann (editors), "A simple guide to Verifiable AI". Published on the AI4EU platform: https://www.ai4eu.eu/ June 24, 2020.
25. Brundage M, Avin S, Wang J, Belfield H, Krueger G, Hadfield G, et al. Toward trustworthy AI development: mechanisms for supporting verifiable claims. arXiv preprint arXiv:200407213. 2020.
26. Dreossi T, Fremont DJ, Ghosh S, Kim E, Ravanbakhsh H, Vazquez-Chanlatte M, et al., editors. VerifAI: A Toolkit for the Formal Design and Analysis of Artificial Intelligence-

Based Systems; 2019; Cham: Springer International Publishing.

27. Garfinkel S, Matthews J, Shapiro SS, Smith JM. Toward algorithmic transparency and accountability. ACM New York, NY, USA; 2017.
28. High Level Expert Group on Artificial-Intelligence. Policy and Investment Recommendations for Trustworthy AI. Brussels: European Commission; 26 June 2019.
29. European Commission. Requirements of Trustworthy AI 2020. Available from: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1. [Accessed 04 December 2020]
30. Euractiv. Digital Brief: Tech Biopower. 2019 Available from: https://www.euractiv.com/section/digital/news/digital-brief-tech-biopower/. [Accessed 04 December 2020]
31. Hamon R, Junklewitz H, Sanchez I. Robustness and explainability of artificial intelligence. Publications Office of the European Union. 2020.
32. London AJ. Artificial Intelligence and Black-Box Medical Decisions: Accuracy versus Explainability. Hastings Cent Rep. 2019;49(1):15-21.
33. European Parliamentary Research Service. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence Luxembourg: Office for Official Publications of the European Communities. 2020. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf. [Accessed 23 November 2020]
34. European Parliament and Council of the European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) 2019. Available from: https://eur-lex.europa.eu/eli/reg/2019/881/oj [Accessed 04 December 2020]
35. Allen B, Jr., Seltzer SE, Langlotz CP, Dreyer KP, Summers RM, Petrick N, et al. A Road Map for Translational Research on Artificial Intelligence in Medical Imaging: From the 2018 National Institutes of Health/RSNA/ACR/The Academy Workshop. Journal of the American College of Radiology. 2019;16(9):1179-89.
36. Challen R, Denny J, Pitt M, Gompels L, Edwards T, Tsaneva-Atanasova K. Artificial intelligence, bias and clinical safety. BMJ Quality &amp; Safety. 2019;28(3):231-7.