# E-HEALTH AS A RESULT OF AI, A "PANDORA'S BOX" FOR PRIVACY?

Rob van den Hoven van Genderen

Rob van den Hoven van Genderen, Professor of AI & Robotlaw, Faculty of Law of the University of Lapland, director of the center for Law &internet at the Law Faculty of the Vrije Universiteit Amsterdam and visiting professor at the National Taiwan University and the Kyushu University (Japan). Further he is the Chair of the Netherlands Association for AI and Robotlaw (NVAIR) and science partner of Switch legal lawyers Amsterdam.

***Keywords*** ***ehealth, GDPR, privacy, ethics, artificial intelligence, covid-19, diagnosis, fundamental rights, data protection***

***Abstract*** *In a growing, worldwide increase of aging population and a fundamental lack of suitable medical personal Ehealth can be a considerable help to support the flaws in care and medical support. Ehealth is the next step in medical industry and medical communication on every level, from lifestyle advice to surgery and communication of medical data between professionals as well as between patients or governmental health authorities. In this respect it will be necessary to look into the ethical and legal acceptability of AI in the health discipline, considering the requirements of privacy, ethics and the protection of sensitive data as regulated in the GDPR.*

## 1. Introduction

The medical profession is bound by the Hippocratic oath to follow the ethical as well as practical rules to do no harm. This oath gives specific rules to practice this "art" meticulously. It even gives rules to protect the privacy of patients:

> *"Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private."*[1]

These basic values should also be part of practicing medical professions in a wide sense using new technologies as artificial intelligence (AI) and robotics. AI is everywhere; Pandora's Box is opened to an unlimited and intrusive number of applications concerning ehealth. AI will be everywhere, supporting patients who need care by telemetry, telemedicine and connected to caretakers and virtual and real doctors and specialists. AI can be used to follow elderly people to mitigate risks or analyze movements of people in case of contagious diseases as it became a useful instrument in the covid-19 pandemic. AI generated Apps can recognize tumors, nano- robots can remove them. AI will propose medical care actions.[2] AI will have a massive influence on the use and exchange of medical and very personal data. This development will certainly have positive effects: direct actions and control for the people who need them, but they will also be connected to exchange platforms, to smart meters and mobile devices, personal computers and maybe even smart vehicles. These devices are fed with sensitive personal information. This information is shared with third parties who provide services and return the specified information that is required from smart assistants and is analysed by specialists, caretakers and specified third parties as medical insurances. They will be informed about everything concerning health and care. But are those the natural and legal persons that should be informed? These data are specified

1 http://data.perseus.org/citations/urn:cts:greekLit:tlg0627.tlg013.perseus-eng3:1, accessed 30 May 2021.

2 See for an overview of several applications of AI in the medical industry: [https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare] accessed 30 May 2021.

in the General Data Protection Regulation (GDPR[3]) as Data according to Article 9 GDPR (sensitive data) and need explicit permission to be processed.[4] So what about the privacy of those people that are subject to these processes? How is this sensitive information protected? How to make the requirement of transparency, explainability and informed consent of real value to the data subject? Are the security measures and technology sufficient? What regulatory measures are taken? Is the GDPR a valuable instrument to protect the personal data and privacy and is the process "hack-free"? It is always difficult to make predictions certainly when it considers the future, but we can be sure that the use of AI will increasingly run through all veins of society. In this chapter the possibilities of protecting the privacy for eHealth applications in that future will be scrutinized. Who will be the owner of those data if any, what possible dangers lure to the physical and psychological human integrity?[5]

## 2. A short introduction on the relevance of AI and big data

The use of AI in ehealth is an increasing development that is unavoidable and requires increasing financial investments.

The importance of AI for ehealth (and the EU) is constantly stressed by actors in the field as is made clear by the European Union: *"A high-standard health system, rich health data and a strong research and innovation ecosystem are Europe's key assets that can help transform its health sector and make the EU a global leader in health-related artificial intelligence applications"*.[6] To understand its importance it is helpful to explain the essence of AI and its possible development.

### 2.1. Artificial intelligence as an engine, data is the fuel

Artificial intelligence, mimicking human intelligence is too undefined to define specifically, so I will add another description to enhance the confusion. Several scholars gave different description of the phenomena.[7] Generally one could describe that it is a technology that provides the possibility for an artificial system or entity to perform tasks in a human – like way –, in a gradual scalability. The Oxford dictionary describes AI as: "The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."[8] The Cambridge dictionary describes AI as: "the study of how to produce machines that have some of the qualities that the human mind has, such as the ability to understand language, recognize pictures, solve problems, and learn".[9]

Although these definitions are varied, there are some common themes. The first is that A.I. typically takes actions (it acts on information rather than simply processes it), and does so with a degree of autonomy (i.e. A.I.

---

3 REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ #.

4 Referring to special categories of "sensitive" data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, article 9 GDPR.

5 Ethical concerns relating to autonomy, trust, consent, identification, inclusion and digital divides, security, harm, misuse, and deception, to name just a few Jiya, T. (2019). Ethical Reflections of Human Brain Research and Smart Information Systems. *ORBIT Journal*, *2* (2). https://doi.org/10.29297/orbit.v2i2.113 [https://www.project-sherpa.eu/ethical-reflections-of-human-brain-research-and-smart-information-systems/].

6 [https://ec.europa.eu/jrc/en/news/being-smart-about-our-health-how-artificial-intelligence-can-help-transform-europe-s-health-sector], accessed May 2021.

7 [Artificial Intelligence Defined: Useful list of popular definitions from business and science [https://digitalwellbeing.org/artificial-intelligence-defined-useful-list-of-popular-definitions-from-business-and-science/].

8 "Artificial intelligence" [https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095426960, accessed May 2021.

9 ARTIFICIAL INTELLIGENCE | meaning in the Cambridge English Dictionary [https://dictionary.cambridge.org/dictionary/english/artificial-intelligence], accessed May 2021.

automates intelligent actions typically taken by a human). Secondly, A.I. is task or outcome-focused and adapts its behavior to achieve its goals. Thirdly, A.I. can re-program itself, based on what it learns. In other words, A.I. is active, agentic, automatic and adaptive. More simply, these definitions can be synthesized by summarizing A.I. as any "technology that behaves intelligently" ***[insofar as it responds adaptively to change]*** (the capacity to respond adaptively to change through the acquisition and application of knowledge is a hallmark of intelligence – i.e. the ability to cope with novel situations).[10]

## 2.2. Different levels of AI

Overall, AI is commonly divided into four different levels, two of them actually in place[11]:

1. Weak or narrow artificial intelligence, which is designed for specific and limited tasks as in production industry but also speech recognition and translators and even face recognition technology but also the artificial personal assistants, such as Apple's Siri, Amazon's Alexa, are a form of weak AI. But also the decision supporting systems based on the use of algorithms can be considered weak (although the effects can be strong);
2. Strong AI, is capable to perform different tasks at the same time not fully developed yet, is capable to gather, analyze and decide on data with less or no human control like a fully autonomous car.
3. General Artificial Intelligence (GAI), is one step beyond strong AI, capable to analyze all kinds of data and perform activities based on comparable neural networks like a human brain; Also emotional and creative intelligence based on the self-learning and evolutionary capability of independent functioning and developing algorithms can develop a system or entity like a growing and learning human brain, be it in shorter time
4. Artificial Super Intelligence (ASI), based on singularity, the surpassing of the capacity of the human brain on all intelligence levels.[12] This development is still science fiction but could be the result of the further development of AI. Of course this leads to dark expectations of AI taking over the world based on the thought that also AI will strive for power, per definition a human vice.

In a public consultation on the EU white paper on AI[13] also these worries were ventilated by several parties, be it on the present AI developments, requiring an independent supervisory system and liability rules for developing and using AI. Concerning ehealth AI will be of great help in discovering diseases as well as further research on diagnoses and treatment. In a research on the acceptance and use of AI this is recognized although there is a difference of acceptance between male and female researchers and practitioners.[14] On the darker side there also will be risks and dangers concerning misuse and vulnerability of personal data and possible bias

[10] Artificial Intelligence Defined: Useful list of popular definitions from business and science – digitalwellbeing.org] accessed 30 may 2021.

[11] See also [https://spotle.ai/feeddetails/What-Is-AI-Weak-AI-Strong-AI-with-examples-Key-disciplines-and-applications-Of-AI-/3173] accessed 30 May 2021.

[12] Based on Moore's law : exponential increase(transistor) (in this case) AI capacity.

[13] White Paper on Artificial Intelligence – *A European approach to excellence and trust* (COM(2020) 65 final), available on: [https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf] and PublicConsultationAIWhitePaper_Finalreportpdf.pdf accessed 30 May 2021.

[14] 219 people from 31 countries took part in the survey. 81% (n = 177) of participants agreed that AI will improve the daily work of Medical Physics Experts (MPEs) and 88% (n = 193) of respondents expressed the need for MPEs of specific training on AI. The average level of AI knowledge among participants was 2.3 ± 1.0 (mean ± standard deviation) in a 1-to-5 scale and 96% (n = 210) of participants showed interest in improving their AI skills. A significantly lower AI knowledge was observed for female participants (2.0 ± 1.0), compared to male responders (2.4 ± 1.0). 64% of participants indicated that they are not involved in AI projects. The percentage of female leading AI projects was significantly lower than the male counterparts (3% vs. 19%). O. Díaz, Gabriele Guidi, +2 authors F. Zanca, Published 2021in Physical media: PM: an international journal devoted to the applications of physics to medicine and biology : official journal of the Italian Association of Biomedical Physics, 13 January, 2020, DOI:https://doi.org/10.1016/j.ejmp.2020.11.037.

and discrimination.[15] This aspect will be scrutinized after the general description of six of the most common applications of AI in the medical sector.

## 2.3. (Big) Data, personal data and medical data.

Data can be of a technical, functional or personal character. Data are representations of a certain value. The combination and processing of data will produce information. Strange enough the Cambridge dictionary equals data with information.[16]

Personal data is data that can directly identify a natural person or is considered identifiable. Big data are vast amounts of data from variable sources that are processed with great velocity, logically by great computer power as is possible with AI generated systems. Big data are not organized and can lead to a variety of results dependent on the purpose and the way the underlying algorithm is functioning. Different descriptions of Big Data are represented in the figure as cited from the presentation of the big data university (IBM)

### 2.3.1. Medical data

The concept of medical data refers to all data of a biometric or physiological character of a natural person including personal data that can be used for applications for medical purposes such as personal data that is used for "track and trace" in medical emergency circumstances as for instance epidemic or pandemic or use of data for other public health purposes.

In the GDPR, article 4, there are 3 separate definitions that are considered medical data as described above:

> (13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
>
> (14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;[17]
>
> (15) 'Data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

All these data are considered to be of a sensitive character as referred to in the GDPR when these data are identifiable to a natural person. This also accounts for pseudonymized data that can be made identifiable by means of (AI) technology that will have the capability to make a person identifiable.[18]

'Data concerning health' is defined in Art. 4(15) GDPR as 'personal data'. The principle of purpose limitation intends to, inter alia, prevent data from being retained without reason. How narrowly such purpose must be chosen has not yet been clarified and is still discussed controversially. In any case, a change of purpose is only

[15] See also a comparable analysis of the issue: Emmanuel Salami, Artificial Intelligence (AI), Big Data and The Protection of Personal Data in Medical Practice *European Pharmaceutical Law Review*, Volume 3 (2019), Issue 4, Page 165–175.

[16] Information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer https://dictionary.cambridge.org/dictionary/english/data.

[17] See also: *Biometrics technologies: a key enabler for future digitalservices*, [https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Biometrics%20technologies_v2.pdf].

[18] Article 4 (5) GDPR: 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

possible under certain conditions, as defined in Art. 6(4) GDPR. In the study "Assessment of the EU Member States' rules on health data in the light of GDPR" the practical observation of ehealth data is covering a wide spectrum: "GDPR Article 4(15) defines data concerning health as personal data related to the physical and mental health of a natural person, all biometric technologies referring to all processes used to recognize, authenticate and identify persons based on physical and/or behavioral characteristics and the provision of health care services, which reveal information about a persons health status. In practice, however, health data are often understood as any personal data generated within healthcare systems, and some may also include data concerning health which are collected by citizens and patients through wearable devices, apps and self-reported information. In this chapter a wide definition of health data is used to include all the above, as well genetic data and biometric data. The data generated in the context of healthcare includes both personal data as defined in Article 4(1) GDPR and sensitive personal data as defined in Article 9(1) GDPR. Health and social care are understood in the sense of article 9(2)(h) GDPR, to include direct care provision, such as long-term care."[19] This means that there is a growing extension of personal data that can be considered ehealth data and therefore sensitive data.

## 4. The data protection problem concerning ehealth

In a report on AI by the UK parliamentary committee, Cotton-Barratt identified the 'large benefits,' as well as the challenges, that arise when AI is applied in healthcare: If it can automate the processes and increase consistency in judgments and reduce the workload for doctors, it could improve health outcomes. To the extent that there are challenges, essentially it means there is less privacy from the same amount of shared data, in that people can get more information out of a limited amount of data.[20]

While opening a world of new opportunities, rapid advances in AI and big data processing have been likened to be a "Pandora's Box," potentially unleashing a number of ethical dilemmas and raising uncertainty in the current legal frameworks on privacy and data protection. It is being argued that AI systems, for example, may run afoul of the consent of data subjects as it oftentimes collects processes and transfers sensitive personal data in unexpected ways without the means of giving adequate notice, choice, and options in a timely manner.

What impacts will AI systems have on biomedical and automated scientific research, especially on data sharing and confidentiality? What kind of control over their data should be adjudicated to patients? How can we ensure that AI-based methods and solutions adhere to general legal and ethical principles? And how will these technological advancements in the medtech industry are affected by different legal frameworks?[21] The EU, in this case the European Parliament proposes to lay the burden of data protection and security with the developers of the AI systems and applications and the supervisory role with national authorities. Although this resolution and underlying report of the Committee on Civil Liberties, Justice and Home Affairs is published in 2017, has not led to substantial acceptation of the European Commission it is still giving high-level indications for future regulations by stressing the responsibility of the developers and designers of AI applications. These rules are rather high level and not specifically directed to applications of ehealth.

Therefore it has to be interpreted to see the implications for the applicable phrases on the use of AI in ehealth:

> "(6.) Reiterates that the right to the protection of private life and the right to the protection of personal data as enshrined in Article 7 and 8 Convention of Fundamental Rights and Article 16 TFEU apply to all

[19] Assessment of the EU Member States' rules on health data in the light of GDPR, p. 14 [https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf].

[20] Robotics and artificial intelligence: Ethical and legal issues' (UK Parliament website, 5 October 2016) [https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14506.htm] accessed 31 May 2021.

[21] MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION with recommendations to the Commission on Civil Law Rules on Robotics[ https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html].

areas of robotics and artificial intelligence and that the Union legal framework for data protection must be fully complied with;

Underlines the responsibility of designers of robotics and artificial intelligence to develop products in such a way that they are safe, secure and fit for purpose and follow procedures for data processing compliant with existing legislation, confidentiality, anonymity, fair treatment and due process;

Furthermore, the Committee stresses the fact that the rapid development of AI and robotics is to be controlled by legislation that will ensure the principles of privacy by design, also or certainly concerning cyber-physical systems, being integration of human bodies (and minds!) with AI appliances.[22] Transparency an ethical aspect must be taken into account in the development by designers of AI applications for ehealth as well.[23]"

These principles that are mentioned in this resolution are of a general, mostly privacy protection oriented level and are confirmed on higher level in the European Charter on Human Rights and more specific in the GDPR. But the fact stays that also the GDPR, due to its historical, structural and political background is not specific enough to give solutions for the many different applications of AI in the ehealth sector.

## 5. The GDPR and health data

The EU General Data Protection Regulation (GDPR) is developed in a time that there was hardly any knowledge about the developments of AI and smart applications.

This means that it often is difficult adequately respond to these technological challenges However, many uncertainties still remain regarding the scope, direction and effects of the impact of AI in eHealth systems and personalized medicine. The main problem of GDPR is that the regulation, due to the high level of giving instructions to the addressees, is not capable to specify on different AI applications.[24] Addressing the many challenges generated by AI requires going beyond any one disciplinary perspective or frame of reference. From the start the GDPR was negotiated the purpose has been high level harmonization and technological neutrality. No specific reference to AI, let alone the effect of AI on ehealth, can be found as a result. There are important general principles that apply on the protection of personal data to take into account that will be applicable to ehealth data and the processing by AI.

There are though very important general principles that always have to be taken into account: Recital 4 of the preamble to the GDPR states: "The processing of personal data must be designed to serve humanity". This re-

[22] (7.) Calls on the Commission to ensure that any Union legislation on robotics and artificial intelligence will include measures and rules which take into account the rapid technological evolution in this field, including in the development of cyberphysical systems, to ensure that Union legislation does not lag behind the curve of technological development and deployment; stresses the need for such legislation to be compliant with rules on privacy and data protection, i.e. concerning information obligations, the right to obtain an explanation of a decision based on automated processing, the requirement to follow the principles of privacy by design and by default, the principles of proportionality, necessity, data minimization, purpose limitation, as well as transparent control mechanisms for data subjects and data protection authorities, and appropriate remedies in compliance with current legislation; calls for the review of rules, principles and criteria regarding the use of cameras and sensors in robots, artificial intelligence in accordance with the Union legal framework for data protection.

[23] (10.) Calls on the Commission and the Member States to promote strong and transparent cooperation between the public and private sectors and academia that would reinforce knowledge sharing, and to promote education and training for designers on ethical implications, safety and respect of fundamental rights as well as for consumers on the use of robotics and artificial intelligence, with particular focus on safety and data privacy European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on Legal Affairs with recommendations to the Commission on Civil Law Rules on Robotics' (23 November 2016) 2015/2103(INL). As also referred to in: Robert van den Hoven van Genderen, *Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics, EDPL, 3/2017*.

[24] On top of that, because it is a European Regulation having direct effect and binding for all Member States, although harmonizing, there are 27 (28 in time of enacting) that have to agree on its contents.

cital is in line with the ongoing debate that modern technology should improve the lives, privacy and security of individuals and not undermine fundamental rights.

Pursuant to Article 5 GDPR, the fundamental principles of the processing of personal data are: "The processing of personal data must be lawful, fair and transparent, relevant, limited to its purpose, accurate and secure." That means that also concerning e health the processing should take place with the utmost care and limited to its purpose and not shared with other parties without the consent or vital need of the data subject.

In Recital 78 it is stated that: 'The requirements of the protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organizational measures be taken to ensure that the requirements of this Regulation [...]'. That means that ultimate security measure should be in place on technical and organizational level. Data sharing should only be allowed with the consent of the data subject or when the patient's life is in danger.

## 6. Conclusion

Ehealth covers a wide spectrum of data. It is essential that personal data can be processed by means of AI to increase the quality of healthcare. Also, other AI applications in robotics and mobile and remote medical care certainly will be more efficient with the help of AI. For research as well for diagnostics the solution is to work with anonymized data. Informational rights for the data subject and transparency of the process cannot always be applied to integrated AI, certainly not if this is integrated into the physical functions of the human being. As far as possible the use of personal data must be processed in accordance with fundamental rights of the data subject and the requirements of the GDPR.

There is though, a significant risk of chilling effects for the development of AI and robotics if the GDPR has to be enforced on all AI applications.[25]

In a report of the Science and Technology Committee of the UK Parliament, the need for unhindered but controlled applications of AI technology is stressed:

> "*It is important to ensure that AI technology is operating as intended and that unwanted, or unpredictable, behaviors are not produced, either by accident or maliciously. Methods are therefore required to verify that the system is functioning correctly. According to the Association for the Advancement of Artificial Intelligence: it is critical that one should be able to prove, test, measure and validate the reliability, performance, safety and ethical compliance – both logically and statistically/probabilistically – of such robotics and artificial intelligence systems before they are deployed*."[26]

Of course there has to be room for critical and relevant questions for applying AI concerning ehealth. AI applications can result in lack of transparency an insufficient control of the data processing and even can be sensitive to intrusion and misuse of personal data. As questioned by Miller:

---

[25] Rob van den Hoven van Genderen, *Does Future Society Need Legal Personhood for Robots and AI?*, p. 257–292 in Erik Ranschaert c.s., Artificial Intelligence in Medical Imaging: Opportunities, Applications and Risks, Springer 2019.

[26] Interesting is the concluding recommendation of the Science and Technology Committee: "73. We recommend that a standing Commission on Artificial Intelligence be established, based at the Alan Turing Institute, to examine the social, ethical and legal implications of recent and potential developments in AI. It should focus on establishing principles to govern the development and application of AI techniques, as well as advising the Government of any regulation required on limits to its progression. It will need to be closely coordinated with the work of the Council of Data Ethics which the Government is currently setting up following the recommendation made in our Big Data Dilemma report.
74. Membership of the Commission should be broad and include those with expertise in law, social science and philosophy, as well as computer scientists, natural scientists, mathematicians and engineers. Members drawn from industry, NGOs and the public, should also be included and a programme of wide ranging public dialogue instituted." [https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14506.htm#_idTextAnchor014.].

> "Questions remain about the applicability, practicality, and value of AI in medical practice: How is AI use in medical practice distinguished from big data analytics applications for health care delivery and population health? Can AI address medical practice 'pain points', providing more efficient and efficacious care while de-escalating physician burnout? Will AI improve patient outcomes when used at the point of care? Can Internet-of-Things health care facilities and medical homes become a platform for safer, higher quality, more connected patient care?"[27]

On the other hand we have to watch for bioconservatism as a stance of hesitancy and skepticism regarding radical technological advances, especially those that seek to modify or enhance the human condition. This line of thinking even could lead to conspiracy theories that governments or medical industry wants to control human life by body integrating technology or advanced track& trace or other control applications as for instance a corona-app. Also conservatism could strengthen thoughts about compromising human dignity, and opposition to movements and technologies including transhumanism, human genetic modification, "strong" artificial intelligence, and the technological singularity. Many bioconservatives also oppose the use of technologies such as life extension and pre-implantation genetic screening. On the other hand AI- bioliberals believe that enhancement should generally be permitted. They do not view enhancement and AI applications as unusually risky but can open chances and improvement of human life, helped by technological developments. The ultimate claim on the positive use of AI would fit the conviction of the transhumanist ideas where AI in ehealth to enhance the human improvement is considered to be the way to go forward in society.

The deployment of AI in ehealth though should not set aside ethical and legal requirements of processing data as well as protection as set high level principles in the GDPR.

Several general and specific rules could be used as a basis for guidelines in this perspective. Hereby reference can be made to the European Ethical Guidelines on AI as applications should be:

(1) Lawful – respecting all applicable laws and regulations;

(2) Ethical – respecting ethical principles and values;

(3) Robust – from a technical perspective while taking into account its social environment.[28]

The Council of Europe, to be precise, the Consultative Committee Of The Convention For The protection Of Individuals With Regard To Automatic Processing Of Personal Data, in her Guidelines proposes a comparable set, logically more specifically oriented on the aspect of privacy as it concerns Convention 108. The key elements of this approach are:

– lawfulness, fairness, purpose specification, proportionality of data processing, privacy-by-design and by default, responsibility and demonstration of compliance(accountability),
– transparency, data security and risk management.
– AI applications should allow meaningful control by data subjects over the data processing and related effects on individuals and on society.[29]

Specifically, the use of sensitive personal data and location data must be backed by more specific regulation where there is a necessity to do so. Principle requirements as stated in article 5, 6 and 9 GDPR should be taken in consideration by programming and deployment of the apps. Further it must be clear that the applications of processing data by AI will differ relating to function and implication on the purpose of the processing and will have variable implications. If it concerns non-personal i.e. fully anonymized data the effect on the data-subject will be nonexistent maybe except for all over implications for society. If the processing is concerning personal data though, it has to be temporary (and therefore reversible), strictly necessary, proportional, transparent and verifiable, even with consent of the data subject. This also concerns the ehealth applications in broader sense,

[27] Miller AJoM, p. 130 [https://web2.augusta.edu/mcg/medicine/documents/dougmillerartiintelligence.pdf].
[28] [https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf].
[29] [https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8].

including processing behavioral patterns of the data subjects processed by ehealth connected actors in the field like medical experts, (academic) research, health authorities, test labs, psychological and social support, etc.).

Although the general effect of using AI on ehealth data processing can be considered as a positive development that will increase efficiency and effectivity on all levels. Still there will be points of attention to guard. Effectiveness and credibility of the use of AI on ehealth data will depend on the reliability of procedures. AI and the underlying algorithmic basis have to be specifically purpose oriented. Biased data must be filtered out to avoid unreliability which can lead to a greater risk of contamination of results. False positives (and negatives) create ‚false security'. All kinds of negative, social chilling effects must be taken into account and measures taken to prevent them as much as possible. There must be a clear, transparent and understandable information policy to inform the data subject and the ehealth actors about the purpose and use of the personal ehealth data being processed, and which parties can access the information. It can be considered to evaluate the supervisory function of the national privacy authority over the use of AI in ehealth and to specify its task concerning ehealth. The processing of ehealth data by AI is here to stay. We have to welcome the positive effects without losing attention for the possibility of risks of this development.

> *So long as I maintain this Oath faithfully and without corruption, may it be granted to me to partake of life fully and the practice of my art, gaining the respect of all men for all time. However, should I transgress this Oath and violate it, may the opposite be my fate.*[30]

## Bibliography


Allen, F., Crepaldi, L., Alsinet, C. *et al. Predicting the mutations generated by repair of Cas9-induced double-strand breaks. Nat Biotechnol* 37, 64–72 (2019). [https://doi.org/10.1038/nbt.4317, as referred to in https://www.nature.com/articles/s41746-019-0191-0.] accessed 25 May, 2021.

Dolev, S., Rosenblit, M. and Narayanan R. P., "Design of Nano-Robots for Exposing Cancer Cells," *2018 IEEE 18th International Conference on Nanotechnology (IEEE-NANO)*, Cork, Ireland, 2018, pp. 1–5, doi: 10.1109/NANO.2018.8626359. [https://ieeexplore.ieee.org/document/8626359] accessed 21 May, 2021.

Esteva, A. et al. *Dermatologist-level classification of skin cancer with deep neural networks*. *Nature* 542, 115–118 (2017).

European Commission, 'White Paper on Artificial Intelligence 'A European approach to excellence and trust'(COM(2020) 65 final.

European Commission, 'Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society'COM/2018/233 final.

European Commission, 'Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics' COM(2020) 64 final.

European Commission, Study on Big Data in Public Health, Telemedicine and Healthcare December 2016, by Gesundheit Österreich Forschungs-und Planungs GmbH December –2016 EW-06-16-218-EN-[https://ec.europa.eu/health/sites/health/files/ehealth/docs/bigdata_report_en.pdf] accessed 21 May, 2021.

European Commission, Proposal For A Regulation Of The European Parliament And Of The Council laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts{-Sec(2021)167final}-{Swd(2021)84final}-{Swd(2021)85final}(Artificial Intelligence Regulation) Brussels, 21.4.2021 Com(2021) 206 Final [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1] accessed 31 May.

European Data Protection Board, 'Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak' (2020) [https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf] accessed 31 May 2021.


[30] Idem note 1.

European Data Protection Board, "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak", Adopted on April 21, 2020, p. 3 [https://edpb.europa.eu/sites/edpb/fi les/fi les/fi le1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.] accessed 31 May 2021.

Hoven van Genderen, van den, R, *Does future society need legal personhood for Robots and AI?* In E. R. Ranschaert, Sergey Mozorov, Paul R. Algra, *Artificial Intelligence in Medical Imaging Opportunities Applications and Risk*, p. 257 – 290 Springer Publishing international AG, 2019.

Li G., Eby D.W., Santos R., Mielenz T.J., Molnar L.J., Strogatz D., Betz M.E., DiGuiseppi C., Ryan L.H., Jones V., Pitts S.I., Hill L.L., DiMaggio C.J., LeBlanc D., Andrews H.F.; LongROAD Research Team. *Longitudinal Research on Aging Drivers (*LongROAD): study design and methods. Inj Epidemiol. 2017 Dec; 4(1):22. doi: 10.1186/s40621-017-0121-z. Epub 2017 Aug 1. PMID: 28736796; PMCID: PMC5537138.

Maestro, Del. F., the Virtual Operative Assistant: *An explainable artificial intelligence tool for simulation-based training in surgery and medicine, Plos one*, February 27, 2020, [ https://doi.org/10.1371/journal.pone.0229596 ] accessed 21 May, 2021.

Miller, D. Douglas & Eric W. Brown, *Artificial Intelligence in Medical Practice: The Question to the Answer?*,The American Journal of Medicine, Vol 131, No 2, February 2018.

Montani, Stefania *Exploring new roles for case-based reasoning in heterogeneous AI systems for medical decision support*, Springer, 2007, Appl Intell (2008) 28: 275–285 DOI 10.1007/s10489-007-0046-2.

Owkin, Ai For Medical Research [https://owkin.com/federated-learning/?utm_source=adwords&utm_medium=cpc&utm_campaign=FL&gclid=Cj0KCQiA4L2BBhCvARIsAO0SBdY3JwiMhSkjUglGPu_veaXKuLOIz2A57MKeL04A_xt_J4gtwLpK6QgaAgQrEALw_wcB] accesed, 25 May, 2021.

Strodthoff, N. & Strodthoff, C. *Detecting and interpreting myocardial infarction using fully convolutional neural networks*. *Physiol. Meas.* 40, 015001 (2019).

Su, H., Yang C., Ferrigno G. and De Momi E., "*Improved Human–Robot Collaborative Control of Redundant Robot for Teleoperated Minimally Invasive Surgery*," in *IEEE Robotics and Automation Letters*, vol. 4, no. 2, pp. 1447–1453, April 2019, doi: 10.1109/LRA.2019.2897145. [https://ieeexplore.ieee.org/document/8633418] accessed 18 May, 2021.

Uddin, M., Wang, Y. & Woodbury-Smith, M. *Artificial intelligence for precision medicine in neurodevelopmental disorders*. *npj Digit. Med.* 2, 112 (2019). https://doi.org/10.1038/s41746-019-0191-0.

UK Parliament, '*Robotics and artificial intelligence: Ethical and legal issues'* (UK Parliament website, 5 October 2016) [https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14506.htm] accessed 31 May 2021.

Robitzski, D., *Neoscope*, 28 Januari, 2020 [Remote Controlled Neural Implant Controls Rats' Brains (futurism.com)] accessed 21 May, 2021.

Salami, Emmanuel, Artificial Intelligence (AI), Big Data and The Protection of Personal Data in Medical Practice, *European Pharmaceutical Law Review*, Volume 3 (2019), Issue 4.

Warwick K. et al. (2004). "*Thought Communication and Control: A First Step Using Radiotelegraphy*." *IEE Proceedings on Communications* 151 (3): 185–189.