Applications of AI technology are being developed in healthcare. The prospects for the deployment of targeted AI applications in medical treatment, clinical trials, drug research, and public health are promising and groundbreaking.

But the deployment of these new technologies in healthcare also raises legal questions, especially from a human rights perspective. This contribution therefore focuses on the human rights analysis of AI applications in healthcare and how these applications relate to the Oviedo Convention.

Key words: artificial intelligence, patients’ rights, Oviedo Convention.

1. Introduction

The rise of Artificial Intelligence (AI) goes beyond self-driving cars and other intelligent control systems in many sectors (industry, agriculture, etc.).
Applications of AI technology are also being developed in healthcare and are even being used on an experimental basis, especially in diagnostics. The prospects for the deployment of targeted AI applications in medical treatment, clinical trials, drug research, and public health are promising and groundbreaking.

But the deployment of these new technologies in healthcare also raises legal questions, especially from a human rights perspective. These involve more than guaranteeing privacy when processing large numbers of health data. Other questions relate more to access to AI applications, the duty to inform and thus the informed consent principle, the quality and safety of AI systems, and related liabilities for faulty AI products/services.

This contribution therefore focuses on the human rights analysis of AI applications in healthcare and how these applications relate to the Oviedo Convention (OC).

2. AI applications in health care

What is AI?

After the development of eHealth in all its guises, Artificial Intelligence (AI), whether or not in combination with other digital technologies, may constitute a new revolution in healthcare. The applications are numerous, but what do we mean by AI? Basically, AI refers to a computer programme using algorithms for rapid analysis of large volume of data to predict or recommend decisions. The OECD Council of Artificial Intelligence defines AI systems as: ‘a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy’.*

In addition, different types of AI technology can be identified, including machine-learning applications (where computer systems are trained to recognise pattern/algorithms intended to perform a particular function).** Deep learning or “deep structured learning” (DL) is a subset of machine learning (ML) training the computer to learn on its own by recognizing patterns using many layers of processing (so-called neural networks).*** Such systems employ very large datasets, and are what is called ‘data-driven’. Given the data processing complexity, ML algorithms are also classified as “black-boxes”, i.e., the results are very difficult for physicians to interpret fully.**** As will be discussed hereafter, that is one of the main legal challenges in health care.

---

*** Ibid, p. 4.
AI applications in health care

In healthcare, such AI systems can be used to improve different aspects of clinical practice such as diagnostics and imaging. Examples mentioned include for instance, AI-aided diagnosis of diabetic retinopathy to avoid blindness,* identifying cardiac failure among patients with AI-enabled ECG algorithm for patients with dyspnea,** and enhancing MRI analysis in detecting breast cancer.*** Other applications could predict illnesses or major health events before they occur and are therefore used for prevention or disorders (e.g., suicide prediction,**** or the risk of cardiovascular disease, ***** epilepsy,****** etc.). Furthermore, AI applications are used as supporting clinical decision-making,******* such as aiding personalised COVID-19 treatment decisions, leading to a 50% reduction in COVID-19 mortality rates,******** and helping physicians to manage antiretroviral therapy by predicting resistance to HIV medicines and disease progression,********* as well as accelerating clinical research and the development of new medicines.********

* F. Ursin and others, ‘Diagnosing Diabetic Retinopathy with AI: What information should be included to ensure Ethical Informed Consent?’ Frontiers in Medicine July 2021, p 1–6.
Outside the clinical setting AI applications are being used – although in an early stage – for tracking infectious disease outbreaks and surveillance and forecasting epidemics.*

**Advantages**

These applications should improve the quality of patient care, more accurate diagnoses, more effective and efficient treatment (optimizing treatment plans), supporting pandemic surveillance and emergency response, as well as shortening the development process of new medicines and vaccines.

The advantages are promising but many applications are still in the early stages and are related to specific functions. AI is expected to be used more widely, either alone or in combination with other new technologies (eHealth, precision medicine, etc.).** When these expectations come true, AI could become ‘the new stethoscope of the 21st century’, a full-fledged health tool displacing the stethoscope as the symbol of health care.*** Perhaps exaggerated, but that the use of algorithms can lead to better decision-making in medicine is not controversial.

### 3. Human rights concerns

Apart from possible improvements, the use of AI in healthcare does raise several legal questions, especially from a human rights perspective. There are a number of concerns, including equal access to AI-based medical technologies. But it also affects the doctor-patient relationship, more specific the physician’s duty of inform patients about involving AI, as well as the level of information provided. Especially when AI systems become more autonomous and therefore more complex (the ‘black box’ problem), the question of their operation and possible risks becomes even more urgent. The call for professional standards and the potential risks of AI applications is then the next focus of attention. Liability issues may arise from the ‘many hands’ problem (the involvement of many actors and safety concerns, which makes it difficult to find a responsible person).**** Finally, AI applications may raise possible privacy issues when processing of big data.


The use of AI-applications in medical practice and health policy-making covers therefore a wide range of legal topics. Even more, legal analysis may urge the legislator to intervene and drafting new legal norms. Prior to that analysis, these technologies should comply basic human rights standards as confirmed in the Oviedo Convention. But what does that mean?

**Equal access**

Equal access to health care has been recognised as a human right on many occasions, including the Oviedo Convention (Article 3). The right to health for *everybody* imposes that Member States, irrespective of the healthcare system, must ensure a minimum level of healthcare services, accessible by the entire population without their suffering financial hardship. Or, as interpreted by the ICESCR General Comment on the right to health, ‘equitable healthcare not only requires availability for all, but also concerns the accessibility, acceptability and quality of healthcare services and goods’ (Article 12 ICESCR).* The AAAQ-approach under the ICESCR corresponds with the interpretation under Article 3 OC. This means that healthcare services should be available in sufficient quantity within the country, must be accessible to everybody without discrimination, that all health services should be respectful of medical ethics and cultural differences, and, finally, must be scientifically appropriate and of good quality.**

Non-discrimination means that AI applications should be available for all. But errors in AI algorithms or data may result in excluding certain patients from the best treatment option, thus undermining the non-discrimination principle. For instance, a predictive AI system developed to detect skin cancer based on exclusively white coloured patients’ data, may exclude other coloured patients from the best treatment.*** Individuals or vulnerable groups may therefore be adversely affected by errors in algorithmically informed decisions (racial data bias). Or clinical decision-support systems could stratify and select patients with certain diagnosis. Once it is learned that life-saving interventions with chronic diseases are always fatal and recommend non-treatment, it will exclude all patients although in specific cases it might be effective.**** Algorithm or data bias is already known from clinical trials and excluded groups (women or children, and thus generating different outcomes). Preventing such bias requires therefore better understanding

---


*** WHO guidance, note 2, p. 29.

who is developing the technology, generating the data sets, and who will benefit from it.

The AAAQ interpretation raises several questions: is it indeed a provision that falls under a minimum level of health care provision, and how is such a level defined? Clearly, essential medicines and emergency health care fall within the scope of minimum level of health care standard, but what about an AI-based breast cancer diagnostic device, or any other AI-based tool for screening and detecting purposes? Interpreted as necessary health care, that would depend on national criteria, meaning that low-income countries (LICs) may prioritise AI-based technologies differently as high-income countries (HICs). That is not different from other new technologies. It is therefore up to health policy makers to decide whether innovative technologies, including AI systems comply with the minimum level of health care services.

Besides a minimum level, the right to health aims at the highest level of health care, to be realised progressively. This means therefore a continuing obligation ‘to move as expeditiously and effectively as possible towards the full realisation of the right to health’. Ultimately, that would mean that States have to facilitate and provide AI technologies in health care.

Even then, the technology should respect all AAAQ criteria. Thus, apart from (geographical) availability, financial accessibility, AI technologies should comply the acceptability and quality criteria, triggering questions such as: is a particular AI application generally accepted among physicians, and of good quality, does it comply with the professional standards? Inherent to new medical technologies is the lack of evidence-based studies on proven efficacy, safety and efficiency. In most cases experimental technologies do not comply the so-called gold standard of evidence used in medicine. However, this does not preclude them from being recommended as diagnostics or treatment method, using differently graded levels of evidence. But alternative standards and little evidence may hamper to define AI-applications as good medical practice. In case AI does not (yet) comply the professional standards this will affect medical decision-making, including informing the patient.

**The doctor-patient relationship: information and informed consent**

The use of AI decision-making can help the diagnosis and treatment of disease. But is not without risks, as mentioned. Therefore, and also from an informed consent perspective, the physician should inform the patient when employing machine learning technologies for diagnostic purposes. Informed consent requires physicians to provide the best available evidence, and supporting patients being faced with making decisions. Making informed decisions requires the physician to inform the patient about the purpose and nature of the diagnosis, treatment options, possible risks and side-effects (Article 5 OC).

* M. Pot and others, ‘Not all biases are bad: equitable and inequitable biases in machine learning and radiology’ *Insights Imaging* 1(2021)13, cited by Hartlev, note 22.
Taking the right to information seriously, one may argue that the physician’s duty to inform also includes the use of AI driven diagnostics, when available. Such technologies should be in line with the patient’s preferences and values. Then, the question is whether physicians actually provide the patient with this information and to what extent. For example, should the patient be informed about the potential errors in predicting outcomes? Assuming there is an obligation to inform the patient using AI supportive systems, certain AI programmes are ‘black boxes’, with the health professional unable to understand and verify the algorithm’s predictive outcome, let alone explaining it to the patient. Then what would be the value of consent when the physician is unable to clarify the meaning of the predicted outcome and recommended treatment option? Knowing that the information ‘must be sufficiently clear and suitably worded for the person who is to undergo the intervention’,* which patient would trust the physician incapable the understand the AI functioning (including the method of collecting data, processing and labelling), and unable to inform about potential risks inherent to the nature of AI? Since autonomous machine learning algorithms are becoming increasingly incomprehensible, doctor’s awareness about the system’s risks will be more urgent, and thus the duty to alert the patient about such risks.

Valid patient consent requires first of all providing general information about the AI system (autonomous functioning or not), its use, predicted adequacy and control, and potential risks. Clearly one cannot expect the physician explaining all the technical details on AI functioning, but it should include ‘meaningful information’ about its functioning, the logic involved, as well as the consequences for the patient. As a general norm in order to make an adequate informed decision ‘AI technologies should be explainable to the extent possible and according to the capacity of those to whom the explanation is directed’.** Thus, the level of adequacy of information provided to patients may differ per case. Such an approach however is not much different from using other new technologies in health care.

Data privacy

Most AI systems in health care rely on health data derived from electronic health records, laboratory tests, research, insurance data, wearable health devices, etc. A key question is whether patient’s privacy is sufficiently protected when processing (i.e., collecting, recording, storage, use, disseminating) health data for AI purposes? Article 10 OC establishes a general right to privacy of information in health care, reaffirming that principle introduced in the European Convention on Human Rights (Art. 8 ECHR), Convention 108 on Automatic Processing of Personal Data, and reiterated in the EU General Data Protection Regulation (GDPR).

---

* Explanatory report (EXP), para 36 OC.
** WHO guidance, note 2, p. 27.
The GDPR includes the most advanced framework on data protection acknowledges several general principles to be respected when processing (e.g., storage of data, alteration, use, or dissemination) health data, such as the ‘data minimisation’ principle, i.e. collecting health data for research and treatment purposes (Art. 5 (1)(b), but limited to what is necessary to the purposes for which they are processed (Art. 5(1)(c)).* Moreover, the data should be accurate and, where necessary, kept up to date, meaning that ‘every reasonable step must be taken to ensure that personal data that are inaccurate, … are erased or rectified without delay’ (accuracy principle, Art. 5(1)(d). Also, the collected data will be no longer stored than necessary for research purposes (‘storage limitation’, Art 5(1)(e)). And finally, the processing system will ensure protection against unauthorised or unlawful access and against accidental loss (‘integrity and confidentiality’, Art. 5(1)(f)).

Apart from these general principles applicable, as a general rule, consent of the data subject is essential for the lawfulness of processing (Art. 6(1) (a)) and (Art.9(2)(a), including compliance with the conditions for consent (Art.7). However, in case the practitioner intends to use these data for research purposes, the patient’s explicit consent for processing such data is not necessary. The waiver meets practical objections to the consent requirement for conducting medical research. As long as appropriate safeguards such as anonimisation or pseudonymisation (reversible form of anonimisation) should ensure data minimization (Art. 89(1)). Nevertheless, data protection is not fully guaranteed. Interconnecting different data sets, especially in the case of genetic data sets, cannot exclude the risk of de-anonymisation.** Additional safeguards, e.g. the prohibition of re-identification, are then unavoidable. Such safeguards are not superfluous, especially since data subjects cannot exercise the right to information about the (purpose of) processing, rectification and erasure of personal data (Art. 15(1)(a)(e)). In case of processing big data, such safeguards would seriously impair the fulfilment of research purposes (Art. 89(2)).

The question of whether the processed data may also be used for follow-up research other than clinical research of the individual patient has been confirmed in Art 5(1)(b) GDPR. Therefore, collected data based on the physician-patient relationship, can be used for other scientific purposes (‘secondary use’).

But even in the case of prior consent, future research purposes are not always clear in advance. In that respect, presumed consent (‘broad consent’)

---


** E. Hayden, Privacy loophole found in genetic databases. DNA donors’ identities can be determined from publicly available records. Nature News, 17 January 2013; M. Gymrek, Identifying personal genomes by surname inference, Science (2013) Jan 18;339(6117):321-4; interconnecting of medical databases with other data systems (e.g., on insurance coverage) and AI algorithms may support to detect health care fraud, see note 4, p. 5.
for related medical research can be a solution, instead of explicit consent for each new research.

Further international cooperation between hospitals and research institutes can also lead to the exchange of health data derived from patients’ electronic health records. This cross-border transfer of health data will become even more relevant when using AI-based datasets for clinical decision-support or research purposes (e.g., rare diseases). Apart from the cross-border flows of health data within EU member states, the GDPR also applies the transfer to third countries or international organisations (Art. 44). A key principle is that the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, and such transfers may only be carried out in full compliance with this Regulation. It is therefore essential that the controller can ensure that appropriate safeguards protecting the data subject rights in a third country are available and that effective legal remedies are available (Art. 46).

Besides the importance of the continuity of scientific research, public health can also justify an exception to the processing of personal health data without the consent of the patient/data subject. Such an exception falls under the ‘task carried out in the public interest or in the exercise of official authority vested in the controller’ (Art.6(1)(e) and Art 9(2)(i) GDPR, such as the public health monitoring and surveillance of pandemic diseases, carried out by Public Health authorities. AI-powered surveillance of public health data could be a valuable public health instrument, monitoring the spread of Covid-19, and even identifying infected patients (by facial recognition and gps mapping). But AI surveillance tracking health data to predict the outbreak, may violate privacy. Finding a workable solution requires therefore the balancing of both the public and individual interest, taking into account the above-mentioned principles.

**Security of personal data**

Data security is a key element in protecting personal data in health care. Cyberattacks on hospitals or other health care institutions may seriously threaten the patient care and data protection. Cybersecurity incidents may include the deployed the ransomware into the organization’s IT-system.* Computer systems will be locked up and patient files may not be accessible.**


** C. Cimpanu, First death reported following a ransomware attack on a German hospital, ZD https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/
Such attacks may also involve AI systems, corrupting data and infecting algorithms, leading to incorrect and unsafe treatment recommendations.* Other data breaches include the unlawful loss or alteration, or unauthorised disclosure of, or access to, patient data stored and require proper measures to mitigate these risks. These measures should ensure ‘an appropriate level of security’, taking into account the state of the art and the costs of implementation in relation to the risks and likelihood of breaching patients’ rights’ (Art. 32(1) GDPR). Health care institutions should therefore implement both technical and organisational measures (pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and periodical review of the security system’s effectiveness in ensuring processing).

Data protection impact assessment

Finally, prior to the processing, health care providers (the controller) will likely have to carry out a data protection impact assessment for new AI applications (Art. 35 GDPR). Such an assessment examines the impact of the envisaged processing on the protection of personal (genetic) data (section 2), and covers several elements, including (i) a description of the processing activities, and its purpose (ii) reviewing the necessity and proportionality of the processing operations in relation to the purposes; (iii) the risks to the rights and freedoms of data subjects involved, as well as (iv) the security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR (Art. 35(7)).

Liability issues

The use of AI applications in health care may, similar to other medical technologies, raise some liability issues. For instance, liability may arise in case of diagnosis or treatment errors suggested by using machine learning in complex medical cases. This may create professional liability since the physician is responsible for using supportive decision-making systems. Alternatively, or in addition, errors in diagnosis or treatment options may create product liability of the manufacturer for a defective product, assuming that AI applications (software and algorithms) can be considered as a product.** Such AI-based medical devices are subject to both EU product liability rules, the new

---


** In more detail, see S. Palmieri and others, Inevitable Influences: AI-based Medical Devices at the Intersection of Medical Devices Regulation and the Proposal for AI Regulation, *EJHL* (2021) 341–358.
Medical Devices Regulation (MDR) and the proposed AI regulation (AIR).* As a consequence, the Regulation’s safety requirements are applicable (risk management measures, adequate transparency rules and information to users, etc.). Other liabilities may arise from breaches of processing AI-based health datasets, causing data leaks, or corrupted data which may harm patient care.

Despite existing EU and national liability frameworks, it has been questioned whether this is sufficient to compensate for damages caused by new technologies, such as AI.** For instance, getting compensation for damage caused by autonomous AI applications may become problematic, as the algorithm’s functioning is difficult to understand, its limited predictability, and vulnerability to cybersecurity threats. These, and other new obstacles may hinder the victim to make a liability claim. Given the different risks posed by AI, legal experts have recommended several adjustments to EU and national liability regimes.***

4. How to address these concerns

Alongside the obvious benefits of AI applications in healthcare, there are questions regarding the safeguarding of patients’ rights. Some of these questions are new and may or may not be covered by existing human rights treaties. Additional regulation would then be necessary precisely because it concerns the guarantee of essential human rights. On the other hand, there are also calls for a new legally binding framework on AI inspired by the EU draft Regulation on AI,**** or even a separate Convention on AI.***** Whatever the exact design will be (Additional Protocol, Convention or even non-legally binding guidelines), such a set of human rights standards should cover the issues mentioned above. In this respect, a valuable initiative is the draft legal framework on artificial intelligence the CoE ad hoc committee on artificial intelligence (CAHAI) incorporating the human rights elements, to be complemented with health care specific principles and rights.******

**** European Commission, note 32.
****** Ibid.
In the health care setting newly defined AI rules should address the following rights:

– guaranteeing a high level of health care services for all, has confirmed by Article 3 OC. The potential risk of algorithmic bias or excluding certain patients from the best treatment option, has been covered already by the non-discrimination principle. It has been emphasized that a better understanding of generating datasets and who will benefit from it may prevent such bias or exclusion. Safeguarding non-discrimination will foster human dignity, the core human right.

Defining the nature and scope of health care services – and thus incorporating AI applications in the health services package – however, remains an issue to be decided by individual Member States, as long as a minimum level of essential health services is covered, and the concept of progressive realization will be respected. That margin of appreciation has been confirmed both in the Explanatory Report* and by the ECtHR's jurisprudence of positive state obligations under the ECHR.** Affirming the right to equal access to health care as accepted under international law could therefore acknowledge its relevance to AI technologies in health care.

– Respecting the right to information and informed consent are also well-established rules under international health law protecting the patient’s autonomy. Information about the use of AI decision support systems is therefore part of the doctor’s duty, as concluded before. International law, and the Oviedo Convention in particular, set some general rules on providing ‘appropriate information on the purpose and nature of the intervention, as well as the consequences and risks’ (Article 5 OC). This includes basic information on the use and functioning of the AI diagnostic devices, supporting medical decision-making.

The argument that the use of AI applications can be regarded as routine interventions, and therefore implied consent would be sufficient, seems untenable. After all, it concerns a new (possibly experimental) technology of which not all risks and potential benefits are known. Explicit consent is therefore more likely, which corresponds with the Oviedo interpretation on informed consent and emerging risks.***

– The processing of AI generated health data has been widely protected under international law, including the GDPR. For instance, for research purposes, collected data based on the physician-patient relationship can be used for other scientific purposes (‘secondary use’), as confirmed by the public interest waiver under Article 9(2)(g)(j) GDPR waiver. Explicit consent of the patient is therefore not necessary when the patient’s privacy is respected.

* EXP, para 27 OC.
** E.g., Sentges v. the Netherlands, no. 27677/02 (ECtHR, 8 July 2003); Pentiacova and Others v. Moldova, no. 14462/03 (ECHR 4 January 2005); McDonald v United Kingdom, no. 4241/12 (ECtHR, 20 August 2014).
*** Exp. para 37.
But what if the scientific purposes are not known in advance? Will the waiver then be sufficient?

For new research purposes ‘broad consent’ for processing data has been suggested as a more practical solution. Broad consent is specific to genomic research, in which the research subject will be asked for consent only once. The subject’s consent concerns the extraction of biological data, storage and future use of unspecified research purposes.* It has been argued that broad consent complies the GDPR waiver under EU law** but under the Oviedo Convention such an unconditional waiver is unlikely since it is not mentioned in the Convention, nor the explanatory report. Renewed consent for future use (i.e., storage and research) of AI-based data is therefore required. Given the large quantities of health data and data subjects involved that may seriously impair research purposes. For that reason, introducing broad consent for achieving future research purposes would be legitimized.

What remains is the risk of de-anonymization by linking multiple datasets. Particularly genomic information pooled in different datasets is sensitive to re-identification of individuals. In that respect, additional measures should ensure the patient’s privacy and prevent possible breaches of confidentiality. One of these measures could be the introduction of a so-called non-reidentification clause to protect health data. A similar approach has applied in genetic research, authorizing researchers to access data when respecting the institution’s basic terms and conditions such as the use of health data in research.*** The introduction of similar access rules or codes of conducts to AI-based health data could ensure anonymity.

– Ensuring the right to private life (Article 10 OC) requires adequate data security measures to prevent the disclosure of health data to unauthorised persons. That approach has been confirmed by other Council of Europe treaty documents such as Convention 108 protecting patients’ health data undergoing automated processing Convention 108, Additional Protocol 223 and the ECtHR’s jurisprudence on protecting health data.****

AI health systems are not an exception and may also be vulnerable to data breaches and cyberattacks, threatening the patient’s health. The Oviedo Convention’s Explanatory Report already refers to Convention 108 requiring

---

* D. Hallinan, Broad consent under the GDPR: an optimistic perspective on a bright future, Life Sciences, Society and Policy (2020), 1–18, at p. 3.
** Ibid Hallinan.
**** Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223); I. v. Finland, no. 20511/03, (ECtHR, 17 July 2008); L.L. v. France, no. 7508/02 (ECHR, 12 February 2007), and L.H. v. Latvia, no. 52019/07 (ECtHR, 29 July 2014).
Member States to comply to the Convention’s basic principles (e.g., basic duties, ensuring quality of data, data security and additional safeguards).* In addition, Additional Protocol 223 extends the scope to specific (genetic) data and creates several new rights in AI decision-making (e.g., the right to challenge a decision who may be subject to a purely automated decision, and to know the reasoning underlying the processing of data, including the consequences of such a reasoning, Article 9).

At the same time, the Cybercrime Convention harmonises criminal rules combatting cybercrime and to protect data-driven technologies including AI systems.** Applying the Conventions’ principles will contribute to counter the threats posed by cybercrime in the health care setting.

– Although the Oviedo Convention does not set any norms on harmonising national liability regimes, AI causes major challenges for existing liability frameworks. For instance, the ‘many hands’ involved and increased autonomous operation due to machine learning capabilities make it difficult to identify who is responsible for using the AI-system and what caused the harmful operation, the risk of biased decision-making, as well as the connectivity with other non-AI (e-health) systems, and its dependency on external data. Defining additional rules adjusting existing civil liability regimes should therefore be considered providing citizens the same level of protection and rights. At EU level, such an initiative has resulted in a draft Regulation on liability for the operation of AI-systems.*** It focuses on claims against the operator of an AI-system, who exercises a degree of control over the risk connected with the operation and functioning of an AI-system (Article 4). This set of common European standards aims at preventing ‘regulatory fragmentation’, to strengthen patients’ confidence in AI technologies in health care, and as such contribute to acceptability of AI innovations in health care.****

5. Conclusions

One of the key issues of AI in health care is about trust: a fundamental aspect in the patient-doctor relationship. Can the physician rely on the accuracy and quality of AI-driven medical technologies? But also, will patients accept the use of such technologies in medical decision-making? That requires first of all clarity about the functioning of AI-based technologies, and potential risks involved. Physicians should therefore have some understanding of the algorithm predictive understanding, to inform the patient. Patient’s trust starts with awareness of potential risks and basic knowledge on AI applications in health care.

* Explanatory Report OC, Art. 10.
** Convention on Cybercrime ETS 185, Budapest, 23.XI.2001 and Additional Protocols.
*** Draft AI Act, note 32.
**** Ibid, par 8, 20.
Awareness on the use of AI applications in healthcare is reflected by the information requirement under the Oviedo Convention. Moreover, the explanation provided should include meaningful information about its functioning, and the consequences for the patient. What that means, may differ by patient. But such an approach is not different from using other new technologies in health care. In this respect, revision of the Convention is therefore not necessary.

But regarding the processing of health data, the Oviedo standard of explicit consent should be reconsidered, introducing broad consent for future use of unspecified research purposes. Otherwise, the large volumes of health data and data subjects involved may seriously impair research purposes.

Finally, to prevent unauthorised disclosure of health data, the existing legal framework seems adequate, given the Cybercrime Convention protecting AI data-driven systems.

As a result, the adequacy and the completeness of the Oviedo legal system in the light of AI challenges in health care has been largely confirmed. What remains is then ratifying and implementing the Convention and related treaties, protecting the rights of patients.

Andre den Exter
magistr prawo, doktor filozofii,
Uniwersytet Erasma Rotterdama/
Naționalna škola gromadskogo zдорov’ja Lisabona
https://orcid ID: 0000-0002-0938-6603
email: denexter@law.eur.nl

Штучний інтелект в охороні здоров’я та Конвенція Ов'єдо

Технології штучного інтелекту (ШІ) стрімко розвиваються у сфері охорони здоров’я. Перспективи розгортання цільових застосувань ШІ в лікуванні, клінічних випробуваннях, дослідженнях лікарських засобів і громадському здоров’ї є багатообіцяючими і революційними.

Упровадження цих нових технологій в охороні здоров’я породжує низку правових питань, особливо з точки зору прав людини. Автор публікації зосередив увагу на аналізі прав людини при застосуванні ШІ в охороні здоров’я і на тому, як ці застосування пов’язані з Конвенцією Ов’єдо.

Ключові слова: штучний інтелект, права пацієнтів, Конвенція Ов’єдо.

Стаття надійшла до редакції 21.06.2022
Прийнята до друку 10.07.2022