radiation

MDPI

Review

Legal and Regulatory Framework for AI Solutions in Healthcare in EU, US, China, and Russia: New Scenarios after a Pandemic

Filippo Pesapane [1,*], Daniele Alberto Bracchi [2], Janice F. Mulligan [3], Alexander Linnikov [4], Oleg Maslennikov [5], Maria Beatrice Lanzavecchia [6], Priyan Tantrige [7], Alessandro Stasolla [8], Pierpaolo Biondetti [9,10], Pier Filippo Giuggioli [2], Enrico Cassano [1] and Gianpaolo Carrafiello [9,10]

[1] Breast Imaging Division, IEO European Institute of Oncology IRCCS, 20141 Milan, Italy; enrico.cassano@ieo.it
[2] Agnoli e Giuggioli Law Firm, University of Milan, 20122 Milan, Italy; daniele.bracchi@unimi.it (D.A.B.); pier.giuggioli@unimi.it (P.F.G.)
[3] California Law Firm of Mulligan, Banham & Findley, San Diego, CA 92101, USA; mulligan@janmulligan.com
[4] Department of World Economy and International Business of the Faculty of International Economic Relations, Financial University under the Government of the Russian Federation, 123112 Moscow, Russia; ASLinnikov@fa.ru
[5] Information Technology and Digital Economy Department, Ivanovo State University of Chemistry and Technology, 153000 Ivanovo, Russia; olegmaslennikov@yandex.ru
[6] Isolabella Law Firm, 20122 Milan, Italy; mariabeatrice.lanzavecchia@studioisolabella.it
[7] Interventional Radiology, King's College Hospital NHS Foundation Trust, London SE5 9RS, UK; priyan.tantrige@gmail.com
[8] UOC Neuroradiologia Diagnostica ed Interventistica, A.O.S. Camillo Forlanini, 00152 Rome, Italy; alestaso@tiscali.it
[9] Diagnostic and Interventional Radiology Department, Fondazione IRCCS Ca Granda—Ospedale Maggiore Policlinico, 20122 Milan, Italy; pierpaolo.biondetti@unimi.it (P.B.); gianpaolo.carrafiello@unimi.it (G.C.)
[10] Department of Health Sciences, University of Milan, 20122 Milan, Italy
[*] Correspondence: filippo.pesapane@ieo.it; Tel.: +39-02-52774632

check for updates

Citation: Pesapane, F.; Bracchi, D.A.; Mulligan, J.F.; Linnikov, A.; Maslennikov, O.; Lanzavecchia, M.B.; Tantrige, P.; Stasolla, A.; Biondetti, P.; Giuggioli, P.F.; et al. Legal and Regulatory Framework for AI Solutions in Healthcare in EU, US, China, and Russia: New Scenarios after a Pandemic. *Radiation* **2021**, *1*, 261–276. https://doi.org/10.3390/radiation1040022

Academic Editor: Gabriele Multhoff

Received: 9 August 2021
Accepted: 11 October 2021
Published: 15 October 2021

Simple Summary: We offer an overview of the state of regulation of AI in healthcare in the European Union, the United States of America, the China, and the Russian Federation and future strategies to make AI applications safe and useful.

Abstract: The COVID-19 crisis has exposed some of the most pressing challenges affecting healthcare and highlighted the benefits that robust integration of digital and AI technologies in the healthcare setting may bring. Although medical solutions based on AI are growing rapidly, regulatory issues and policy initiatives including ownership and control of data, data sharing, privacy protection, telemedicine, and accountability need to be carefully and continually addressed as AI research requires robust and ethical guidelines, demanding an update of the legal and regulatory framework all over the world. Several recently proposed regulatory frameworks provide a solid foundation but do not address a number of issues that may prevent algorithms from being fully trusted. A global effort is needed for an open, mature conversation about the best possible way to guard against and mitigate possible harms to realize the potential of AI across health systems in a respectful and ethical way. This conversation must include national and international policymakers, physicians, digital health and machine learning leaders from industry and academia. If this is done properly and in a timely fashion, the potential of AI in healthcare will be realized.

Keywords: artificial intelligence; policy; ethics; healthcare; regulation; accountability; telemedicine; data protection

1. Development in Healthcare Scenarios during and after COVID-19 Pandemic

The coronavirus disease (COVID-19) and its pressure on the healthcare system is happening at a time of technological optimism and promise. The digitalization of health data, together with the advent of artificial intelligence (AI) solutions, have the potential to completely change the current pattern of the healthcare scenario and provide precise and predictive medical assessment for individuals in the future [1,2].

The new frontiers of research made possible by AI algorithms based on machine learning (ML) and deep learning (DL) give the technological possibility of using aggregated healthcare data to produce models that enable a true precision approach to medicine [3–8]. Such innovation may facilitate and improve the accuracy of diagnosis, tailoring treatments and targeting resources with maximum effectiveness in a timely and dynamic manner [7–11].

However, such innovative technology must be robust enough to avoid biased learning, which can happen when training datasets are too skewed, too small, and/or poorly annotated. This issue demands a global effort in the field of cross-disciplinary, international agreements for standardization, anonymization, validation, and data sharing. Moreover, it calls for continuous monitoring, starting from appropriate legal and regulatory policies to be shared among different countries and different health systems.

In the last two years, new technologies such as AI proved helpful in the management of the COVID-19 pandemic [12–18]. During the first months of 2020, chest computed-tomography scans showed the extent of lung damage caused by COVID-19; accordingly, efforts were established around the world to facilitate data sharing, model training, and scan assessment [10,15]. In Europe, 30 international partners created the Imaging COVID-19 AI, which provided an automated quantitative analysis of COVID-19 based on imaging [16].

Similarly, telemedicine has boomed. Many telemedicine platforms made their services available for free, including Doctolib in France, Kry in Sweden, and Adent Health in Denmark. Push Doctor, a company in the United Kingdom (U.K.) that has partnered with the National Health System (NHS), claimed in March that usage of their product had increased by 70% [19]. Moreover, NHS England recommended general practitioners to change face-to-face appointments to telephone or video appointments in March 2020 [20]. Regulation in telemedicine was also updated: the French government and German health insurance companies removed reimbursement restrictions on video consultations, and in the United States of America (U.S.), Medicare expanded its coverage to include telemedicine [19]. The British Medicine and Healthcare Products Regulatory Agency authorized fast-track approval of medical devices during the outbreak, and the Food and Drug Administration (FDA) in the U.S. stated that it did not intend to enforce requirements for certain lower risk device software functions, including symptom checkers [21]. Telemedicine advancements in the U.S. are discussed in a specific section below.

In many cases, such quick and wide response has already provided beneficial support, but at the same time, there have been some warning signs. Predictive models for COVID-19 are at high risk of bias, mostly due to nonrepresentative sample selection; when tested on a different, larger sample, their accuracy could decrease significantly [22]. Moreover, there have been concerns that some tools, particularly those used for location and contact tracing, may compromise personal privacy [1,23].

With different roles and competences, every healthcare stakeholder necessarily must evaluate and implement AI with a critical eye, keeping in mind current AI limitations—not only technical but even ethical limitations, such as the concern that AI algorithms may mirror human biases in decision making [1]. Since healthcare delivery may depend by ethnicity, some ethnic biases could inadvertently be built into healthcare algorithms. The intent behind the design of AI also needs to be considered, because some devices can be programmed to perform in unethical ways (i.e., to guide users toward clinical actions that would generate increased profits for their sellers by recommending specific tests or drugs) and not necessarily reflect better care [24]. The progress made in regard to AI and digital healthcare in a matter of months could have, under other circumstances, taken several years. Accordingly, it is even more important than ever to monitor advances carefully, to ensure that patients receive the best possible care, and to earn the trust of both the clinical community and patients. Avoiding missteps at this time is essential not just for the management of the pandemic, but to ensure the credibility and the future of digital AI-powered healthcare.

In this scenario, the issues showed in this paper acquire particular importance and urgency. They display the complexity of AI-based healthcare and highlight the need to develop policies and legal strategies that carefully consider the multiple dimensions of the integration process, and this need for multidisciplinary efforts to coordinate, validate and monitor the development and integration of AI tools in the healthcare [19]. Challenges such as organizational and technical barriers for health data use, the debate about the ownership of data and privacy protection, the regulation of data sharing and cybersecurity surrounding it, and accountability issues will have to be addressed as soon as possible.

This paper explores the status of legal and regulatory frameworks for healthcare AI in the European Union (EU), the U.S., China, and the Russian Federation, analyzing challenges, hurdles, and opportunities. The results are particularly significant, as the COVID-19 pandemic is triggering an unprecedented surge in the development of and demand for digital and AI technologies worldwide.

2. Organizational and Technical Barriers for the Adoption of AI in the Medical Field

Both ML and DL technologies require the availability of large amounts of comprehensive, verifiable datasets; integration into clinical workflows; and compliance with regulatory frameworks [1,23]. With improved global connectivity via the internet and cloud-based technologies, data access and distribution have become easier, with both beneficial and malicious outcomes [25]. Adequately regulated integration of health data and disease will provide unprecedented opportunities in the management of medical information at the interface of patients, physicians, hospitals, policymakers, and regulatory institutions. However, despite the pervasive enthusiasm about the potential of AI-based healthcare, there are only a few healthcare organizations with the data infrastructure required to collect the sensitive data needed to train AI algorithms for patients [26]. Consequently, published AI success stories fit the local population and/or the local practice patterns centered on these organizations and should not be expected to be directly applicable to other cohorts [27] (i.e., an AI algorithm trained on one specific population is not expected to have the same accuracy when applied elsewhere) [28].

3. Telehealth: A Boon Redefining Medicine for the 21st Century or a Short-Term Fix during the COVID-19 Pandemic?

Telehealth (or telemedicine as it is sometimes called) is literally “healing at a distance”, with the provider in one location and the patient somewhere else [29]. Although the concept of telemedicine has existed for decades, developments in technology galvanized the ability to provide this service on a large-scale basis. In the U.S., historically, the largest hurdles to universal adoption of telehealth were twofold: first, insurance reimbursement was lacking; and second, the intricate and inconsistent web of state laws barred out-of-state doctors from practicing medicine across state lines.

With one fell swoop, the COVID-19 pandemic temporarily chipped away at these barriers. The U.S. Congress enacted legislation allowing the U.S. Department of Health and Human Services to issue waivers for telemedicine under Section 1135 of the Social Security Act. Additionally, former President D. Trump issued a Proclamation Declaring a National Emergency Concerning the Novel Coronavirus Disease Outbreak under the U.S. National Emergencies Act. The Emergency Proclamation authorizes HHS to offer additional waivers designed to increase providers’ ability to treat the anticipated influx of ill patients.

The U.S. Centers for Medicare and Medicaid Services (CMS) now allows Medicare to cover telehealth visits and pay for such visits at the same rates as traditional, in-person visits. Private health insurance carriers quickly followed suit.

This waiver had a profound effect on the delivery of telehealth services in the U.S. University of California, San Diego Health (UCSDH), for example, had a long history of performing telemedicine on a limited basis before the pandemic. Its telemedicine infrastructure provided care to other remote centers for telestroke and telepsychiatry, amounting to up to 15 service lines in the past ten years. Through a small-scale pilot project, UCSDH provided 870 ambulatory home telemedicine video visits over the course of three years. Because this foundation, though limited in scope, was in place, when the waivers for telemedicine were issued, UCSDH was able to leverage its experience to quickly provide wide telemedicine services during the pandemic. Over a 5-month period, UCSDH conducted over 119,500 ambulatory telemedicine evaluations (a remarkable increase from the pre-COVID-19 waiver period) [30].

The CMS also issued several nationwide blanket emergency waivers available throughout the duration of the pandemic, including a waiver of federal regulation 42 CFR 485.608(d), which required that critical access hospital staff (CAH) be certified in accordance with federal, state, and local laws and regulations. Under this waiver, out-of-state providers need no longer be in the same state as the patients to whom they provide telehealth services—if permitted by state law [31].

Each state has its own laws governing telemedicine, and the state in which the patient is located controls whether an out-of-state doctor must be licensed in that state at the time of the telehealth visit. While 40 states have issued waivers modifying their licensure requirements for telehealth visits by out-of-state physicians, the waivers are only effective during the pandemic [32].

Forty-nine state boards still require physicians engaging in telemedicine to be licensed in the state in which the patient is located [33]. One potential solution was advanced by the Interstate Medical Licensure Compact Commission (IMLCC). The IMLCC has an expedited pathway to licensure for qualified physicians seeking to obtain multiple licenses. Twenty-four states, Guam, and the District of Columbia enacted legislation to join the Compact. Still, with fewer than half of the states belonging to the Compact, there is still a long way to go for a permanent fix to this problem. While penalties vary from state to state, there are significant civil, professional, and even criminal licensure consequences for violating state telemedicine laws.

Several other challenges also remain with the delivery of telemedicine services in the U.S. Telemedicine is widening the existing gap in access to care. One recent study found that patients over 65 years old have the lowest odds of using telemedicine services, and that Black and Hispanic patients have lower odds of using these services than their White or Asian counterparts [34]. Additional concerns remain involving patient privacy. The HHS has waived penalties against providers that fail to comply with many of the U.S. HIPAA Privacy Rules until the Emergency Proclamation is rescinded, i.e., throughout the pandemic [35].

While we may be awed by technological advancements that allow for more medical services to be delivered remotely, long after the pandemic is over, Americans will continue to be challenged by the legal issues raised by telemedicine. The biggest impediment may be a real belief by state medical associations that telemedicine might adversely affect doctor incomes by allowing out-of-state providers to compete, resulting in continued rules restricting this highly efficient method of delivering medical services.

4. Regulatory Issues and Policy Initiatives

In the last few years, governments have started to promote data sharing [36]. For instance, anonymized benchmarking datasets with annotated diagnoses have been created to provide reference standards [37,38]. Existing examples of data-sharing efforts include biobanks and international consortia for medical imaging databases, such as the Cancer Imaging Archive (TCIA) [39], the Visual Concept Extraction Challenge in Radiology Project [40], the Cardiac Atlas Project [41], the U.K. Biobank [42], and the Kaggle Data Science Bowl [25], the latter of which represents a valuable step in the direction of an open-access database of anonymized medical images coupled with histology, clinical history, and genomic signatures.

Despite those hopeful examples, the amount of data sharing required for widespread adoption of AI technologies across different health systems demands still more efforts. It will probably depend more on the socioeconomic context of the health system in question rather than on technology itself, which has already been showed to be available and ready.

Once AI in healthcare is fully institutionalized and its rules are defined, it may be difficult to change those rules. To prevent this, state regulation and supervision should remain flexible and proactive [26].

The role of the government in the legal discipline of AI-based medical systems must manifest itself in the following activities:

- securing patients' medical privacy;
- creating regulatory sandboxes and experimental legal regimes;
- supervising medical organizations that use AI-based medical solutions;
- certifying software engineers for development of such systems;
- certifying AI-based medical systems and confirming their quality and effectiveness;
- avoiding uniformity in the process of AI-based medical systems development;
- providing state funding in the form of grants, subsidies, etc.

4.1. Legal and Regulatory Framework in EU

The "Medical Device Regulation" (MDR) should have been initially applied starting from 26 May 2020, but on 23 April 2020, the EU Council and the EU Parliament postponed the date of application for most of the MDR's provisions by one year, until 26 May 2021. On the other hand, the "In Vitro Diagnostic Medical Device Regulation" (IVDR) will apply, as initially provided, starting from 26 May 2022 [43].

The MDR and IVDR do not substantially impact the purposes of previous sets of EU laws. First, like the previous Directives [44,45], the new Regulations aim to:

- harmonize the single market by granting uniform standards for the quality and safety of medical devices;
- classify medical devices and in vitro diagnostics based on the relevant risk profiles by requiring different, specific assessment procedures in relation to such classifications;
- highlight responsibilities of notified bodies and competent authorities.

The main reasons behind the regulatory change consisted of divergent interpretations of the previous Directives [44,45], incidents concerning product performance, and lack of control of notified bodies. Thus, the legislation's revision was required to reach high standards of product quality and safety concerning evolving technologies, including AI, and to reconsolidate the EU's leading role in the medical-devices field [37]. The new Regulations should ensure a consistently high level of health protection and safety for EU citizens using AI-based products; the free and fair trade of the products throughout the EU; and the adaptation of EU legislation to the significant technological and scientific progress in the AI-based medical device sector over the last 20 years [43].

The scope of the new legislation includes a wider range of products, extends liability in relation to defective products, strengthens the requirements for clinical data and traceability of devices, increases clinical investigation requirements and manages risk to ensure patient safety, reinforces surveillance and management of medical devices as well as the lifecycle of in vitro diagnostic medical devices, and, finally, improves transparency relating to the use of personal data.

According to the new legislation, a software, whether as a component in a wider medical device or standing alone, is qualified as a medical device without any other specifics.

Starting from 24 May 2018, the General Data Protection Regulation (GDPR) applied in the EU. This new legislation is a suitable instrument to regulate AI because it has an extended territorial scope and wide rights for data subjects, providing, overall, more rights to citizens vis-à-vis information about the use of their personal data and giving clear responsibilities to people and entities using personal data [23,46,47].

The GDPR established rules to strengthen citizens' rights as regards the process of consent to the collection, use, and sharing of their personal data [23]. The regulation explained that consent must be explicit and unambiguous, and that data controllers must demonstrate that a person has given consent (in other words, the burden of the proof is with them). Consent must be informed, which it means it has to be demanded in intelligible and easily accessible forms using clear and plain language. In addition, patients should be informed on how to withdraw consent prior to giving it.

Under the GDPR, patients have the right to access their own medical records and health data when they are being processed (i.e., with remote access). However, the GDPR does not make clear that access must be provided for free and even allows data controllers to charge a fee for administrative costs if data subjects ask for the data more than once [23].

4.2. Legal and Regulatory Framework in the U.S.

In the U.S., the 21st Century Cures Act [48] of 2016 defined the medical device as a tool "intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals" [49].

The FDA categorizes medical devices into three classes according to their use and risk (the higher the risk, the stricter the control) and regulates them accordingly.

The black box nature of AI applications will make it difficult for the FDA to approve all the new medical devices that are quickly being developed, given the volume of innovation and the complex nature of the testing and verification involved. For instance, the introduction of computer-assisted detection (CAD) software for mammography [49] required many years and extensive lobbying to obtain clearance from the FDA to be used as a second screening reader [50]. FDA clearance is even harder to obtain for an AI system that does not need humans' supervision and cannot be compared to predicated medical devices used as replacement for radiologists. Therefore, AI systems are usually presented today as merely support for physicians rather than as tools that substitute them [7,51–54].

The FDA and the International Medical Device Regulators Forum (IMDRF) recently assessed that AI technologies are different from traditional medical devices. The IMDRF is a voluntary group of medical device regulators including the EU, the U.S., Canada, Australia, Brazil, China, Japan, Russia, Singapore, and South Korea that works toward harmonizing international medical device regulation. The collaboration between IMDRF and the FDA defined a new category called "Software as Medical Device" (SaMD), pointing out for the need for an updated regulatory framework [25,54] that considers that AI systems must face safety challenges in the forms of complex environments, i.e., periods of learning (during which the system's behavior may be unpredictable) that may result in significant variation in the system's performance [54]. These organizations recommended a continuous iterative process based on real-world performance data and stated that low-risk SaMDs may not require independent review [25].

According to Thierer et al. [55], there are two main approaches to regulating new technologies. The "precautionary approach" gives some limits (or sometimes outright bans) to certain applications because of their potential risks: this means that these systems are never tested because of what could happen in the worst-case scenarios. On the contrary, the "permission-less innovation approach" allows experimentation to proceed freely; the issues that do arise are addressed as they emerge.

4.3. Legal and Regulatory Framework in China

Although COVID-19 has accelerated ongoing digital healthcare trends, in China, the regulation of AI is still developing [56].

China's regulatory body for life sciences products, the National Medical Product Administration (NMPA), certifies that products meet the requisite standards. However, once market approvals are granted, there is low control because of the continuous nature of software development and because software updates can so readily be pushed out to the public/market. For AI products that change second-to-second as the product adapts to a variety of inputs, the challenge is even more urgent.

Nevertheless, with a number of recent announcements and guidelines over the past few years, the NMPA has demonstrated a maturing approach [57].

The role of the NMPA Legal Agent, the key contact for the NMPA for each registered device, has correspondingly increased in importance. Like the EU and U.S., China requires a local entity before market clearance applications are accepted, but this need not be the manufacturer itself. A local distributor (that thereby tends to gain inordinate power over the foreign manufacturer) or a third-party service provider may also perform this role [56].

The NMPA has issued various guidelines relating to AI in catchup to the FDA, which approved an AI-based diabetes-related device in 2018. Furthermore, the NMPA issued in 2019 the "Technical Guideline on AI-Aided Software", in which it clarified that for AI software, version naming rules should cover algorithm-driven and data-driven software updates and should list all typical scenarios for major software updates [57].

For AI devices, the NMPA recognized that the risk-based method is the guiding principle in determining whether and when a product change needs to be filed.

Therefore, whether AI device updates require product change approval depends on statistical significance. Where the software maintains its effect based on the original application, there is no need to obtain preapproval.

In China, the following fast track pathways are available [56]:

- innovative approval;
- priority approval;
- emergency approval.

Innovative approval has a number of criteria to be satisfied, most relevantly that the product has significant clinical application value and a national patent and that no other similar products are already present on the market [56].

Priority review relates to treatment of rare diseases using devices with significant application value.

Emergency approvals are for public health crises, which was relevant in 2020 to face the COVID-19 pandemic, but such applications were no longer accepted in 2021.

4.4. Legal and Regulatory Framework in the Russian Federation

In the Russian Federation, the government has taken on the role of an observer and does not outrace developers with supervisory and regulatory measures. Striving instead to form an institutional basis for a wide range of AI development and application, Russia keeps up with the creation of different strategies, roadmaps, and standards. These documents have a defined, hierarchical structure. The National Program "Digital Economy of the Russian Federation" [58] consists of a description of the main directions, tasks, and goals for the development of the digital economy, and AI is mentioned in this document solely in the context of regulation and lawmaking.

The Decree of the President of the Russian Federation of 9 May 2017, 203, "On the Strategy for the Information Society Development in the Russian Federation for 2017–2030" [59] proclaimed the necessity and importance of intensification in the field of digital technologies, including AI. The Decree of the President of the Russian Federation of 10 October 2019, No. 490, "On the Development of Artificial Intelligence in the Russian Federation", together with the "National Strategy for the Artificial Intelligence Development" for the period up to 2030 [60], listed a number of AI solutions in healthcare, such as the creation of prediction models, reduction of risks and negative effects of pandemics, preventive screening, diagnostics based on medical images, automation, and increasing accuracy and effectiveness of physisicians.

In the Federal Law No 323-FZ of 21 November 2011, "On the Fundamentals of Healthcare in the Russian Federation", a "medical device" was defined as "any tools, equipment, devices, materials and other products used for medical purposes, necessary accessories and software" (article 38) [61]. Therefore, any AI solution, used independently or in combination with other medical devices, must be registered as a medical device, passing through clinical testing and acceptance according to article 36.1 of said Federal Law. The Russian supervisory authority—the Federal Service for Supervision of Healthcare

(Roszdravnadzor)—requires technical and clinical tests as well as examination of the safety, quality, and effectiveness of all medical devices prior to their use and sale.

Moreover, according to the Federal Law 152-FZ of 27 July 2006, "On Personal Data" [62], it is necessary to obtain consent even for anonymized data. Article 9 of this Federal Law dictated that "the subject of personal data decides on the provision of his personal data and agrees to their processing freely, of his own free will and in his interest". Consent to processing of personal data must be specific, informed, and conscientious. In accordance with Article 91 (part 2) of the Federal Law 323-FZ of 21 November 2011 [61], "On the Fundamentals of Healthcare in the Russian Federation", "processing of personal data in information systems in the healthcare sector is carried out in compliance with the requirements established by the legislation of the Russian Federation in the field of personal data and medical secrecy". Thus, for individuals and institutions dealing with personal data, there are legal risks and limitations that can be regarded as a factor that counteracts medical AI-software development.

Currently, in Russia, developers of medical software are required to register their software with Roszdravnadzor according to regulatory documents and standards, which are currently unavailable for AI-based solutions. However, the authorities are taking measures to remedy this situation. The first part of this standard was released in August 2020 and is available on the Federal Agency for Technical Regulation and Metrology (Rosstandart). State standard "Artificial Intelligence Systems in Clinical Medicine. Part 1. Clinical tests" will regulate the methodological basis of the clinical test process, the procedures for conducting clinical tests, accuracy indicators, and audits and quality control of medical AI systems. The other six parts are: "Technical test program and methodology"; "Application of quality management to retraining programs. Algorithm change protocol"; "Assessment and control of performance parameters"; "Requirements for the structure and application of a dataset for training and testing algorithms"; "General requirements for operation"; and "Life cycle processes".

According to the current regulation, it is exceedingly difficult to obtain subjects' consent to subsequent personal data processing. Therefore, it is difficult to use AI technologies for medical purposes, as they involve the analysis of information about thousands of patients and thus require many consents for the processing of personal data. In July 2020, it was proposed to remove the processing of personal data within the framework of experimental legal regimes from the norms of the federal laws "On Communications", "On Personal Data", and "On the Basics of Protecting Citizens' Health" [63]. However, while the usage of regulatory sandboxes and experimental regimes may represent a solution for understanding the problems, risks, and benefits of AI-based medical software, this proposal was regarded by many experts as very ambiguous and leading to many risks that would be hard to evaluate and prevent.

5. Ownership and Control of the Data

When using personal data such as the health information of patients, AI algorithms need to comply with regulatory frameworks. Accordingly, such data would need to be anonymized, or at least pseudo-anonymized, with an informed consent process that includes the possibility of wide distribution [64].

Therefore, the rules of patient privacy, the notions of patient confidentiality, and cybersecurity measures will be increasingly important in healthcare systems [65]. Currently, healthcare organizations are the owners (and, at the same time, the guardians) of patient data in the healthcare system. However, informed consent from patients would be mandatory should their data be used in a manner not pertaining to their direct care [23].

Some have argued that patients should be the own holder of their health data and subsequently consent to their data being used to develop AI solutions [66], but governance is needed to provide the appropriate regulations and surveillance. Both the GDPR in the EU and California's Consumer Privacy Act in the U.S. legitimately tried to regulate the ownership of health data [23]. Although these regulations are necessary, they may limit the growth of smaller healthcare providers and technology organizations.

The GDPR requires informed consent before any collection of personal data, but it allows processing of anonymized health data without explicit patient consent in the interest of health care in the EU [23].

In the last decade, new issues arose complicating the health data ownership scenario. The healthcare system is in a slow transition from a hospital-centric to a more patient-centric data model [67]. This hinders the integration of new information acquired through health wearables, i.e., devices that consumers can wear to collect data about their personal health and exercise. Moreover, open data sharing has resulted in huge collections of data available in the cloud, which can be used by anyone to train and validate their algorithms [25,40] with the risk of disconnected and non-standardized cloud solutions [25,68].

With the GDPR, healthcare operators and regulatory bodies are called to closely protect patient data [23]. The development of huge health datasets including wide ranges of clinical/imaging data and pathologic information across multiple institutions for the development of AI algorithms will require a reexamination of issues surrounding patient privacy and informed consent. However, Article 23 of the GDPR allows member states to restrict data subject rights, as well as the principles outlined in Article 5, by way of a legislative measure that respects the essence of fundamental rights and freedoms. These restrictions, if they are embodied in necessary and proportionate measures, should aim to safeguard "important objectives of general public interest including monetary, budgetary and taxation matters, public health and social security". With the COVID-19 pandemic, processing personal data was necessary to take appropriate measures to contain the spread of the virus and mitigate its effects. In such a scenario, relevant personal data can be processed in accordance with both Articles 6(1)(d) and (e) of the GDPR because they are necessary either to protect the vital interest of individuals or to safeguard the public interest or the exercise of official authority vested in the controller. Notably, Recital 46 of the GDPR explicitly mentions the monitoring of epidemics as a circumstance in which data processing may serve both important grounds of public interest and the vital interests of data subjects. Nevertheless, specific safeguards should be implemented because of the sensitivity of these categories of data. Among the possible safeguards, policymakers should take measures aimed at: (a) limiting access to the data, (b) establishing stricter retention times, (c) training staff, (d) minimizing the amount of processed data, and (e) keeping records of any related decision-making process.

The ownership of health data is also part of the discussion on the application of different ownership rules to original, deidentified, anonymized, and processed data [69]. Once again, only collaboration among patients, healthcare operators, and policymakers will be able to prevent the risks of inappropriate use of sensitive datasets, inaccurate or inappropriate disclosures, and limitations in deidentification techniques.

5.1. The Problem of Anonymization

In healthcare, a balance between privacy and better user experience is demanded. AI algorithms should use DL to provide patients' data without saving their personally identifiable information. Therefore, anonymization or at least deidentification (true anonymization is an irreversible process that is not easily achievable) must be performed to generate such dataset with removal of all personal health information [70].

However, current anonymization and deidentification techniques are still substandard [71]. There are no currently available certifications for tools or methods for anonymization because no known method can currently guarantee 100% data protection. If data is made anonymous, its information content is inevitably reduced and distorted.

In data anonymization, the conflict between security and usability means that so far, no European data protection authority has extensively evaluated or even certified technologies or methods for data anonymization outside of specific use cases [72]. Collaboration among different institutions is crucial when sharing data to perform ML or DL studies that, by definition, are based on big data.

5.2. Data Protection and Cybersecurity Implications

The legal obligation to protect the privacy of data, especially health data, is a crucial priority, as the circulation of confidential information in huge numbers of copies among many unregulated companies is increasingly risky.

As access to vast amounts of medical data is needed to train AI algorithms [73], policies should prevent the collection of illicit or unverified sensitive data [74]. Although data privacy concerns are still growing, we still face a lack of unique and clear regulations in data protection and cybersecurity regulations [75].

The concept of physician–patient confidentiality requires that a doctor withholds medical information in line with the patient's wishes as long as this poses no risk to the patient or others [24]. Once a medical choice based on AI algorithms is integrated into clinical care, withholding information from digital data impairs the validity of algorithm-driven medical practice. The privacy of such health data must be protected against both external cyberattacks and the same bodies collecting it.

Per the EU Cybersecurity Directive [76], EU member states must respect some requirements to ensure that health operators take appropriate measures to minimize the impact of incidents and to preserve service continuity (Articles 14(2) and 16(2)) (Table 1). Moreover, according to Articles 14(3) and 16(3), supervisory authorities must be notified of incidents without undue delay [75,76].

Table 1. Regulatory framework in the EU on data protection.

Directive 95/46/EC	**Directive on Data Protection Was Replaced by the GDPR**
GDPR	Regulation on data protection Applied from 24 May 2018 Replaced Directive 95/46/EC
Directive (EU) 2016/1148	Directive on cybersecurity Applied from 10 May 2018

EC, European Community; GDPR, General Data Protection Regulation; EU, European Union.

In the U.S., the Health Insurance Portability and Accountability Act (HIPAA) is a compliance focus for health information [54], defining standards to protect patients' data and health information that apply to all healthcare providers, including insurers.

Cybersecurity is dealt with by the FDA, and providers must report only a limited number of risks their devices present and the actions taken to decrease vulnerability [54].

Considering that the amount of data and the number of AI applications can only grow, regulatory actions regarding cybersecurity will face continuous challenges [74]. Instead of resorting to government overregulation, a technological solution of cybersecurity implications is most necessary, as data protection can no longer rely on current technologies that allow the spreading of personal data at a large and uncontrolled scale [77]. Blockchain technology, an open-source software, may allow the creation of large, decentralized, and safe public databases, containing ordered records arranged in a block structure [78]. Different blocks are stored digitally, in nodes, using the computers of the blockchain network members themselves, and the information on all transactions are stored in the nodes [79]. Although blockchain technology is most famously used in field of economics (i.e., cryptocurrencies), its usefulness is extending to other fields, including health data [79]. Blockchain can be used to validate the provenance of and facilitate the distribution of data without compromising the quality of said data. As the blocks are impossible to change, it is impossible to delete or to modify anything without leaving a mark, and this is crucial in the case of sensitive data such as medical information. Unfortunately, the flipside of the coin is that to obtain greater security, privacy is compromised. Patients would need to accept sharing their sensitive data without a central authority to decide what is right or wrong.

6. Accountability and Liability

Alongside AI regulations and data protection issues, there are other legal implications of AI and its use in healthcare, namely, accountability and liability.

Modern medicine is strongly shaped around a multidisciplinary approach. It involves not only medical professionals with different fields of expertise and levels of experience, but also professionals from radically different backgrounds, such as biomedical engineers and medical physicists. Multidisciplinary teamwork has greatly enhanced, both in quality and quantity, the level of healthcare provided to patients. That said, this approach also comes with its unique shortcomings, which include uncoordinated administrative support, insufficient circulation of relevant information, and an excessive focus on a professional's own specific point of view, to the detriment of a holistic, comprehensive evaluation of the patient's case.

Unavoidably, those shortcomings pose a significant challenge not only from a clinical perspective but from a juridical one, as they alter the ordinary criteria that regulate the assessment of medical liability, which—especially when it comes to criminal liability—are traditionally shaped with reference to the individual rather than to a team of a different professionals.

To address this challenge, legal systems have developed a number of consolidated principles aimed at assessing medical liability while taking into account both the different roles and levels/fields of expertise of each professional and the common duties that fall upon all the members of a medical team simply because they work toward the same goal (i.e., the well-being of the patient).

Those principles revolve around the so-called "principle of trust", first theorized by the German doctrine under the name "Vertrauensgrundsatz" [80], which is specifically designed to regulate (from a liability perspective) the various possible forms of collaboration among two or more human professionals. This brings us back to the core topic of this paper: what happens if one of the members of a medical team is an AI-based software or machine? To what extent can the principles that regulate the collaboration among human colleagues be applied when one of those colleagues is not human at all? Is there room—in the juridical mind as much as the clinical one—to conceive a "principle of trust" with reference to a form of intelligence that does not have a human nature? These questions might seem very abstract, but the answers that will be developed within each legal system will certainly lead to very tangible consequences, not only for hospitals and medical professionals but for the companies that produce and market clinical tools based on AI and for the agencies and public authorities that regulate the use of these tools.

For instance, in most European legal systems, the principles that govern the assessment of professional liability within a medical team provide that each member of the team, consistently with their own role and level/field of expertise, has a specific duty to challenge the decisions made by their colleagues anytime they have reasons to believe that those decisions could be detrimental to the patient's wellbeing, particularly if they are aware of any circumstance that would lead them to doubt their colleagues' reliability (among others, overtiredness, inexperience, or lack of information about a particular patient).

If we were to apply the same criteria to the hypothesis of collaboration between a human professional and an AI software, it would be crucial to establish the inherent value attributed to the opinion expressed by this kind of device, also considering that, in most cases, the human professional has no visibility of the reasoning behind such opinion, as AI devices can neither explain nor elaborate on the outcomes of their analysis.

As long as opinion expressed by the AI device aligns to the opinion of the human professional, there is no particular issue, as the AI device acts merely as a confirmation of a previously existing conviction (even though one could argue that the medical professional might feel comforted in a wrong decision and be less inclined to seek consultation with their human colleagues).

On the other hand, if the opinion expressed by the AI device differs from the opinion of the medical professional, the situation becomes more complicated. Taking the situation to its extreme consequences, ultimately, the human professional needs to choose whether to trust the AI device over their own judgment, thereby taking advantage of the full potential of this technical innovation—even though they will be exposed to the liability arising from any mistake committed by the device—or to trust their own judgment over that of the AI device, thereby avoiding any potential liability for a mistake committed by the device.

This is not an easy choice, and not one that medical professionals should be left to face alone. It is crucial that both hospitals and professional associations take an active step toward their employees and members by offering specific instruments (such as guidelines, protocols, and training programs) that can help medical professionals to understand the functioning of the AI devices they use and, therefore, to better assess the reliability of the opinions offered by those same devices and resolve possible discrepancies.

Moreover, as soon as AI devices start making autonomous decisions about the management of patients, ceasing to be only a support tool, problems will arise as to whether their developers can be held accountable for their decisions. As a matter of fact, errors in AI happen mainly when confounding variables are correlated with pathologic entities in the training datasets rather than in actual symptoms. When AI devices make decisions, the decisions are based on a combination of the collected data and the algorithms the devices are based on (and what they learnt). Conclusions of AI algorithms may be unpredictable for humans [81] because, while we consider only the intuitive, AI can evaluate every potential scenario and detail, leaving humans with a decision not derived from a common basis [82,83]. Therefore, it is worth considering whether, when something fails following a decision made by an AI application, it might be the developer of that device, rather than the medical staff who relied on its opinion, that should be considered at fault.

Without some clear guidance and a proper understanding of the potential and limits of the increasingly advanced AI systems that are now being implemented in many hospitals, it can be very difficult for medical professionals to get to know those devices and, therefore, to build real confidence in the support they offer.

Furthermore, specific guidance issued by a reliable a source (be it a hospital or a professional association) could also represent a useful reference from a legal point of view, as abiding by such guidance may—to a certain extent—shield medical professionals from the criminal and civil liability potentially arising from malpractice claims/complaints. Of course, there will always be clinical cases wherein the complexity and peculiarity involved make it impossible to rely on existing guidelines. Nevertheless, guidelines and protocols represent the most common term of reference for courts and authorities that are required to assess the potential malpractice liability of medical professionals, even more so when the cases brought to their attention involve a significant degree of complexity (e.g., because of the number of professionals that handled the same case, or because of the involvement of an AI device).

Therefore, proper guidance could both help medical professionals exploit the full potential of AI devices and protect them against the setbacks of that same technology from a legal standpoint. This could greatly enhance the level of confidence with which both professionals and courts look at the introduction of AI devices in the medical field, as well as the level of trust that patients themselves put in this kind of nonhuman intelligence.

Medical liability cases—like medical practice itself—essentially revolve around the patient or the patient's family. Therefore, educating patients about the potential benefits of the use AI devices is just as important, from a legal perspective, as increasing the sensitivity of courts and authorities toward this very same subject.

In conclusion, although the complexity of AI makes unavoidable that some of its inner workings will always appear to be a black box [74], that is not enough to keep liability out of the question. Because, over the coming years, AI devices are bound to play an increasingly crucial role in the healthcare scenario, the issue of accountability for AI-based decisions will need to be properly addressed by competent authorities, always keeping in mind the core ethical principles of the medical profession: to respect patients and to do good for them [24].

7. Conclusions

Some laws and policies about AI regulation in healthcare, such as the GDPR, have just entered into force. Although, in the short term, such policies may potentially delay AI implementation in healthcare, in the long term, they will facilitate implementation by promoting public trust and patient engagement. With an appropriate and updated legal and regulatory framework around healthcare all over world, good employment of AI may be helpful and powerful for both healthcare providers and patients. On the contrary, bad application of AI may be dangerous. Patients, physicians, and policymakers must work to find a balance that provides security, privacy protection, and ethical use of sensitive information to ensure both humane and regulated management of patients.

Although technological advancement will continue to create new situations for which policymakers will be demanded to create new laws and ethical standards, physicians and healthcare workers should never forget whom they should serve and therefore strictly adhere to their oath, "primum non nocere" (first, do no harm). For this reason, the ownership and control of data and the relevant accountability and responsibility need to be assessed and clarified to realize the potential of AI across health systems in a respectful and ethical way.

Author Contributions: Conceptualization, D.A.B. and G.C.; methodology, D.A.B.; investigation, F.P. and D.A.B.; data curation, D.A.B. and M.B.L.; writing—original draft preparation, F.P., D.A.B., J.F.M., A.L., O.M., M.B.L., P.T., A.S., P.B., P.F.G., E.C. and G.C.; writing—review and editing, F.P., M.B.L. and D.A.B., O.M., P.T.; supervision, G.C.; project administration, G.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Pesapane, F.; Codari, M.; Sardanelli, F. Artificial intelligence in medical imaging: Threat or opportunity? Radiologists again at the forefront of innovation in medicine. *Eur. Radiol. Exp.* **2018**, *2*, 35. [CrossRef] [PubMed]
2. Wu, H.; Chan, N.-K.; Zhang, C.J.P.; Ming, W.-K. The role of the sharing economy and artificial intelligence in health care: Opportunities and challenges. *J. Med. Internet Res.* **2019**, *21*, e13469. [CrossRef] [PubMed]
3. Miller, D.D.; Brown, E.W. Artificial intelligence in medical practice: The question to the answer? *Am. J. Med.* **2018**, *131*, 129–133. [CrossRef]
4. Ching, T.; Himmelstein, D.S.; Beaulieu-Jones, B.K.; Kalinin, A.A.; Do, B.T.; Way, G.P.; Ferrero, E.; Agapow, P.-M.; Zietz, M.; Hoffman, M.M.; et al. Opportunities and obstacles for deep learning in biology and medicine. *J. R. Soc. Interface* **2018**, *15*, 20170387. [CrossRef] [PubMed]
5. Lee, J.-G.; Jun, S.; Cho, Y.-W.; Lee, H.; Kim, G.B.; Seo, J.B.; Kim, N. Deep learning in medical imaging: General overview. *Korean J. Radiol.* **2017**, *18*, 570–584. [CrossRef]
6. Lambin, P.; Leijenaar, R.T.H.; Deist, T.M.; Peerlings, J.; de Jong, E.E.C.; van Timmeren, J.; Sanduleanu, S.; Larue, R.; Even, A.J.G.; Jochems, A.; et al. Radiomics: The bridge between medical imaging and personalized medicine. *Nat. Rev. Clin. Oncol.* **2017**, *14*, 749–762. [CrossRef]
7. Pesapane, F.; Rotili, A.; Bianchini, L.; Botta, F.; Origgi, D.; Cremonesi, M.; Cassano, E. Radiomics of MRI for prediction of pathological response to neoadjuvant chemotherapy in breast cancer: A single referral centre analysis. *Eur. Radiol.* **2021**, *13*, 4271.
8. Pesapane, F.; Rotili, A.; Agazzi, G.; Botta, F.; Raimondi, S.; Penco, S.; Dominelli, V.; Cremonesi, M.; Jereczek-Fossa, B.; Carrafiello, G.; et al. Recent radiomics advancements in breast cancer: Lessons and pitfalls for the next future. *Curr. Oncol.* **2021**, *28*, 2351–2372. [CrossRef]
9. Shaban-Nejad, A.; Michalowski, M.; Buckeridge, D.L. Health intelligence: How artificial intelligence transforms population and personalized health. *NPJ Digit. Med.* **2018**, *1*, 1–10. [CrossRef] [PubMed]
10. Schiaffino, S.; Codari, M.; Cozzi, A.; Albano, D.; Alì, M.; Arioli, R.; Avola, E.; Bnà, C.; Cariati, M.; Carriero, S.; et al. Machine learning to predict in-hospital mortality in COVID-19 patients using computed tomography-derived pulmonary and vascular features. *J. Pers. Med.* **2021**, *11*, 501. [CrossRef] [PubMed]

11. Pesapane, F.; Suter, M.B.; Rotili, A.; Penco, S.; Nigro, O.; Cremonesi, M.; Bellomi, M.; Jereczek-Fossa, B.A.; Pinotti, G.; Cassano, E. Will traditional biopsy be substituted by radiomics and liquid biopsy for breast cancer diagnosis and characterisation? *Med. Oncol.* **2020**, *37*, 29. [CrossRef] [PubMed]
12. Barbieri, D.; Giuliani, E.; Del Prete, A.; Losi, A.; Villani, M.; Barbieri, A. How artificial intelligence and new technologies can help the management of the COVID-19 pandemic. *Int. J. Environ. Res. Public Health* **2021**, *18*, 7648. [CrossRef] [PubMed]
13. Pesapane, F.; Penco, S.; Rotili, A.; Nicosia, L.; Bozzini, A.; Trentin, C.; Dominelli, V.; Priolo, F.; Farina, M.; Marinucci, I.; et al. How we provided appropriate breast imaging practices in the epicentre of the COVID-19 outbreak in Italy. *Br. J. Radiol.* **2020**, *93*, 20200679. [CrossRef] [PubMed]
14. Pesapane, F.; Ierardi, A.M.; Arrichiello, A.; Carrafiello, G. Providing optimal interventional oncology procedures at one of the COVID-19 referral center in Italy. *Med. Oncol.* **2020**, *37*, 83. [CrossRef] [PubMed]
15. Shah, V.; Keniya, R.; Shridharani, A.; Punjabi, M.; Shah, J.; Mehendale, N. Diagnosis of COVID-19 using CT scan images and deep learning techniques. *Emerg. Radiol.* **2021**, *28*, 1–9. [CrossRef]
16. Imaging COVID19 AI. Available online: https://imagingcovid19ai.eu (accessed on 1 September 2021).
17. Mashamba-Thompson, T.P.; Crayton, E.D. Blockchain and artificial intelligence technology for novel Coronavirus disease-19 Self-testing. *Diagnostics* **2020**, *10*, 198. [CrossRef]
18. The Medical Futurist. The (Sober) State of Artificial Intelligence in the Fight against COVID-19. Available online: https://medicalfuturist.com/the-sober-state-of-artificial-intelligence-in-the-fight-against-covid-19/ (accessed on 1 September 2021).
19. IE University. Digital Health and AI in the Time of COVID-19. Available online: https://www.ie.edu/building-resilience/knowledge/digital-health-ai-time-covid-19/ (accessed on 1 September 2021).
20. NHS. *Clinical Guide for the Management of Remote Consultations and Remote Working in Secondary Care during the Coronavirus Pandemic*; NHS England: London, UK, 2020.
21. FDA. *Digital Health Policies and Public Health Solutions for COVID-19*; FDA: Silver Spring, MD, USA, 2020.
22. Clift, A.K.; Coupland, C.A.C.; Keogh, R.H.; Diaz-Ordaz, K.; Williamson, E.; Harrison, E.M.; Hayward, A.; Hemingway, H.; Horby, P.; Mehta, N.; et al. Living risk prediction algorithm (QCOVID) for risk of hospital admission and mortality from coronavirus 19 in adults: National derivation and validation cohort study. *BMJ* **2020**, *371*, m373. [CrossRef]
23. Pesapane, F.; Volonté, C.; Codari, M.; Sardanelli, F. Artificial intelligence as a medical device in radiology: Ethical and regulatory issues in Europe and the United States. *Insights Imaging* **2018**, *9*, 745–753. [CrossRef]
24. Char, D.S.; Shah, N.H.; Magnus, D. Implementing machine learning in health care—Addressing ethical challenges. *N. Engl. J. Med.* **2018**, *378*, 981–983. [CrossRef]
25. He, J.; Baxter, S.L.; Xu, J.; Xu, J.; Zhou, X.; Zhang, K. The practical implementation of artificial intelligence technologies in medicine. *Nat. Med.* **2019**, *25*, 30–36. [CrossRef]
26. Hansen, A.; Herrmann, M.; Ehlers, J.P.; Mondritzki, T.; Hensel, K.O.; Truebel, H.; Boehme, P. Perception of the progressing digitization and transformation of the German health care system among experts and the public: Mixed methods study. *JMIR Public Health Surveill.* **2019**, *5*, e14689. [CrossRef]
27. Gijsberts, C.M.; Groenewegen, K.A.; Hoefer, I.E.; Eijkemans, M.J.C.; Asselbergs, F.; Anderson, T.J.; Britton, A.R.; Dekker, J.M.; Engström, G.; Evans, G.W.; et al. Race/ethnic differences in the associations of the framingham risk factors with carotid IMT and cardiovascular events. *PLoS ONE* **2015**, *10*, e0132321. [CrossRef]
28. Hermansson, J.; Kahan, T. Systematic review of validity assessments of framingham risk score results in health economic modelling of lipid-modifying therapies in Europe. *Pharmacoeconomics* **2018**, *36*, 205–213. [CrossRef]
29. World Health Organization (WHO). *Opportunities and Developments Report on the Second Global Survey on eHealth Global Observatory for eHealth Series*; World Health Organization: Geneva, Switzerland, 2020; Volume 2.
30. Meyer, B.C.; Friedman, L.S.; Payne, K.; Moore, L.; Cressler, J.; Holberg, S.; Partridge, B.; Prince, B.; Sylwestrzak, M.; Jenusaitis, M.; et al. Medical Undistancing through telemedicine: A model enabling rapid telemedicine deployment in an academic health center during the COVID-19 pandemic. *Telemed. e-Health* **2021**, *27*, 625–634. [CrossRef]
31. Centres for Medicare & Medicaid Services (CMS). *COVID-19 Emergency Declaration Blanket Waivers for Health Care Providers*; Centres for Medicare & Medicaid Services (CMS): Woodlawn, MD, USA, 2020.
32. Federation of State Medical Boards. U.S. States and Territories Modifying Requirements for Telehealth in Response to COVID-19. Available online: https://www.fsmb.org/siteassets/advocacy/pdf/states-waiving-licensure-requirements-for-telehealth-in-response-to-covid-19.pdf (accessed on 1 September 2021).
33. Federation of State Medical Boards. Telemedicine Policies Board by Board Overview. Available online: https://www.fsmb.org/siteassets/advocacy/key-issues/telemedicine_policies_by_state.pdf (accessed on 1 September 2021).
34. Rotenstein, L.S.; Friedman, L.S. The Pitfalls of Telehealth—and How to Avoid Them. Available online: https://hbr.org/2020/11/the-pitfalls-of-telehealth-and-how-to-avoid-them (accessed on 1 September 2021).
35. Department of Health & Human Services. *COVID-19 & HIPAA Bulletin Limited Waiver of HIPAA Sanctions and Penalties during a Nationwide Public Health Emergency*; Department of Health & Human Services: Washington, DC, USA, 2020.
36. Jiang, F.; Jiang, Y.; Zhi, H.; Dong, Y.; Li, H.; Ma, S.; Wang, Y.; Dong, Q.; Shen, H.; Wang, Y. Artificial intelligence in healthcare: Past, present and future. *Stroke Vasc. Neurol.* **2017**, *2*, 230–243. [CrossRef] [PubMed]
37. Pizzini, F.B.; Pesapane, F.; Niessen, W.; Geerts-Ossevoort, L.; Broeckx, N. ESMRMB Round table report on "Can Europe lead in machine learning of MRI-data?". *Magma* **2020**, *33*, 217–219. [CrossRef]

38. Pesapane, F. How scientific mobility can help current and future radiology research: A radiology trainee's perspective. *Insights Imaging* **2019**, *10*, 85. [CrossRef] [PubMed]
39. The Cancer Imaging Archive (TCIA). Available online: http://www.cancerimagingarchive.net (accessed on 1 September 2021).
40. Jimenez-Del-Toro, O.; Muller, H.; Krenn, M.; Gruenberg, K.; Taha, A.A.; Winterstein, M.; Eggel, I.; Foncubierta-Rodriguez, A.; Goksel, O.; Jakab, A.; et al. Cloud-based evaluation of anatomical structure segmentation and landmark detection algorithms: VISCERAL anatomy benchmarks. *IEEE Trans. Med. Imaging* **2016**, *35*, 2459–2475. [CrossRef] [PubMed]
41. Fonseca, C.G.; Backhaus, M.; Bluemke, D.; Britten, R.D.; Chung, J.D.; Cowan, B.R.; Dinov, I.; Finn, J.P.; Hunter, P.; Kadish, A.H.; et al. The cardiac atlas project—An imaging database for computational modeling and statistical atlases of the heart. *Bioinformatics* **2011**, *27*, 2288–2295. [CrossRef]
42. UK. Available online: http://www.ukbiobank.ac.uk/ (accessed on 1 September 2021).
43. The European Parliament and the Council of the European Union. *Regulation 2020/561 on Medical Devices Regarding Application Dates of Certain of Its Provisions*; The European Parliament and the Council of The European Union: Strasbourg, France, 2020.
44. The European Parliament and the Council of the European Union. Regulation (EU) 2017/745 of the European Parliament and of the Council on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745 (accessed on 1 September 2021).
45. The European Parliament and the Council of the European Union. Regulation (EU) 2017/746 of the European Parliament and of the Council on In Vitro Diagnostic Medical Devices and Repealing Directive 98/79/EC and Commission Decision 2010/227/EU. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0746 (accessed on 1 September 2021).
46. European Commission. *Science, Research and Innovation Performance of the EU 2018*; European Commission: Brussels, Belgium, 2019.
47. European Commission. MDCG 2018-2 Future EU Medical Device Nomenclature—Description of Requirements. Available online: https://ec.europa.eu/docsroom/documents/28668 (accessed on 1 September 2021).
48. 114th Congress (2015–2016). H.R. 34—21st Century Cures Act. Available online: https://www.congress.gov/bill/114th-congress/house-bill/34 (accessed on 1 September 2021).
49. Méndez, A.J.; Tahoces, P.; Lado, M.J.; Souto, M.; Vidal, J.J. Computer-aided diagnosis: Automatic detection of malignant masses in digitized mammograms. *Med. Phys.* **1998**, *25*, 957–964. [CrossRef] [PubMed]
50. Azavedo, E.; Zackrisson, S.; Mejàre, I.; Arnlind, M.H. Is single reading with computer-aided detection (CAD) as good as double reading in mammography screening? A systematic review. *BMC Med. Imaging* **2012**, *12*, 22. [CrossRef]
51. Recht, M.; Bryan, R.N. Artificial intelligence: Threat or boon to radiologists? *J. Am. Coll. Radiol.* **2017**, *14*, 1476–1480. [CrossRef]
52. Rotili, A.; Trimboli, R.M.; Penco, S.; Pesapane, F.; Tantrige, P.; Cassano, E.; Sardanelli, F. Double reading of diffusion-weighted magnetic resonance imaging for breast cancer detection. *Breast Cancer Res. Treat.* **2020**, *180*, 111–120. [CrossRef]
53. McKinney, S.M.; Sieniek, M.; Godbole, V.; Godwin, J.; Antropova, N.; Ashrafian, H.; Back, T.; Chesus, M.; Corrado, G.S.; Darzi, A.; et al. International evaluation of an AI system for breast cancer screening. *Nat. Cell Biol.* **2020**, *577*, 89–94. [CrossRef] [PubMed]
54. Jaremko, J.L.; Azar, M.; Bromwich, R.; Lum, A.; Cheong, L.H.A.; Gibert, M.; LaViolette, F.; Gray, B.; Reinhold, C.; Cicero, M.; et al. Canadian Association of Radiologists white paper on ethical and legal issues related to artificial intelligence in radiology. *Can. Assoc. Radiol. J.* **2019**, *70*, 107–118. [CrossRef] [PubMed]
55. Thierer, A.D.; O'Sullivan, A.; Russel, R. Artificial Intelligence and Public Policy. Available online: https://www.mercatus.org/system/files/thierer-artificial-intelligence-policy-mr-mercatus-v1.pdf (accessed on 1 September 2021).
56. King, H.E.S. Medtech AI & Software Regulation in China. Available online: https://www.mddionline.com/regulations/medtech-ai-software-regulation-china-5-things-know (accessed on 28 September 2021).
57. China Food and Drug Administration. *Decision of the State Council on Suspending the Implementation of the 'Regulations on the Supervision and Administration of Medical Devices'*; NPC Decision: Beijing, China, 2018.
58. Yang, X.; Yu, X. Preventing patent risks in artificial intelligence industry for sustainable development: A multi-level network analysis. *Sustainability* **2020**, *12*, 8667. [CrossRef]
59. *On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030: Decree of the President of the Russian Federation of 09.05.2017 No. 203*; Boris Yeltsin Presidential Library: St. Petersburg, Russia, 2017.
60. *On the Development of Artificial Intelligence in the Russian Federation: Decree of the President of the Russian Federation of 10.10.2019 No. 490*; Boris Yeltsin Presidential Library: St. Petersburg, Russia, 2019.
61. *Federal Law of the Russian Federation No. 323-FZ of 21.11.2011. On the Fundamentals of Health Protection in the Russian Federation*; The State Duma Library: Moscow, Russia, 2011.
62. *Federal Law of the Russian Federation No. 152-FZ of 27.07.2006. On Personal Data*; The State Duma Library: Moscow, Russia, 2006.
63. *Federal Law of the Russian Federation No. 258-FZ of 31.07.2020. Experimental Legal Regimes for Digital Innovation in the Russian Federation*; The State Duma Library: Moscow, Russia, 2020.
64. Kemp, J.L.; Mahoney, M.C.; Mathews, V.P.; Wintermark, M.; Yee, J.; Brown, S.D. Patient-centered radiology: Where are we, where do we want to be, and how do we get there? *Radiology* **2017**, *285*, 601–608. [CrossRef] [PubMed]

65. The Medical Futurist. Your Data Privacy during a Pandemic. Available online: https://medicalfuturist.com/your-data-privacy-during-a-pandemic/?utm_source=The%20Medical%20Futurist%20Newsletter&utm_campaign=21712e8998-EMAIL_CAMPAIGN_2020_04_28_COVID19_AND_PRIVACY&utm_medium=email&utm_term=0_efd6a3cd08-21712e8998-420636970 (accessed on 1 September 2021).
66. Mandl, K.D.; Szolovits, P.; Kohane, I.S. Public standards and patients' control: How to keep electronic medical records accessible but private. *BMJ* **2001**, *322*, 283–287. [CrossRef]
67. Rajkomar, A.; Dean, J.; Kohane, I. Machine learning in medicine. *N. Engl. J. Med.* **2019**, *380*, 1347–1358. [CrossRef] [PubMed]
68. Bellazzi, R. Big data and biomedical informatics: A challenging opportunity. *Yearb. Med. Inform.* **2014**, *9*, 8–13. [CrossRef]
69. Rosenstein, B.S.; Capala, J.; Efstathiou, J.A.; Hammerbacher, J.; Kerns, S.L.; Kong, F.-M.; Ostrer, H.; Prior, F.W.; Vikram, B.; Wong, J.; et al. How will big data improve clinical and basic research in radiation therapy? *Int. J. Radiat. Oncol. Biol. Phys.* **2016**, *95*, 895–904. [CrossRef] [PubMed]
70. Moore, S.M.; Maffitt, D.R.; Smith, K.E.; Kirby, J.; Clark, K.W.; Freymann, J.B.; Vendt, B.A.; Tarbox, L.R.; Prior, F.W. De-identification of medical images with retention of scientific research value. *Radiography* **2015**, *35*, 727–735. [CrossRef]
71. Aryanto, K.Y.E.; Oudkerk, M.; van Ooijen, P.M.A. Free DICOM de-identification tools in clinical research: Functioning and safety of patient privacy. *Eur. Radiol.* **2015**, *25*, 3685–3695. [CrossRef] [PubMed]
72. Ranschaert, E.R.; Sergey, M.; Algra, P.R. *Artificial Intelligence in Medical Imaging*; Springer: New York, NY, USA, 2019.
73. Kruskal, J.B.; Berkowitz, S.; Geis, J.R.; Kim, W.; Nagy, P.; Dreyer, K. Big data and machine learning—Strategies for driving this bus: A Summary of the 2016 Intersociety Summer Conference. *J. Am. Coll. Radiol.* **2017**, *14*, 811–817. [CrossRef] [PubMed]
74. Castelvecchi, D. Can we open the black box of AI? *Nature* **2016**, *538*, 20–23. [CrossRef]
75. Dilsizian, S.E.; Siegel, E.L. Artificial intelligence in medicine and cardiac imaging: Harnessing Big data and advanced computing to provide personalized medical diagnosis and treatment. *Curr. Cardiol. Rep.* **2014**, *16*, 44. [CrossRef]
76. The European Parliament and the Council of the European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG (accessed on 1 September 2021).
77. Helbing, D.; Frey, B.S.; Gigerenzer, G.; Hafen, E.; Hagner, M.; Hofstetter, Y.; Hoven, J.V.D.; Zicari, R.V.; Zwitter, A. Will Democracy Survive Big Data and Artificial Intelligence? Available online: https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/ (accessed on 25 February 2021).
78. Radanovic, I.; Likić, R. Opportunities for use of blockchain technology in medicine. *Appl. Health Econ. Health Policy* **2018**, *16*, 583–590. [CrossRef]
79. Funk, E.; Riddell, J.; Ankel, F.; Cabrera, D. Blockchain technology: A Data framework to improve validity, trust, and accountability of information exchange in health professions education. *Acad. Med.* **2018**, *93*, 1791–1794. [CrossRef]
80. Baden, B. Das erlaubte Vertrauen im Strafrecht. In *Studie zu Dogmatischer Funktion und Grundlegung des Vertrauensgrundsatzes im Strafrecht*; Nomos: Baden-Baden, Germany, 2017. [CrossRef]
81. Scherer, M.U. Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harv. J. Law Technol.* **2016**, *29*, 354–400. [CrossRef]
82. King, B.F. Artificial intelligence and radiology: What will the future hold? *J. Am. Coll. Radiol.* **2018**, *15*, 501–503. [CrossRef]
83. Mitchell, T.; Brynjolfsson, E. Track how technology is transforming work. *Nature* **2017**, *544*, 290–292. [CrossRef] [PubMed]