# Internet of Healthcare: Opportunities and Legal Challenges in Internet of Things-Enabled Telehealth Ecosystems

Richard Rak
University of Vienna, University of Bologna, University of Turin
richard.rak@univie.ac.at

## ABSTRACT

The COVID-19 public health crisis has accelerated the transformation of health systems to become more closely tied to citizens/patients and increasingly dependent on the provision and use of telehealth services. Internet of Things (IoT)-enabled telehealth systems (deployed in conjunction with AI systems) could facilitate the smart transformation of healthcare from a merely reactive system to a data-driven and person-centred system that provides remote health diagnosis, monitoring and treatment services, integrated real-time response solutions, as well as prospective insights. However, the realisation of these health-related benefits requires the processing of vast amounts of data concerning health. These operations and the use of new enabling technologies raises significant legal concerns and questions the applicability of existing/proposed legal concepts. For this reason, the research analyses the adequateness of EU privacy, data protection, data governance, AI governance and other regulatory rules in IoT-enabled (and AI-augmented) telehealth systems. In addition, the research aims to identify technical and organisational measures (best practices), which could facilitate the implementation of normative principles in these information systems in an effective manner.

## CCS CONCEPTS

• **Applied computing** → Law, social and behavioral sciences; Law.

## KEYWORDS

eHealth, telehealth, Internet of Healthcare, Internet of Things, AI, privacy, data protection, data governance

**ACM Reference Format:**
Richard Rak. 2021. Internet of Healthcare: Opportunities and Legal Challenges in Internet of Things-Enabled Telehealth Ecosystems. In *14th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2021), October 06–08, 2021, Athens, Greece.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3494193.3494260

## 1 INTRODUCTION

The public health crisis caused by COVID-19 has exposed the latent fragilities of health systems and intensified their problems [1]. In order to achieve complex and system-wide changes, the general view is that health systems should be doing more to embrace digital transformation by harnessing data and digital technologies [2]. Data and digital technologies are critical enablers for developing and delivering improved and more personalised health promotion, diagnosis, monitoring and treatment services, and are essential assets for tackling public health emergencies. In the EU, the Commission has emphasised the need to leverage the value of data in healthcare through the uptake of innovative digital technologies and techniques, such as Internet of Things (IoT), cloud infrastructures, data analytics and artificial intelligence (AI) systems [3]. The deployment of new digital solutions and the processing of large volumes of health-related datasets could enable stakeholders to generate meaningful knowledge about the health of individuals and, on a larger scale, of the population. This could facilitate the transformation of healthcare from a merely reactive system to a value-based system that provides integrated real-time tracking and response solutions, as well as prospective insights [4]. However, the Commission has pointed out that success in these endeavours will depend on the availability of vast amounts of high-quality data and appropriate regulatory frameworks that are capable of stimulating innovation while safeguarding the interests of society and the rights of the individual [5].

The pandemic has accelerated the conversion of health systems into a modular ecosystem of delivery, innovation and wellness, more closely tied to citizens/patients and increasingly dependent on the provision and use of telehealth services [6]. Telehealth denotes the use of information and communications technologies to deliver healthcare services at distance [7]. One of the biggest opportunities telehealth presents is increased access to healthcare, especially for underserved persons and communities [8]. During the pandemic, telehealth has become an essential tool in building resilient health systems that are able to adapt to new challenges. When the pandemic undermined in-person patient-physician contact possibilities, especially in general practice, telehealth services shifted to the forefront of primary care [9]. Since the outbreak of COVID-19, healthcare providers have rapidly scaled telehealth services and consumer uptake of telehealth applications has grown at an unprecedented pace [10]. The growing social acceptance of telehealth is, therefore, an opportunity to exploit and translate its capabilities into advancing the smart transformation of healthcare [11].

The inherent tension in telehealth and connected health data ecosystems is that vast amounts of data concerning health needs to be collected, shared, accessed and analysed in order to generate increased value for stakeholders. These efforts are dependent on the uptake of IoT-enabled applications, which can provide increased sensing and communications capabilities about a remotely located individual's health. Although the health-related potentials of using


*ICEGOV 2021, October 06–08, 2021, Athens, Greece*

ACM ISBN 978-1-4503-9011-8/21/10…$15.00
https://doi.org/10.1145/3494193.3494260

data concerning health is enormous, the problem is that these benefits are not realised due to significant concerns about risks posed by unjustified interferences with privacy and/or illicit access to or improper processing of sensitive personal data. For this reason, IoT-enabled telehealth systems (deployed in conjunction with AI systems) must be designed with due regard to regulatory, ethical, technical-architectural and security considerations. On a regulatory level, privacy, data protection, data governance and AI governance should offer adequate legal protection and clarity for all types of data processing operations in the aforementioned information systems.

## 2 RELATED THEORY AND WORKS

### 2.1 Internet of Things in healthcare

IoT envisions a pervasive and self-configuring network infrastructure that interconnects uniquely identifiable objects of the physical world (physical 'things') and of the information world (virtual 'things') with the use of standard and interoperable communication protocols [12]. The revolutionary feature of IoT is that 'things' make themselves recognisable and obtain intelligence by making or enabling context-related decisions due to their capability to communicate information about themselves [13]. Interactions with 'things' are facilitated by interfaces in the form of services which query and change the state of 'things' and information associated with them [14]. In telehealth, IoT devices ('Internet of Health Things') are positioned in proximity to develop relatively stable cyber-physical or cyber-biological connections with the human body [15]. They encompass a diverse range of technologies that rely on the use of embodied (body-centred) computing and materials placed on, around or inside the human body [16]. These solutions include: externally body-affixed (wearable), body-internal or body-melded (implantable, embeddable or ingestible) devices and non-invasive detection modes of visible or bioelectric signals. The common feature of these solutions is that they enable the sensors of IoT devices to perform physiological measurements on the physical and/or biochemical parameters of the human body (and its environment) [17]. In addition to the foregoing devices, it is important to note that IoT devices without an intended medical (health) purpose (e.g. the motion sensors of a mobile phone) may also reveal information about an individual's health [18].

### 2.2 Internet of Healthcare

The deployment and use of IoT devices and concomitant enabling technologies in healthcare could support the integration of telehealth ecosystems, strengthen interconnections between health data ecosystems and leverage data concerning health. On a larger scale, these developments could facilitate the creation of an Internet of Healthcare in which the right information are delivered to the right person (or machine) at the right time and in the right place in order to achieve increased medical intelligence and support decisions affecting health [19]. Although individual IoT devices may send signals that contain valuable data points, advocates argue that it is the combination of multiple data streams what could bring true value to stakeholders in health data ecosystems [20]. An individual using one or more IoT devices may typically share unique types of datasets. Although each of these datasets can help healthcare providers understand a narrowly defined health trend (e.g. blood sugar level), the connection of these unique types of datasets is essential to assemble a multifaceted portrait of the overall health of the individual. On a broader scale, the connection of individuals, each using their own (constellation of) IoT devices, could generate new insights into population health and on how clinical or environmental metrics interact to produce certain outcomes.

## 3 RESEARCH FRAMEWORK AND METHODOLOGY

### 3.1 Research objectives

The purpose of this qualitative research is to describe, explain, critically evaluate and propose reforms to EU legal acts and related privacy, data protection, data governance and AI governance practices that affect the design, implementation and data lifecycle of IoT-enabled telehealth systems that operate in conjunction with AI systems. In connection with these systems, the research seeks to analyse the (lack of) interplay between relevant provisions of EU legislation, understand how specific sources underpin their interpretation and application, and explain what their implications are. On the bases of these findings, the research aims to assess the functioning of legal norms in practice, including of their efficacy and possible shortcomings. Therefore, the main research questions asks: *are existing or proposed EU privacy, data protection, data governance, AI governance and other regulatory rules adequate to effectively protect and govern the processing of data concerning health in IoT-enabled telehealth systems (deployed in conjunction with AI systems)?* The research aims to identify *lex ferenda* measures, state-of-the-art technical tools and good data governance practices, which could be implemented to maximise the benefits and minimise the risks of processing data concerning health in the context of IoT-enabled (and AI-augmented) telehealth systems.

### 3.2 Research methods and sources

The general value of conducting interdisciplinary legal research is that it can help to grasp the forces that act upon the legal system and how the law operates in action, in contrast to just by being interested only in the 'law as such' [21]. In addition to interpreting and systematising the relevant rules, the research aims to connect legal science with other disciplines (and corresponding research methods) in order to explore what the law ought to be in the normative context [22]. The underlying consideration is that privacy and data protection (including data governance and AI governance) rules are 'context-relative informational norms', which means that their normative analyses depends on the distinct social context (healthcare) and technological context (IoT, AI) in which they are interpreted and applied in [23]. To take into account contextual problems and policy issues relating to telehealth and new enabling technologies, the research supplements doctrinal legal research with non-doctrinal legal research methods. This entails the consideration of cutting-edge technologies, cybersecurity solutions, user behavior in information systems and related ethical principles on the bases of academic and non-academic research papers. Special attention is given to sources, which highlight best practices and risk mitigation strategies concerning the design and implementation of IoT-enabled (and AI-augmented) telehealth systems.

In terms of the normative analyses, the sources subject to scrutiny are secondary EU legislative measures adopted or proposed in the area of ICT law and medical law. Sources belonging under ICT law include a broad range of legal acts, the main ones being: the General Data Protection Regulation (GDPR), the ePrivacy Directive, the proposed ePrivacy Regulation, the proposed Data Governance Act (DGA), the proposed Artificial Intelligence Act (AIA) and the forecasted Data Act (due to be tabled in Q3–Q4/2021). Legal sources in the medical (healthcare) sphere encompass the Medical Devices Regulation (MDR), the In-vitro Diagnostics Regulation (IVDR) (applicable from 26 May 2022) and the initiative for a European Health Data Space Regulation (due in Q3–Q4/2021). Since several of the aforementioned sources are still in the legislative or public consultation phases, the research takes into account latest developments. Additional sources for the purpose of legal interpretation may be classified into two categories: the binding judgments of the Court of Justice of the European Union and the (typically) non-binding general guidances and other documents issued by the European Data Protection Board, the European Data Protection Supervisor and the Medical Device Coordination Group. To understand the policy background of the aforementioned legal acts, the research refers to the communications and public consultations of the Commission and the working papers of EU-level expert groups, including the eHealth Network and the High-Level Expert Group on Artificial Intelligence.

## 4 PRELIMINARY RESULTS

The research sheds light on the lack of clarity that existing/proposed EU legal concepts suffer from when applied in the context of IoT-enabled telehealth systems (deployed in conjunction with AI systems). An initial question that needs to be addressed during the development of Internet of Health Things is whether the IoT device qualifies as a 'medical device'. If the answer is affirmative, then the placing on the market, making available on the market or putting into service of the IoT device in the EU are governed by the MDR (and the IVDR). With reference to Article 2(1) of the MDR, the threshold between a 'medical' and 'non-medical' device is the "intended purpose": whether the device is intended to be used by the manufacturer, alone or in combination, for one of the listed "specific medical purposes". The recent rise of consumer (well-being, lifestyle) health devices has blurred the borderline between 'medical' and 'non-medical' devices. In order to prevent potentially risky consumer health devices from falling out of the scope of the MDR, an alternative (or supplementary) regulatory model to the 'intended purpose' could be the introduction of a 'risk-based case-by-case' approach [24].

The boundaries of 'data concerning health' have become obscure in IoT-enabled telehealth systems. With reference to Article 4(15) and Recital 35 of the GDPR, it seems that a case-by-case approach seems the only way to determine what is considered 'direct revelation' of information concerning health. The parameters for determining 'quasi health data' (e.g. inferences which can be drawn about a person's health status from their life habits) necessitates legal clarification [25]. At the same time, IoT-enabled embodied computing has turned the human body into a new 'data platform'. Technological advancements in IoT-enabled neurotechnology devices pose significant challenges to 'informational privacy' and 'informational self-determination', which are prerequisites to exercising rights derived from 'human/patient's autonomy' [26]. For this reason, it would be essential to protect cerebral activity and data, and to adopt a new set of 'neuro-rights' in order to safeguard the individual's cognitive liberty, mental privacy, mental integrity and psychological continuity [27].

Internet of Healthcare is dependent on enhancing sharing of and access to data concerning health. However, the definitions of 'data sharing' and 'access' given by the proposed DGA are dubious, especially in light of the complexities of IoT-enabled telehealth ecosystems. Additionally, the interplay between data protection-based functional roles (i.e. data subject, controller, joint controller, processor, recipient and third party under the GDPR) and data governance-based functional roles (i.e. data holder, data intermediary and data user under the proposed DGA) lack legal clarity [28]. When addressing the latter issue, the legislator should take into account that functional roles in IoT-enabled ecosystems can be viewed from an IoT service-based perspective (e.g. application user, application service provider, application service developer, device manufacturer, platform provider, network provider). This perspective is based on the reference architecture and system models of IoT-related technical standards [29, 30].

Shared computing resources are key to the effective functioning of IoT-enabled telehealth systems (deployed in conjunction with AI systems). Due to the proliferation and heterogeneity of IoT devices and the significant growth in data and traffic, conventional centralised cloud-based data centers are becoming less and less capable of providing efficient and sustainable solutions to IoT-enabled systems and applications [31]. To support and facilitate rapidly developing IoT solutions, there is a trend to shift computing power and resources along the "cloud-to-thing continuum" to the endpoints (edge) of the network in order to better cope with performance, availability, reliability, manageability and cost requirements [32]. IoT-enabled telehealth systems empowered by data science methods (ranging from cloud-based techniques to "embedded" artificial intelligence of things) can transform 'raw big data' into 'smart data' and insights. However, there are currently overlaps and inconsistencies between the GDPR, the MDR and the proposed AIA in terms of the risk management requirements for Internet of Health Things devices used in conjunction with AI systems [33]. It would also be important that the notion of 'cloud infrastructure service providers' is clarified in the proposed DGA; it is unclear whether this new legal notion would encompass other, more scalable and distributed (e.g. fog, edge) computing services.

## 5 FURTHER WORK

The following research steps will focus on the challenge of translating the normative conception of 'privacy and data protection by design and by default' into actionable measures in the context of IoT-enabled telehealth systems (deployed in conjunction with AI systems). The research will map moral and legal requirements that developers and application service providers must satisfy in order to ensure responsible design and trustworthy (ethical and robust) implementation of IoT-enabled telehealth systems (and connected

AI systems). In this regard, the research will provide a risk taxonomy on how the achievement of 'privacy and data protection by design and by default' could be undermined in IoT-enabled telehealth systems (and connected AI systems), if principles relating to the processing of data concerning health are not implemented appropriately and effectively. Ultimately, the research will compare risk management compliance requirements for IoT-enabled telehealth systems deployed in conjunction with AI systems to draw inferences about the practical implications and possible shortcomings of existing or proposed EU privacy, data protection, data governance, AI governance and other regulatory rules.

## ACKNOWLEDGMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska Curie grant agreement No. 814177.

## REFERENCES

[1] OECD and European Union. 2020. Health at a Glance: Europe 2020: State of Health in the EU Cycle. OECD Publishing, Paris, France, 13. DOI: https://doi.org/10.1787/82129230-en

[2] OECD. 2019. Health in the 21st Century: Putting Data to Work for Stronger Health Systems. OECD Health Policy Studies. OECD Publishing, Paris, France, 15. DOI: https://doi.org/10.1787/e3b23f8e-en

[3] European Commission. Commission Staff Working Document Accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018) 233 final, SWD(2018) 126 final (25 April 2018).

[4] Janya Chanchaichujit, Albert Tan, Fanwen Meng, and Sarayoot Eaimkhong. 2019. Healthcare 4.0: Next Generation Processes with the Latest Technologies. Palgrave Pivot, Singapore, 10. DOI: https://doi.org/10.1007/978-981-13-8114-0

[5] European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM/2018/233 final (25 April 2018).

[6] PwC Health Research Institute. 2020. Acceleration of the New Health Economy: The pandemic edits the DNA of the health system. PwC, 1–3. Retrieved from https://www.pwc.com/us/en/industries/health-industries/health-research-institute/assets/pwc-hri-accelerating-nhe-campaign-report.pdf

[7] Tiago Cravo Oliveira Hashiguchi. 2020. Bringing health care to the patient: An overview of the use of telemedicine in OECD countries. OECD Health Working Paper No. 116. OECD Publishing, Paris, France, 10. DOI: https://doi.org/10.1787/8e56ede7-en

[8] World Health Organization Global Observatory for eHealth. 2010. Telemedicine: opportunities and developments in Member States: report on the second global survey on eHealth. Report of the third global survey on eHealth. World Health Organization, Geneva, Switzerland, 13. Retrieved from https://apps.who.int/iris/handle/10665/44497

[9] Livio Garattini, Marco Badinella Martini, and Pier Mannuccio Mannucci, 2021. Improving primary care in Europe beyond COVID-19: from telemedicine to organizational reforms. Internal and Emergency Medicine 16, 255–258. DOI: https://doi.org/10.1007/s11739-020-02559-x

[10] Oleg Bestsennyy, Greg Gilbert, Alex Harris, and Jennifer Rost. 2020. Telehealth: A quarter-trillion-dollar post-COVID-19 reality? McKinsey & Company (29 May 2020). Retrieved from https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality

[11] Healthcare Information and Management Systems Society. 2020. eHealth Study: Non-clinical Telehealth Services Are Most Prevalent, but COVID-19 Accelerates New Trends. HIMSS (7 July 2020). Retrieved from https://www.himss.org/news/ehealth-study-non-clinical-telehealth-services-are-most-prevalent-covid-19-accelerates-new

[12] Roberto Minerva, Abyi Biru, and Domenico Rotondi. 2015. Towards a Definition of the Internet of Things (IoT). Revision 1. IEEE Internet Initiative (27 May 2015), 74. Retrieved from https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

[13] Ovidiu Vermesan, Peter Friess, Patrick Guillemin, and Harald Sundmaeker. 2013. Internet of Things Strategic Research and Innovation Agenda. In: Ovidiu Vermesan and Peter Friess (eds). Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers, Aalborg, Denmark, 7–142 at 8.

[14] Harald Sundmaeker, Partick Guillemin, Peter Friess, and Sylvie Woelfflé (eds). 2010. Vision and Challenges for Realising the Internet of Things. Publications Office of the European Union, Luxembourg, Luxembourg, 43. Retrieved from https://op.europa.eu/s/oKKf

[15] Xiao Liu (ed). 2020. Shaping the Future of the Internet of Bodies: New challenges of technology governance. Briefing Paper (July 2020). World Economic Forum, Geneva, Switzerland, 7. Retrieved from https://www3.weforum.org/docs/WEF_IoB_briefing_paper_2020.pdf

[16] Isabel Pedersen and Andrew Iliadis. 2020. Introduction: Embodied Computing. In: Isabel Pedersen and Andrew Iliadis (eds) Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles. MIT Press, Cambridge, MA, USA, ix–xxxix at xvi. DOI: https://doi.org/10.7551/mitpress/11564.001.0001

[17] Indrakumari Ranganathan, Poongodi Thangamuthu, Suresh Palanimuthu, and Balamurugan Balusamy. 2020. The growing role of Internet of Things in healthcare wearables. In: Valentina Emilia Balas, Vijender Kumar Solanki, and Raghvendra Kumar (eds) Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach. Academic Press, London, United Kingdom, 163–194 at 166–169. DOI: https://doi.org/10.1016/B978-0-12-819593-2.00006-6

[18] Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things (WP 223), 16 September 2014, 7–8 [para. 2.3]. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[19] CISCO Systems. 2015. White Paper: The Internet of Everything (IoE) and the Delivery of Healthcare. CISCO Systems, 1–2. Retrieved from https://www.himss.eu/sites/himsseu/files/education/whitepapers/white_paper_IoE_and_the_Delivery_of_Healthcare.pdf

[20] Jennifer Bresnick. 2016. Can Healthcare Exploit the $7 Trillion Internet of Everything? Health IT Analytics (19 December 2016). Retrieved from https://healthitanalytics.com/news/can-healthcare-exploit-the-7-trillion-internet-of-everything

[21] Mathias M. Siems. 2009. The Taxonomy of Interdisciplinary Legal Research: Finding the Way Out of the Desert. Journal of Commonwealth Law and Legal Education 7, 1, 5–17 at 12. DOI: https://doi.org/10.1080/14760400903195090

[22] Jan M. Smits. 2014. Law and Interdisciplinarity: On the Inevitable Normativity of Legal Studies. Critical Analysis of Law 1, 1, 75–86 at 82–83. Retrieved from https://cal.library.utoronto.ca/index.php/cal/article/view/20974

[23] Helen Nissenbaum. 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Stanford, CA, USA, 3.

[24] Paul Quinn. 2017. The EU commission's risky choice for a non-risk based strategy on assessment of medical devices. Computer Law & Security Review 33, 361–370. DOI: https://doi.org/10.1016/j.clsr.2017.03.019

[25] Gianclaudio Malgieri and Giovanni Comandé. 2017. Sensitive-by-distance: quasi-health data in the algorithmic era. Information & Communications Technology Law 26, 3, 229–249 at 232–234. DOI: https://doi.org/10.1080/13600834.2017.1335468

[26] Andrea M. Matwyshyn. 2019. The Internet of Bodies. William & Mary Law Review 61, 1, 77–168 at 94–115. Retrieved from https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3827&context=wmlr

[27] Marcello Ienca and Roberto Andorno. 2017. Towards new human rights in the age of neuroscience and neurotechnology. Life Sciences, Society and Policy 13, 5. DOI: https://doi.org/10.1186/s40504-017-0050-1

[28] European Data Protection Board and European Data Protection Supervisor, EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), (11 March 2021), Section 3.2.

[29] International Telecommunication Union. Overview of the Internet of things. Recommendation Y.4000/Y.2060 (06/12). International Telecommunication Union, Geneva, Switzerland, Appendix I.

[30] International Electrotechnical Commission. 2018. ISO/IEC 30141:2018(en) Internet of Things (loT) — Reference Architecture, International Organization for Standardization, International Electrotechnical Commission, Geneva, Switzerland, para. 10.5.

[31] Konstantinos M. Giannoutakis, Minas Spanopoulos-Karalexidis, Christos K. Filelis Papadopoulos, and Dimitrios Tzovaras. 2020. Next Generation Cloud Architecture. In: Theo Lynn, John G. Mooney, Brian Lee, and Patricia Takako Endo (eds) The Cloud-to-Thing Continuum. Palgrave Macmillan, Cham, Switzerland, 23–39 at 31. DOI: https://doi.org/10.1007/978-3-030-41110-7_2

[32] Karolj Skala, Davor Davidovic, Enis Afgan, Ivan Sovic, and Zorislav Sojat. 2015. Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing. Open Journal of Cloud Computing 2, 1, 16–24 at 18. DOI: https://doi.org/10.19210%2F1002.2.1.16

[33] Erik Vollebregt. 2021. The new EU AI regulation proposal, medical devices and IVDs (3 May 2021). Retrieved from https://medicaldeviceslegal.com/2021/05/03/the-new-eu-ai-regulation-proposal-medical-devices-and-ivds